Extending Fortinet SD-WAN with Asavie to Secure Mobility and IoT Endpoints

Solving the Enterprise Mobility Security Challenge—Augmenting SD-WAN with Unified Management for Mobile and IoT Endpoints

Executive Summary

Fortinet and Asavie have partnered on a solution that enables mobile network operators (MNOs) and managed security service providers (MSSPs) to deliver highly secure, simplified, and cost-effective Internet-of-Things (IoT) solutions to our joint business customers. The combined offer, called SD Edge, delivers the power of the Fortinet Secure SD-WAN and extends the secure enterprise branch, leveraging Asavie’s technology by eliminating the need for complex virtual private networks (VPNs) and replacing them with a clientless solution for mobile and IoT endpoints.

Joint Solution Benefits

- **Lower cost of ownership:** Maximize return on investment in Fortinet FortiGate by extending protection to mobile endpoints
- **Increased productivity:** CIOs can see all mobile device traffic, facilitating smarter policy management for mobile endpoints
- **Greater insights and controls:** Dashboards offering visibility of all mobile endpoints and granular reporting on a per mobile endpoint basis with real-time security policy controls and enforcement
- **Enhanced security:** No security bypass; policies are applied in the network and are associated to the enterprise mobile SIM
- **Eliminates complexity and cost:** A clientless solution requiring no additional software on the mobile endpoints; ideal for cellular IoT

Business Challenge

70% of enterprise employees don’t sit behind an office desk every day. (Deloitte Insights, “The Untethered Workforce,” December 7, 2018.)

Yet for mobile employees or IoT devices outside the enterprise private network of software-defined wide-area networking (SD-WAN), the connectivity and security experience is less than optimal. CIOs must supplement their SD-WAN with mobile VPN clients, which can be a major source of frustration, not just to the CIO but to road warriors.

- The use of mobile applications for security can be a contributing factor to reduced productivity.
- CIOs and IT lack visibility of what is being accessed on the internet or the necessary controls to manage what mobiles can access online in alignment with corporate internet guidelines.
- Malicious actors are actively targeting mobile devices due to reduced security, creating compliance vulnerabilities in the enterprise.

Enterprises are supplementing their SD-WAN strategy with additional expenditure on siloed solutions to protect mobile assets and VPNs to secure access to enterprise applications. In parallel, the disappearing enterprise perimeter has given rise to zero-trust network access (ZTNA) and cloud access security brokers (CASBs) to protect access to enterprise applications.

Zero-trust access policies utilize unique identifiers such as user single sign-on, location, and device properties of an IP address. However, as mobile IP addresses are not static, this creates a policy challenge for ZTNA. Similarly with CASB, as the focus is on access protection, the mobile endpoint remains unprotected. For as long as mobile endpoints continue to connect to the public internet, the challenge of visibility and control will persist for CIOs.

Asavie has joined the Fortinet Open Ecosystem Partner Program and together we’re addressing the aforementioned challenges of simplifying access to enterprise applications and shielding mobile endpoints from cyber threats. Asavie’s SD Edge allows enterprises to extend the SD-WAN to the mobile edge, in which mobile endpoints appear as a branch of the private network.
The joint solution offers CIOs a unified approach to managing both fixed and mobile assets. Furthermore, CIOs can leverage the enterprise private network and security to protect and manage their mobile and IoT assets. By securing mobile endpoints as a branch of the SD-WAN, CIOs can eliminate the need for mobile VPN clients. Employees now have seamless and secure access to enterprise clouds and applications without the hassle of VPN clients on their devices. The consistent experience inside and outside the enterprise provides for a more productive environment for all. In addition, enterprise IT teams greatly benefit from the unified security management, as mobile endpoints are placed under the same controls of fixed assets, assuring corporate compliance for all assets.

Joint Solution Description
Asavie’s SD Edge combined with the Fortinet FortiGate next-generation firewalls (NGFWs) enables enterprises to extend the enterprise private network to the mobile edge. With minimal effort, CIOs can deliver a seamless enterprise access experience to mobile employees and IoT devices, without the need for software or clients on the devices.

