Intent-Based Network Security

4.1 Introduction

Have you heard of the term “Intent-Based Networking (IBN)”? A certain vendor made a name for themselves by introducing a product line that greatly changes the approach to network design, management, and operation. However, the concept of IBN existed before this, and it does not specify a particular product or solution.

In conventional networks, the intended actions of the user or network administrator are described in the settings for various network equipment. Before configuring network equipment, it is necessary to convert these intended actions into a language that the equipment can interpret, and then can be applied as settings. Regarding the latter, there are multiple methods for reducing the associated load, such as zero-touch provisioning. This enables configuration from a Web-based interface in addition to CLI (command line interface), along with automatic download from networks. However, the network administrator must comprehend the network topology and properties of the equipment to be used before performing the conversion of settings into a language that network equipment can interpret. With mobile and multi-cloud environments often a prerequisite these days, complexity is also increasing.

■ The Focus is “What,” Not “How”

What if the user or network administrator only had to consider “what” they wanted to do, and the network automatically determined “how” to implement the corresponding configuration? On top of that, imagine if the network was able to monitor and manage itself automatically, responding to problems as the situation demanded. IBN is a concept that aims to implement a system that can do both.

4.2 IBN by IIJ

IBN by IIJ is based on the output of research and development for SDN/NFV products that began in earnest at an IIJ group company established in 2012. Figure 1 is a diagram showing the basic architecture of IBN that was built upon this foundation. The user configures “what” action they want to perform on the network via an orchestrator. This input is converted and passed to the controller layer via an Intent North-Bound Interface. The controller can be located on-premises or in the cloud. In addition, a decentralized model is used for the controller layer, with multiple controllers operating in tandem, and the controller layer determining “how” to configure the required settings for network equipment and VNF (Virtual Network Functions) in the network infrastructure layer. VNF can also be located on-premises or in the cloud. Technologies such as OpenFlow or REST API are used as the network controller interface. Our Intent North-Bound Interface is implemented as a proprietary API.

Specifically, with IBN IIJ is aiming to realize a new system of Intent-Based Network Security even with zero trust environments.

■ Zero Trust Environments

As BYOD and IoT have become more popular, a variety of devices are now connected to corporate networks, and it is also common to see places such as medical and manufacturing facilities with a wide range of equipment connected to their network. On the other hand, appropriate security measures are not always applied to these devices. In some cases, devices do not have enough hardware resources to implement security measures, and software embedded in medical or industrial equipment may not be easy to update. Some environments have no supervision over equipment connected to the network. The number

of attacks against specific organizations and people is currently on the rise, and the techniques used are becoming more sophisticated. In other words, no corporate network environment can be considered safe today, which leads to a zero trust approach. Under this philosophy, no user, device, or application is trusted unconditionally. Therefore, verification is always performed to ensure security.

Policy-Based Segmentation

Micro-segmentation is an approach used to minimize the extent of damages when a fault occurs. It can be divided into several categories depending on the target. At IIJ, "policy-based segmentation" is applied based on the two concepts below (policy).

- All users, devices, servers, PCs, and applications are treated equally as "entities" connected to a network
- Entities are only allowed to connect to certain entities

For example, suppose a person belongs to "project a" and "project b". It is possible to apply multiple policies to a single entity, so segments can be assigned for each project. That is to say, a single entity can belong to multiple segments.

This policy-based segmentation is the fundamental idea behind IBN by IIJ. This system only requires you to consider how entities are connected, making it simple and intuitive for network administrators to handle.

