Network Service That Offers a Versatile Network Environment

MOMIYAMA Nanako, TAKIGUCHI Toshiyuki, ARAKUTA Hiroshi, SHIMIZU Akihiko, MIZUSHIMA Kazunori

Abstract

Conventional ICT systems are often restricted by the physical conditions of the network equipment, leading to a rapid expansion in the use of virtual networks in recent years. The ability to respond quickly to fluctuating demands is critical in the world of ICT, especially in the world of cloud computing, where changes can take place very quickly. Nevertheless, the demand for actual hardware that can take maximum advantage of network systems remains deep-seated. To address both of these needs, NEC Cloud IaaS offers a wide lineup that ranges from the virtual to the physical. This paper discusses the configuration of the NEC Cloud IaaS network service, which creates a powerful and versatile network environment ideal for today's requirements.

Keywords

cloud, SDN, network service, physical appliance, virtual appliance

1. Introduction

One of the key requirements of a cloud network today is that it be provided with the functionality and performance necessary to support mission-critical applications, as well as the ability to adapt rapidly to changing needs. In order to facilitate the transition to cloud systems and make the most of all assets, it is also important to effectively manage housing systems and connectivity with the user base and other data centers (DCs).

NEC's Cloud IaaS network includes the following features and concepts:

(1) Wide lineup to meet different user requirements
(2) Network configuration flexibility including external connections
(3) On-demand capability that allows users to use network resources according to their requirements

NEC Cloud IaaS has been designed and built in order to achieve the concepts outlined above. The overall configuration that users can create within the tenant network is shown in **Fig**.

In addition to the private tenant network, NEC Cloud IaaS offers external connection services including Internet connections, virtual private networks (VPNs), and dedicated line connections, as well as firewalls and load balancers. These services and the component technologies that make them possible are described in the following chapters.

2. Basic Network (Virtual LAN)

In the NEC Cloud IaaS, the network rent out to tenants is called a "virtual LAN." The virtual LAN includes a LAN to connect to a server that functions as a system hub connecting servers and network services, a LAN to connect to the Internet, and a LAN to connect to the storage devices where data is stored. Creating and setting the virtual LAN can be performed by users from a self-service portal.

NEC Cloud IaaS offers two services: High-Availability (HA) with high performance and high reliability and Standard (STD) with high cost performance. The HA's virtual LAN utilizes NEC's WebSAM vDC Automation and UNIVERGE PF Series to achieve secure tenant separation and path isolation using a virtual tenant network (VTN) while the STD's virtual LAN uses a VXLAN. The VTN is mapped in the VLAN, as well as in the VXLAN. By taking advantage of these features, we have improved connectivity, inter-tenant separation and isolation, and improved privacy.

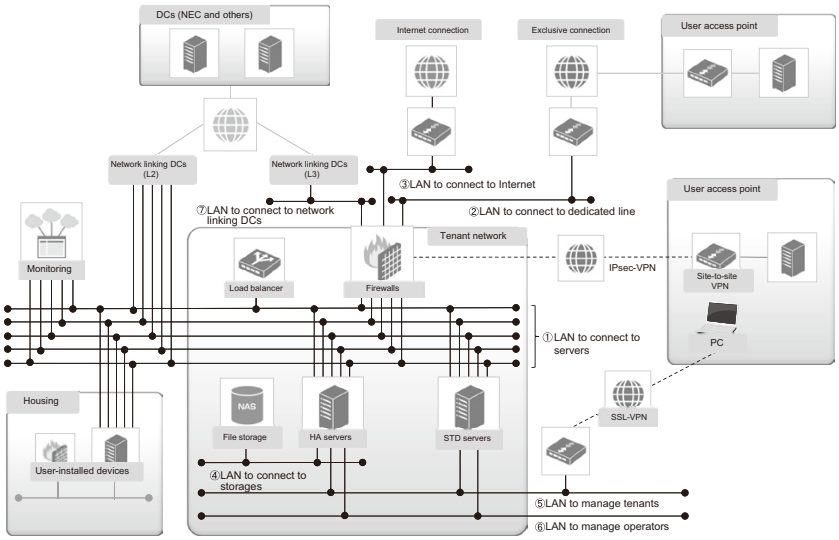

Fig. Outline of NEC Cloud IaaS network service.

3. SSL-VPN

For connection routes that allow users to manage the servers they have created in their tenant network, we offer internet VPNs that use SSL-VPNs. When the users are admitted to tenants, dedicated interfaces and communication policies for SSL-VPN devices are automatically generated and set. Validation/invalidation of the SSL-VPNs and password changes are operable from the self-service portal.