Asavie’s SD Edge extends the power and simplicity of SD-WAN to include mobile devices, which means businesses receive all the power of the Fortinet SD-WAN solution and none of the hassles associated with managing multiple VPN clients across different mobile and IoT device types.

The joint solution from Fortinet and Asavie enables your mobile and IoT endpoints to seamlessly behave as if they are within the enterprise, helping to maximize utilization of existing SD-WAN investments.

The functionality of the joint solution is summarized in the illustration below.

Features:
- Works on all standard mobile devices, eliminating the expense and hassle of managing additional software and hardware per employee
- Secures corporate mobiles from internet threats, wherever the remote employee is working—home, train, conference, etc.
- Minimize rollout effort with over-the-air provisioning, quickly connect individuals to office networks, private data centers, or cloud applications
- Enterprise admin can self-serve security and connectivity management when integrated with Fortinet SD-WAN; includes integrations to enterprise MDMs/UEM for faster rollouts
- Enterprise mobile connections are off the public internet and have clientless access to enterprise private networks/cloud/data centers
- A no-security bypass solution, as the service is tied to the enterprise mobile SIM connection and a private APN

Benefits:
- Increased Security, Endpoints Inside the Enterprise Private Network
  Ease of extending the enterprise private network to mobile and IoT endpoints
- Unified Management
  Simplified and consistent IT administration for all endpoints
- Improved Utilization of Enterprise Security
  Reuse the fixed enterprise network assets to secure mobiles and IoT
Diagram of Joint Solution

Joint Solution Components

Fortinet FortiGate Secure SD-WAN
Fortinet FortiGate Secure SD-WAN offers business application steering, cost savings, and protection for voice, video, and SaaS application performance and availability. Secure SD-WAN includes native integration of NGFW and advanced security features, SD-WAN, and advanced routing capabilities delivering a security-driven networking WAN edge transformation in a single comprehensive solution.

Fortinet FortiGate
FortiGate NGFWs utilize purpose-built security processors and threat-intelligence security services from artificial intelligence (AI)-powered FortiGuard Labs to deliver top-rated protection and high-performance inspection of clear-texted and encrypted traffic. NGFWs reduce cost and complexity with full visibility into applications, users, and networks and provide best-of-breed security.

Figure 1: Unified SD-Branch architecture diagram.
Use Case 1

**Fortinet secure SD-Branch for all endpoints**

- **Visibility across all endpoints.** CIO can now see and control all endpoint traffic
- **Mobile inside private network.** Extension of private network to mobile and IoT (without VPN clients)
- **Single-pane-of-glass management.** Simplified and consistent management and policies for all endpoints
- **Secure fixed and mobile branches.** Embedded NGFWs in secure fixed and mobile branches

Fortinet SD-WAN Rules Engine can be augmented with rules for the mobile SD-branch (e.g., domestic vs. roaming rules by group or individual SIMs).

- Granular Control—Down to individual SIM
- Rich Visibility—Empower CIO with insights

Use Case 2

**Secure web gateway support for all endpoints**

- Fortinet can manage all enterprise endpoints
- Apply unified policies and security
- Single-pane-of-glass management for enterprise CIO
- Clientless solution for mobile and IoT
- Lockdown of mobile/IoT endpoints as no way to bypass
- Still works even if SIM is removed from device; security follows SIM
- Any network controls (e.g., private static IP) will be possible on mobile

![Fortinet Firewall Management architecture diagram](image-url)
About Asavie

Asavie’s vision is to help enterprises transform their businesses in a multi-cloud, multi-network digital world. Our portfolio of self-serve, on-demand services provides unified management of mobile endpoints for a safe internet experience; seamless mobile access to a multi-cloud world and private IoT network.

Asavie’s distributed private network and cloud platform unifies visibility and control across all mobile endpoints, providing enterprises with intelligent insights to reduce cost, increase security, and improve performance of their digital operations.

Learn more at: https://www.asavie.com/products/asavie-sd-edge/.