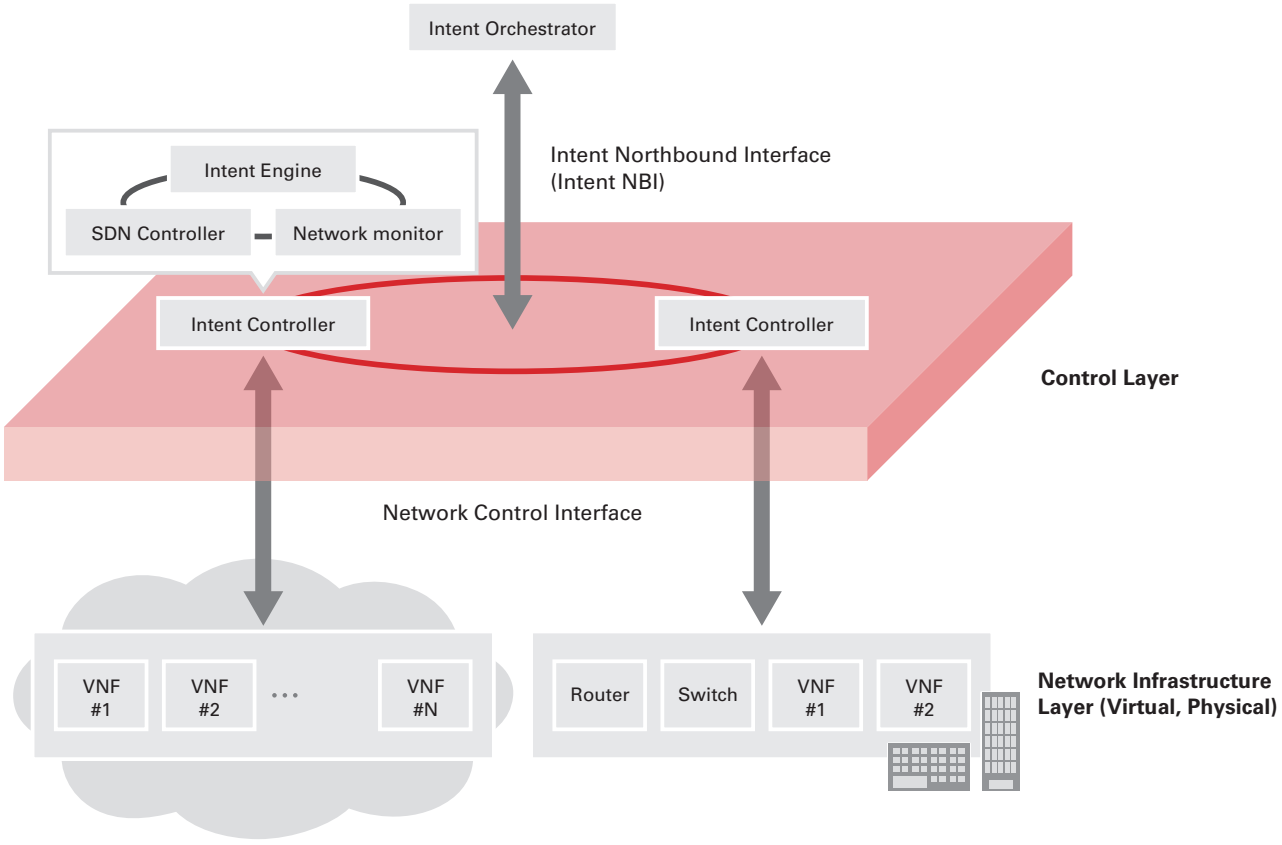

Figure 1: Basic IBN Configuration

Definition of ID and Locator

Normally, an IP address has the dual meaning of ID and locator. While an IP address is a locator (indicating whereabouts) used for routing, from the perspective of upper-layer components such as applications, it is also used as an ID for identifying sessions. As a result, in some cases it is inconvenient for IP addresses to represent two things. For example, when a user or computer moves between networks, a new IP address (both ID and locator) is assigned to the computer, and the session that used the original IP address as the identifier expires. You should only need to update the locator information when a simple change of location is involved, without affecting the ID part of the role.

The main concern of network security administrators is to manage who can access (or cannot access) which information assets, and not the IP addresses themselves. As discussed later, IBN by IIJ solves this issue without managing IP addresses as locators and IDs.

Code Name "FSEG"

Code name "FSEG" is being developed as part of our Intent-Based Network Security initiative. Figure 2 compares the structure of FSEG with the basic structure of the aforementioned IBN. SDN technology is adopted as a method for implementing "monitoring and verification" and "policy-based segmentation" in zero trust environments.

