For Immediate Release

IIJ Develops FSEG, Networking Security Software for Industrial IoT

—Using intent-based network security to realize security countermeasures that prevent interruptions to operations—

TOKYO—November 15, 2018—Internet Initiative Japan Inc. (IIJ, NASDAQ: IIJI, TSE1: 3774), one of Japan's leading Internet access and comprehensive network solutions providers, today announced that it has developed FSEG (pronounced "eff-seg"), a network security suite based on the intent-based network security (IBNS) approach. IIJ will continue to provide factory network security support by entering into alliances with system integrators involved in building and operating networks mainly for factories in the manufacturing industry.

IBNS is an approach in which network administrators establish rules for the network, and then software automatically optimizes the entire network using security policies set by the administrators. The software constantly monitors network traffic, and if a problem arises, the software resolves the incident by automatically taking corrective measures intended to maintain the network's status. FSEG offers mechanisms that automatically distribute the required network configurations and security functions (security VNF(*1)), in accordance with the security policies established by network administrators. SDN(*2) technology provides policy-based segments that differ from conventional L2/L3 segments, and it links multiple security VNFs that are distributed across the network, thereby preventing the spread of problems after their detection and minimizing the harm they cause.

In manufacturing plants, the progress of IoT technology has led to various connected devices throughout factory networks. In the event that a device related to the production process is infected with malware, traditional security policies would isolate the device to prevent the infection from spreading to other devices, but this one-size-fits-all approach could potentially halt the entire production line. FSEG uses SDN technology to manage individual traffic between devices, which allows network administrators to respond by enhancing the monitoring or taking other various measures, without isolating the infected device from the network.

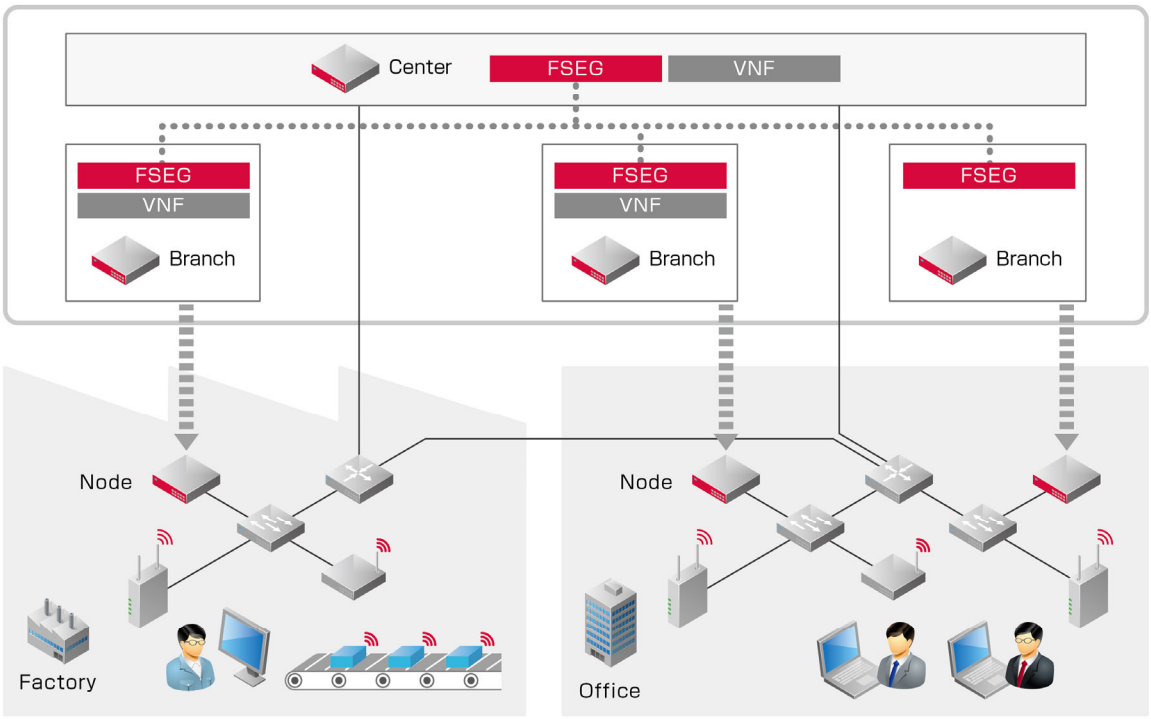
FSEG Features

1) Security policies focused on operational continuity
   Rather than allowing infection to lead to isolation, FSEG mechanisms can increase the monitoring, triage, and segmentation of targeted devices, giving network administrators options in accounting for the effects that measures they take will have on the network or the overall system. Many manufacturers have dedicated networks installed in their production lines. If a manufacturer were to increase monitoring while an infected device remained connected to the network, it would be able to implement a security policy through which its production lines are not halted.

2) No need to install agents
   Because FSEG detects illegitimate traffic and files on the network, it does not need to install agents on each device. As a result, security monitoring is possible for hardware with insufficient specs or for medical devices and other devices on which software cannot be installed due to legal restrictions.

3） Realize whole-network security monitoring
By being distributed throughout and linking the network, FSEG monitors every part of the network, allowing it to detect illegitimate traffic even in environments where connected devices are not fully managed.

Conceptual Diagram



While promoting the introduction of FSEG through alliances with other corporations, IIJ will continue to work on developing services so that users can safely and securely use their networks.

(*1) Virtual Network Function (VNF): Software that provides various network functions. IIJ plans to have FSEG primarily use Trend Micro's security product, Trend Micro Virtual Network Function Suite.

(*2) Software Defined Networking (SDN): This refers to the concept of and architecture for defining networks with software to allow for dynamic network control.

Endorsement

Trend Micro welcomes the announcement that IIJ is offering FSEG. By combining IIJ's software-defined segmentation technology with the Trend Micro Virtual Network Function Suite, which enables the dynamic provision of security functions in NFV environments, users can experience a network security service that responds to their policies. Trend Micro will continue to offer the best security solutions that help users solve their security-related issues.

Hideyuki Tsugane
Head of the Second IoT Business Development Division
IoT Business Promotion Headquarters
Trend Micro Inc.

About IIJ

Founded in 1992, IIJ is one of Japan's leading Internet-access and comprehensive network solutions providers. IIJ and its group companies provide total network solutions that mainly cater to high-end corporate customers. IIJ's services include high-quality Internet connectivity services, systems integration, cloud computing services, security services and mobile services. Moreover, IIJ has built one of the largest Internet backbone networks in Japan that is connected to the United States, the United Kingdom and Asia. IIJ listed on the U.S. NASDAQ Stock Market in 1999 and on the First Section of the Tokyo Stock Exchange in 2006. For more information about IIJ, visit the IIJ Web site at https://www.iij.ad.jp/en/.

The statements within this release contain forward-looking statements about our future plans that involve risk and uncertainty. These statements may differ materially from actual future events or results. Readers are referred to the documents furnished by Internet Initiative Japan Inc. with the SEC, specifically the most recent reports on Forms 20-F and 6-K, which identify important risk factors that could cause actual results to differ from those contained in the forward-looking statements.

For inquiries, contact:
IIJ Corporate Communications
Tel: +81-3-5205-6310 E-mail: press@iij.ad.jp
https://www.iij.ad.jp/en/