

**SOLUTION BRIEF**

# Fortinet and Enea Secure SD-WAN NFV Solution

## Automated, Scalable, and Secure SD-WAN with SDN/NFV Management and Orchestration for White Box uCPE

### Executive Summary

Secure software-defined wide-area networking (SD-WAN) brings the flexibility and cost-efficiency that enterprises are looking for in their digital transformation. Built on white box uCPEs running edge native virtual network functions (VNFs), this new approach is the foundation of a cloud-friendly and agile enterprise network with the potential to accommodate new use cases and growing data traffic.

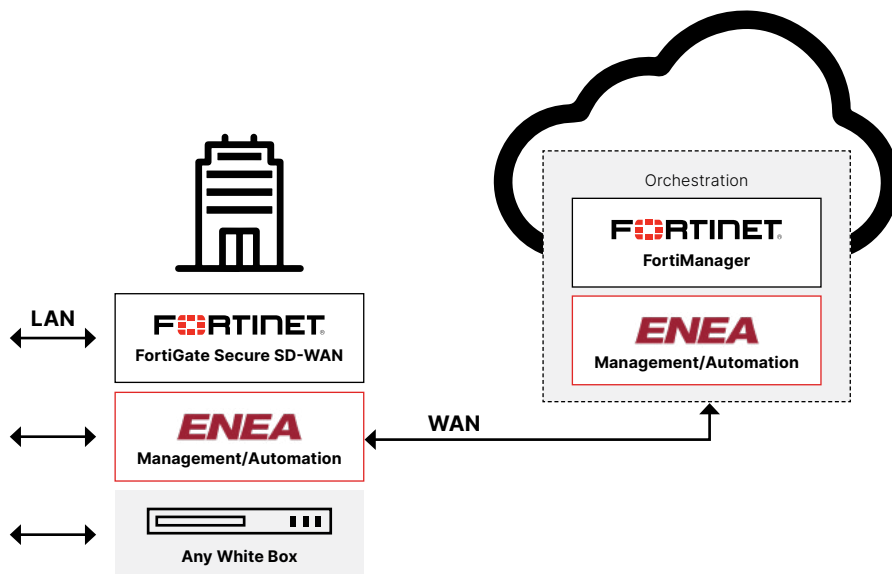
Increasing cyber threats require high-performance and flexible security solutions for SD-WAN. Security is a major consideration when migrating network infrastructure to SDN/NFV, and it needs to be a fundamental part of any SD-WAN implementation, protecting all parts of an enterprise network against malicious attacks and security breaches.

Service providers and enterprises need cost-efficient, scalable, and secure SD-WAN solutions that also provide a good user experience. They want

flexibility to choose white box hardware to keep costs down, they need powerful automation and tools to simplify management and orchestration, and reduce the time to deploy or update services.

### Joint Solution Description

The solution integrates the FortiGate SD-WAN VNF with Enea Edge. This flexible and cost-effective solution is pre-verified and commercially deployable on any white box device scaling from cost-sensitive entry-level to high-performance devices.



### Joint Solution Components

- Fortinet FortiGate Secure SD-WAN
- Enea NFV Access, uCPE Manager

### Joint Solution Benefits

- Cost-efficient secure and virtualized SD-WAN for any white box hardware
- Leveraging the power of FortiGate Next-generation Firewall for Secure SD-WAN
- Flexible and adaptable to different use cases and performance requirements scaling from cost-sensitive tabletop CPE to high-end server deployments
- Powerful automation and secure zero-touch provisioning (ZTP) make large networks and services easy and quick to deploy and manage



Enea Edge Runtime provides the virtualization layer on the uCPE, enabling FortiGate to run as a VNF. Enea Edge Management and Enea Edge Automation provide centralized management and orchestration for automation, ZTP, VNF life-cycle management, FCAPS, telemetry services, and service chaining.

Enea Edge use the industry standard NETCONF protocol for the management interface, keeping complexity and solution footprint to a minimum. This allows the Enea-FortiGate solution to be deployed on any x86 white box uCPE, from slim entry-level devices with as little as 2 cores and 2 GB of RAM, up to high-end devices for high traffic volumes and use cases where FortiGate is chained with other VNFs in multiple configurations.