FSEG is an overlay network of which the main components are FSEG controllers and security VNF groups. FSEG controllers can be placed in the cloud, or on PC servers called FSEG nodes in on-premises environments. A full-mesh L3 tunnel connects the FSEG controllers. FSEG controllers have three main functions: authentication of users and devices, policy control (determining the FSEG controllers under which an entity can access devices), and control of security VNF groups (built into FSEG nodes).

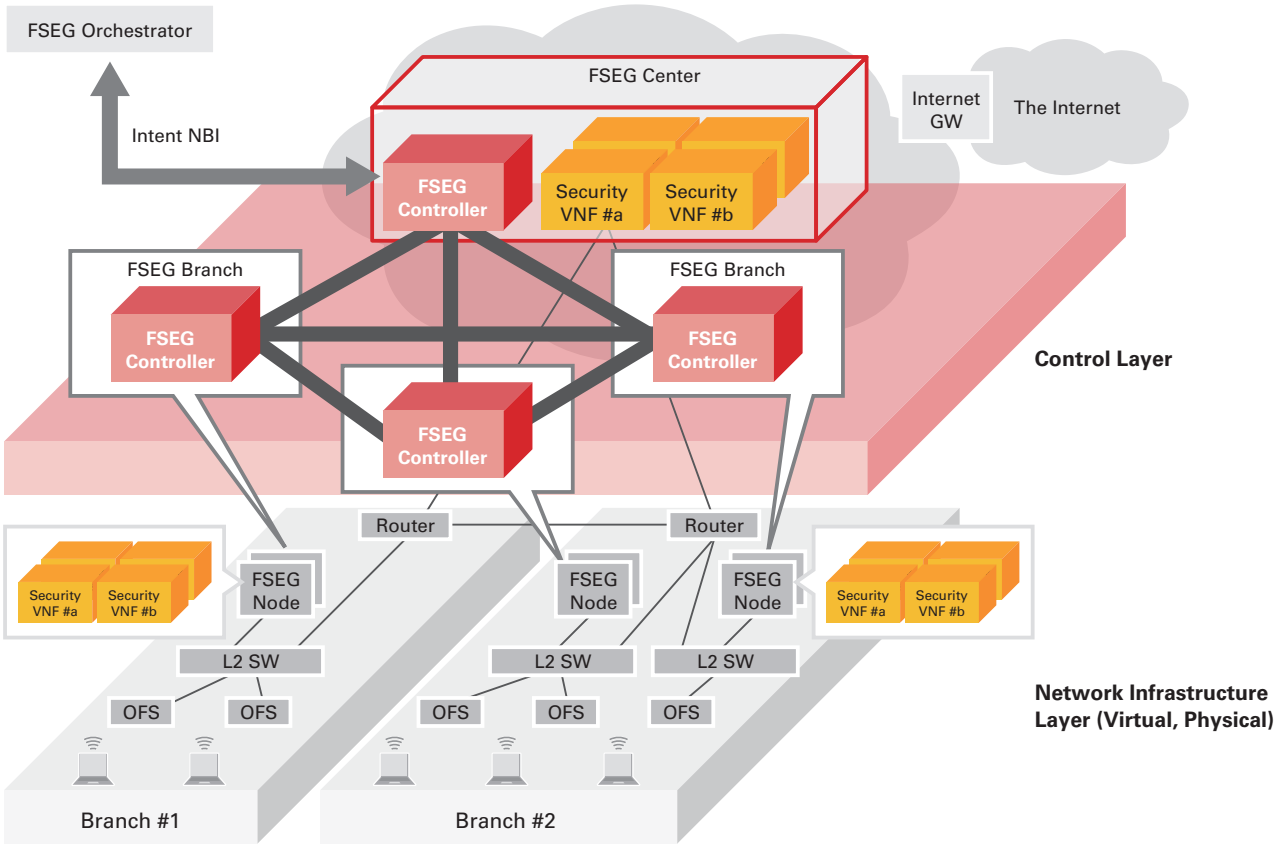

Figure 2: FSEG Overview

FSEG nodes are embedded with security VNF groups in addition to FSEG controllers, and an active-standby configuration for redundancy is an option. Underlay can be simulated with OpenFlow switches connecting users and FSEG nodes in networks.

