Note: This document has been translated from the Japanese original for reference purposes only. In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail.

SecuAvail
NEWS RELEASE

To Whom It May Concern

November 27, 2025
SecuAvail Inc. (TSE Growth: 3042)
Masaomi Yoneima, President & CEO

SecuAvail Offers Limited-Time FortiGate Security Configuration Optimization Service for FortiGate SSL-VPN Service Discontinuation

SecuAvail Inc., a company specializing in IT security (Headquarters: Kita-ku, Osaka; President & CEO: Masaomi Yoneima; TSE Growth: 3042; hereinafter "SecuAvail"), will provide a limited-time security configuration optimization service for Fortinet's firewall product line, the FortiGate series, from January to March 2026.

This service not only includes the diagnosis and review of security configurations, but also supports migration from SSL-VPN to IPSec-VPN, enabling organizations to fully outsource optimization tasks related to internal network security operations.

Due to the growing number of security breaches caused by intrusions through FortiGate's SSL-VPN in corporate internet environments, Fortinet has announced that SSL-VPN tunnel mode will be discontinued starting with FortiOS version 7.6.3, urging organizations to switch to IPsec-VPN.

In some models of the FortiGate series, the SSL-VPN function has already been disabled or restricted, and FortiOS 7.4—considered the last branch that still allows continued use of SSL-VPN tunnel mode—is scheduled to reach end of support around May 2026. For users, a planned migration to IPSec-VPN is essential to maintain a secure remote access environment.

In recent years, security requirements in business-to-business transactions have become increasingly stringent. The Ministry of Economy, Trade and Industry (METI) has been promoting initiatives such as the "Security Assessment Framework for Strengthening Supply Chain Resilience" which establishes standards requiring the management and patch application of network equipment. VPN devices, along with other network equipment, are also subject to these standards, making vulnerability management and proper configuration of VPN devices essential.

In light of these circumstances, SecuAvail will offer the following services at special pricing to support companies using FortiGate in implementing appropriate VPN security measures:

- Migration service from SSL-VPN to IPSec-VPN
- Firewall configuration diagnostic service
- Upgrade service to the latest FortiOS

Customers may choose to utilize all or a combination of the above services.

The service will be available from January to March 2026, not only for user companies utilizing FortiGate but also for vendors handling FortiGate products.

Related Article
Firewall Configuration Diagnostic Service Website
https://www.secuavail.com/event/firewall_audit

About SecuAvail Inc.

Founded in 2001, SecuAvail Inc. is one of the few Japan-based companies exclusively dedicated to network security, offering long-term operational support for corporate and organizational information systems. To ensure robust system security and uninterrupted business continuity, the company provides services that are both highly secure and practically applicable.

For over two decades, SecuAvail has offered *NetStare*, an integrated security operations service that uniquely combines the capabilities of both a Security Operation Center (SOC) and a Network Operation Center (NOC).

Through *NetStare*, the company monitors more than 11,000 client network devices in real time, collecting approximately 2.5 billion log entries per day. This enables rapid detection of equipment failures, communication outages, and cyberattacks—24 hours a day, 365 days a year.

To learn more, please visit: https://www.secuavail.com

Trademarks

Company names and product names mentioned herein are trademarks or registered trademarks of their respective owners.

For inquiries regarding this press release:
SecuAvail Inc. – Marketing Group
TEL: +81-3-6264-7180
Email: marketing@secuavail.com

For IR Inquiries (other than the content of this press release)
SecuAvail Inc. – Corporate Planning Division, Attn: Mr. Hayashi
Urban Ace Higashi-Tenma Building, 1-1-19 Higashi-Tenma, Kita-ku, Osaka
TEL: +81-6-6136-0026

【Explanation of Terms】

・**FortiGate**

FortiGate, developed by Fortinet Inc., a leading U.S.-based cybersecurity company, is a next-generation security appliance (firewall) designed to safeguard enterprise networks. According to Fortinet's official announcement, FortiGate commands over 50% of the global market share in terms of units shipped, underscoring its position as the industry's most widely deployed firewall solution. Installed between the internet and internal networks, FortiGate serves as a trusted security gateway, delivering comprehensive protection and ensuring the resilience of corporate IT infrastructures.

FortiOS is the dedicated operating system used in the FortiGate series. It is designed by Fortinet to provide the core functions and security features that power FortiGate firewalls.

・**VPN**

VPN stands for "Virtual Private Network," a technology that creates a virtual tunnel over the internet to protect data from security risks such as information leakage, intrusion, and tampering during transmission. It is used for connecting corporate offices as well as accessing internal systems from home or on the go, and further enhances security through data encryption.

Examples of VPN Usage

1. **Remote Work:** Securely access internal servers and systems from home, while traveling, or on business trips.
2. **Interconnection of Corporate Offices:** Integrate networks across multiple locations to facilitate smooth information sharing.

3.Use of Public Wi-Fi: Ensure secure communication even when using public Wi-Fi networks with low security.

4.IP Telephony: Encrypt VoIP calls made over the internet with VPN to reduce the risk of eavesdropping.

・SSL-VPN Tunnel Mode

A mechanism that uses VPN client software to securely connect from outside to an internal corporate network. Fortinet has discontinued its FortiGate tunnel mode application and is promoting the transition from SSL-VPN, which poses security issues, to IPSec-VPN. For users who have relied on Fortinet's FortiGate firewalls—publicly declared by the company as holding the world's top market share—for remote work and other purposes via SSL-VPN, prompt action is required.

• Overview of SSL-VPN and IPsec-VPN

Category	SSL-VPN	IPsec-VPN
Primary Usage	Remote access to specific applications via a web browser; simple access	Constructs a VPN by encrypting communication between multiple remote sites with fixed IP addresses; requires complex configuration
Encryption	Encrypts data (communication content)	Encrypts all network traffic (entire communication between sites)
Client Requirements	Accessible with just a web browser (can be used on personal devices)	Requires dedicated applications or hardware
Firewall settings	Since the communication port is HTTPS (port 443), it is more susceptible to external intrusion.	Since multiple ports are used, firewall settings can be adjusted as needed.

・Key Points of METI's "Security Assessment Framework for Strengthening Supply Chain Resilience"

1. Cybersecurity risks across supply chains (i.e., business-to-business transaction networks) are increasing. In particular, if subcontractors or suppliers have insufficient security measures, cyberattacks may propagate throughout the entire supply chain.
2. Ordering companies face a challenge in that it is often difficult to assess whether their suppliers have implemented adequate security controls.
3. To address this issue, the Ministry of Economy, Trade and Industry (METI) aims to establish an evaluation framework that "visualizes" the cybersecurity posture of companies. The goal is to launch this new framework in fiscal year 2026.