4. Physical Appliances

Network appliances that provide the firewall and load balancing functionality required for network configurations in the form of physical hardware are called “physical appliances.” In the NEC Cloud IaaS’s physical appliance service, the original functions provided by the physical hardware are prioritized according to user needs and then offered to the users. With the objective of providing homogenous services even with the virtual appliances described below, this makes it possible to use network services from the self-service portal while still enjoying the same level of operability.

4.1 Firewall (physical)

The firewall services available from physical appliances include a sharing service and an exclusive service. The sharing service provides each user with a firewall device combined with multiple logical firewalls up and running, while the exclusive service makes it possible to take maximum advantage of the device’s capability by letting one user use it exclusively for their tenant network.

When the user signs the contract for the firewall service at the self-service portal, the processes that are required to start using the firewall, such as creation of a logical firewall for a device and setup of communication policy, are executed sequentially. When the user requires an Internet connection, allocation of a global IP address and firewall setting are also performed.

The user can set communication policies for the firewall from the self-service portal.

4.2 Load Balancer (physical)

The load balancing service provided by a physical appliance also features a sharing service and an exclusive service. In the sharing service, logical partitioning is applied to the load balancing resources to provide load balancing to each user. In the exclusive service, on the other hand, the full capabilities of the device are put exclusively at the disposal of a single user’s tenant.

When the user signs the contract for the load balancing service at the self-service portal, the allocation of logical resources and the processes that are required to start using the load balancer are executed sequentially.

The user can perform various settings on the load balancer from the self-service portal; such as virtual server setting, allocated server setting, and health check setting.

5. Virtual Appliances

NEC’s Cloud IaaS offers a firewall and load balancer as virtual appliances. These are built around NEC’s InterSecVM. Virtual appliances are virtual machines on Hypervisor that operate on the general-purpose x86 server. Virtual machines

make it possible to provide the same functionality as a dedicated physical machine at a lower cost.

We developed the REST API cluster to enable users to operate and set the virtual appliances from the self-service portal, while enjoying the same capabilities as would be available from the physical appliances.

5.1 Firewall (virtual)

From the self-service portal, users can control basic firewall's functions in the tenant's network, such as access policy control to determine who is and who is not permitted access from private tenant networks and from the Internet, as well as routing control, and inbound NAT conversion. Operations performed by the user at the self-service portal are interlocked with the REST API cluster, and the settings are made in the firewall.

5.2 Load Balancer (virtual)

Load balancing functions for the virtual servers in tenant networks are provided using a round-robin or least-connection distribution method. Also provided are basic load balancing functions such as session maintenance, health check, and SSL encryption functions, all of which can be accessed from the self-service portal. The operations performed by the user at the self-service portal are interlocked with the REST API cluster, and the settings are made in the load balancer.

6. External Connection Service

6.1 Internet Connection

Servers are provided with Internet connectivity. Best effort and bandwidth guaranteed menus are provided to give users more control over Internet connection usage. Best effort and bandwidth guaranteed menus can be used separately or in combination.

When the server is connected to the Internet, the connection is made via various network devices such as bandwidth control devices, Internet connection switches, and firewalls. Without consistent settings in all of these devices, a reliable, easy-to-use Internet connection is not possible. Logic and API clusters to ensure consistent settings have been incorporated in the NEC Cloud IaaS. This makes it possible to automate the Internet connection and coordinate it with the operations performed by the user at the self-service portal.

6.2 Site-to-site VPN

As one of the means to securely connect between the user site and the user tenant network, a VPN gateway (VPN GW) function is provided to make possible VPN connection via the Internet. By offering the VPN GW function as a firewall option, integrated access control from the self-service portal is possible even for VPN communications.

To avoid the restrictions on the VPN GW (vendors, products, applications, etc.) that may be applied at the user site, we use IPSec, which is the standard system for an inter-site VPN.

6.3 Dedicated Line Connection

When users provide dedicated line devices on their sites and at the NEC Cloud IaaS site, they can make an exclusive connection between their site and the NEC Cloud IaaS.

6.4 Inter-DC Network Connection

Network connection is possible between the NEC cloud IaaS and NEC's main DCs. We offer best effort and bandwidth guaranteed menus to make it possible to flexibly configure inter-DC network connection as is the case with the Internet connection described in 6.1 above. It is also possible to use the best effort and bandwidth guaranteed menus in combination.

The following two menus are offered as connection policies. Connection is possible whether or not the server inside the NEC Cloud IaaS and the device in the DC on the opposite side have the same network addresses.