■ Monitoring and Verification, Segments

Direct communication between devices (port-to-port communication) is prohibited under the OpenFlow switch located within FSEG. All traffic is forwarded to the FSEG node above, so all device-to-device communication is made possible via FSEG nodes. This is for traffic monitoring on FSEG nodes (FSEG controller inside). The FSEG node (FSEG controller inside) also has a policy control function, as well as a database containing policy information indicating "what entity (person or device) can access it." FSEG nodes can apply policies for each type of traffic (controlling the destinations based on the database). Segmentation is implemented by controlling the connection destination for each type of traffic using FSEG nodes. These segments identify "entities," unlike segments based on network equipment settings like conventional VLANs.

The high compatibility with existing networks is one of the characteristics of FSEG. In an FSEG environment, IP addresses are merely underlay technology for connecting entities, and use an FSEG-Private IP address. "Entities" obtain a FSEG-Private address from a DHCP server in FSEG. On the other side, the OpenFlow switches under FSEG nodes can provide NAT function. Therefore, in cases where entities assigned to an existing network use the FSEG environment, this NAT function automatically translates the IP address for inside and outside FSEG. As a result, entities do not need to be aware of changes to the IP address. Regardless of whether the IP address is assigned by the FSEG node DHCP server or the one used in an existing network, the FSEG node manages which type of IP address has been assigned to an entity, so it can be placed under the control of the FSEG controller. FSEG makes it possible to segment all entities and apply policies. This enables existing network environments and FSEG environments to coexist easily, and, for example, customers can start with a small-scale Proof of Concept (PoC).

4.3 Networks with Security Sensors

FSEG Intent-Based Network Security offers new security infrastructure. Not just a concept of intrusion prevention, this constructs a security sensor for early-stage detection and prevention of spreading in enterprise networks today.

■ Entity Authentication

First, FSEG supports multiple authentication systems for a variety of devices to identify entities that are components of policy-based segmentation as below.

- IIJ ID (multi-factor authentication)
- Account + password (Web-based authentication)
- MAC address authentication
- Time range authentication
- Location authentication (which OpenFlow switch it is connected to)
- Combination of the above

Event history is managed for information, such as time range / MAC address / location (switch) / IP addresses, and authentication result.

■ Sharing Threat Information Across All Areas

As mentioned in the previous section, all traffic from entities flows through FSEG nodes, and the FSEG controller on an FSEG node forwards the traffic to associated security VNF. FSEG controllers within the FSEG nodes are also connected via full mesh, and if a threat is detected by a FSEG controller, there is a system for sharing that information with all other FSEG controllers. Each FSEG controller manages whether the security VNF groups under its control are enabled or disabled, as well as which security VNF should be applied to which traffic and in what order (service chaining). Using these systems, after threats are detected in a certain FSEG controller, related FSEG controllers are able to add or edit security VNF, and/or change network settings to isolate the entire segment where the threat was detected. In summary, security sensors covering all networks monitor traffic comprehensively, and can change the shape of networks on the fly based on information obtained through monitoring. Using this same system, load/function balancing between on-premises and cloud can be implemented. For example, when an IPS function located on-premises fails to keep up with processing, a new IPS function can be set up in the cloud to implement load balancing.

■ Preventing Infection

A policy-based segment is a set of entities to which the same policy can be applied. If you were to compare it to a company, it would resemble a group of users and devices in the same department that connect to the same internal work server. A threat discovered in a department could have already spread throughout the department by the time it is discovered. When using FSEG, you can prevent infection in a segment by changing the policy of the segment to which it belongs, based on the threat information found by security sensors. This enables you to perform settings to prevent infection dynamically, such as changing the level of traffic monitoring for each segment where threats are found, or applying new security VNF, to minimize any unexpected damage.