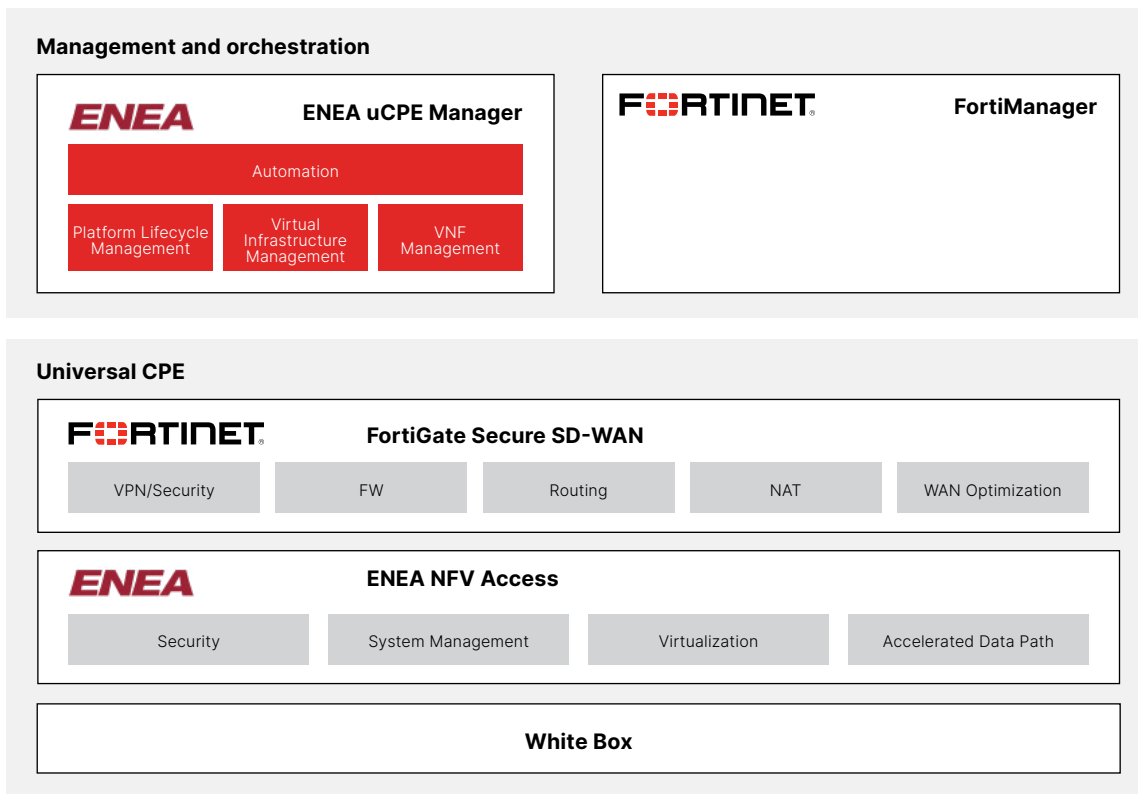


Figure 1: Joint solution diagram.

## Joint Solution Components

### ENEAA Edge

Enea Edge is an open virtualization and management platform for white box uCPEs. It provides minimal footprint and maximum networking performance for SD-WAN and edge applications.

The award-winning Enea Edge is purpose-built to host virtual networking, security, and edge applications on white box uCPE. Unlike solutions originating from the data center, Enea Edge provides virtualization and management without OpenStack, significantly reducing overheads and complexity.

Enea Edge combines the uCPE operating system with extensive cloud-based automation and orchestration capabilities.

## FortiGate Secure SD-WAN

The Fortinet FortiGate network security platform provides high-performance, layered security services and granular visibility for end-to-end protection across the entire enterprise network. Innovative virtual security processor (vSPU) technology delivers high-performance application layer security services (next-generation firewall [NGFW], secure sockets layer [SSL] inspection, and threat protection), coupled with a fast SSL inspection engine to help protect against malware hiding in SSL/transport layer security (TLS) encrypted traffic. FortiGate SD-WAN replaces separate WAN routers, WAN optimization, and security devices with a single solution that is application-aware, offers automatic WAN path control and multi-broadband support. It improves application performance, reduces WAN operating expenses (OpEx) and minimizes management complexity. The platform also leverages global threat intelligence to protect individual customers, by using Fortinet's FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

## About ENEA

Enea develops the software foundation for the connected society. We provide solutions for mobile network traffic management, network virtualization, network traffic classification, embedded operating systems, and professional services. Solution vendors, systems integrators, and service providers rely on Enea when creating new world leading networking products and services. More than 3 billion people around the globe already depend on Enea technologies in their daily lives.

Learn more at [www.enea.com](http://www.enea.com).



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.