■ Placing Security on Networks

As previously mentioned, we should not assume that security functions have been applied to IoT devices themselves. With government work style reform, in the near future many IoT devices will be used in offices to make the work environment more convenient. These will not operate independently, as communications will always occur with entities outside the device as well. We need to implement security functions on the network side to detect and remove threats. FSEG is the best solution for IoT environments as well, as it treats everything as an entity, while also providing security and preventing infection throughout the entire network.

4.4 Outlook for FSEG

The IBN by IIJ initiative has two strengths. First, we began research and development for SDN technology products at an early stage, and our work is based on the achievements and know-how that we built up by providing our own SDN solutions ahead of other companies, particularly in the enterprise domain. For example, we utilize it to manage traffic used for policy-based segments as described in this report. Our other strength is that we defined a clear and specific use-case, namely providing a new security system for enterprise networks. As a result, it has been easier to obtain the cooperation of partner companies, implementation has already been performed using the methods described here, and a PoC has also been completed.

■ CPE and Switches

While considering the use-case, you should think about how you will provide the service. When providing FSEG as an IIJ solution, we must consider how to design and implement FSEG nodes as CPE installed on the customer side. As mentioned above, in FSEG operation all traffic flows through FSEG nodes. This means traffic loads are concentrated on the FSEG nodes. We have dispelled these concerns using the following three approaches. First, we built a system that did not always require traffic to pass over FSEG

nodes. In cooperation with the OpenFlow switch under an FSEG node, a decision is made for each flow about whether to pass traffic through FSEG nodes. Secondly, the FSEG node itself automatically scales out under high loads. Finally, we use technologies such as DPDK and ASIC for hardware acceleration. We will combine these in the future, so that we can prepare the most suitable solutions for our customers.

Also, although we described a configuration featuring OpenFlow switches under FSEG nodes, OpenFlow switches are not necessarily required. In such cases, entities are directly connected to FSEG nodes, and the functions of the OpenFlow switch explained here (such as prohibiting direct communication between entities) are implemented on the FSEG nodes.

■ Linking to SOC

What is needed to further enhance FSEG implementations of Intent-Based Network Security? FSEG, a security sensor that encompasses an entire network, can collect data from sensors. It is also able to convert "what" the desired action is into "how" it will be implemented. What is missing is a function for determining "what" to do based on large quantities of data. In other words, the goal is "utilizing a large amount of collected data and knowledge-based analysis." IIJ has also launched the wizSafe security brand as part of our security initiatives. The Security Operation Center (SOC) is also up and running, analyzing vast quantities of data and accumulating knowledge. We are considering linking these with FSEG to build a more robust and sophisticated security infrastructure.

■ Conclusion

The approach of customers only needing to be aware of "what" they want to achieve, leaving the question of "how" to implement this up to IIJ, is something that we have been working on for a while. In this report, we discussed our FSEG solutions, which are part of our IBN initiative based on SDN and NFV technology. However, earlier technologies that IIJ developed such as SMF*1, SACM*2, and Omnibus*3 have also brought this concept to fruition. We will continue to develop FSEG, carrying the torch forward and striving to incorporate cutting-edge technology.

Author:
Masakazu Mizuno
Mr. Mizuno is a Senior Product Manager in the SDN Development Department of the Network Division, IIJ. He has been engaged in the development of products and business with SDN/NFV technology since Stratosphere Inc.

*1 SMF (SEIL Management Framework): patented in March, 2006 (patent 3774433).
*2 SACM (Service Adaptor Control Manager): management service infrastructure for providing auto-connect and comprehensive management systems for SMFv2 (Japan: patent 4463868, United States: patent 7660266) to OEM. SMFv2 enables the centralized management of not only "SEIL series" products but also the network equipment of other companies, covering everything from initial settings to configuration changes and operation management.
*3 Omnibus: a new cloud-based network service that utilizes SDN and NFV technology (https://www.iij.ad.jp/omnibus/) (in Japanese).