(1) Bridging connection (L2) service
(2) Routing connection (L3) service

7. Housing Coordination Service

DCs that offer the NEC Cloud IaaS offer housing services in the same building. The users of the NEC Cloud IaaS can use both the housing services and the NEC Cloud IaaS.

By using the housing service, the users can communicate with the NEC Cloud IaaS within the housing environment. When a user installs the housing environment with devices and functions not available from the NEC Cloud IaaS, users can expand the capabilities of the NEC Cloud IaaS and enjoy greater flexibly.

8. Automation of Network Services

In this section, we will discuss the automation of the network services provided by the NEC IaaS. We developed our automation functions in order to automate the allocation of the network services described above and to make those services available at the self-service portal.

The NEC Cloud IaaS uses a wide array of network devices. Although we cannot introduce all of them, some of the most important include NEC's Software-Defined Networking (SDN) products - the UNIVERGE PF Series, QX Series, and IX Series, as well as NEC's WebSAM vDC Automation and

InterSecVM. OEM products and non-NEC products include Fortinet's FortiGate, F5 Networks' BIG-IP, Anritsu Networks' PureFlow, and Cisco's Router Switch.

These devices have different specifications, setting methods, access protocols, and execution multiplicities. To achieve an appropriate network service, it is essential that devices are managed and controlled to ensure that settings are consistent between devices. While ensuring these controls, the functions developed to automate the allocation of network services and of making them available at self-service portals are called "SDN automation functions."

SDN automation functions are composed of the SDK layer, which conceals setting methods, access protocols, and authentication methods that differ depending on devices, the sequence layer, which controls the sequences of devices in combination with the SDK layer, and the network service layer, which performs the settings by controlling multiple sequence layers.

Operations performed by the users at the self-service portal are transferred to the network service layer, while processing for multiple devices is performed at appropriate multiplicities and sequences. The differences in the specifications and setting methods depending on the devices are handled here. By interacting with the GUI at the shared self-service portal, the user can use the network services without having to perform complicated settings for individual devices.

9. Conclusion

In this paper, we have described the network service that offers a versatile network environment that is provided via NEC Cloud IaaS. NEC's Cloud IaaS incorporates a wide array of appliances, while using SDN to ensure flexible and rapid responsiveness to changing requirements. The result is a diverse range of offerings, flexible user-configurable networks, and on-demand capabilities. At NEC, we are committed not only to keeping pace with the fast-changing world of ICT and cloud computing, but in pushing forward and pioneering new and improved network services to meet the ever-changing needs of our users.

* FortiGate is a registered trademark of Fortinet, Inc.

* BIG-IP is a trademark or registered trademark of F5 Networks, Inc. in the U.S. and other countries.

* PureFlow is a registered trademark of Anritsu Corporation.

Authors' Profiles

MOMIYAMA Nanako
SDN Strategy Division

TAKIGUCHI Toshiyuki
SDN Strategy Division

ARAKUTA Hiroshi
Assistant Manager
SDN Strategy Division

SHIMIZU Akihiko
Manager
3rd Software Division
NEC Solution Innovators, Ltd.

MIZUSHIMA Kazunori
Assistant Manager
UN System Division
NEC Solution Innovators, Ltd.

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.9 No.2 Special Issue on Future Cloud Platforms for ICT Systems

Remarks for Special Issue on Future Cloud Platforms for ICT Systems
NEC's Approach to Orchestrating the Cloud Platform

NEC C&C cloud platforms ? NEC Cloud IaaS Services
Portal Services Integrate Multi-Cloud Environments
A Hybrid Server Hosting Which Have Broader Range of Applications
Network Service That Offers a Versatile Network Environment
Dependable Security Service That Takes Advantage of Internal Control Methodology
Data Center Service That Supports Cloud Infrastructure

Products and latest technologies supporting NEC C&C cloud platforms
MasterScope Virtual DataCenter Automation - Entire IT System Cost Optimization by Automating the System Administration
Integrated Operation and Management Platform for Efficient Administration by Automating Operations
Micro-modular Server and Phase Change Cooling Mechanism Contributing to Data Center TCO Reduction
iStorage M5000 Providing a High-Reliability Platform for the Cloud Environment
The iStorage HS Series Features the Superior Data Compression and High-Speed Transmission Capabilities that are Essential Functions of Big Data Storage
SDN Compatible UNIVERGE PF Series Supports Large-Scale Data Centers by Automating IT System Management
Phase Change Cooling and Heat Transport Technologies Contribute to Power Saving

Future technology for NEC's C&C cloud platforms
Accelerator Utilization Technology That Cuts Costs, Reduces Power Consumption, and Shrinks Hardware Footprint
Scalable Resource Disaggregated Platform That Achieves Diverse and Various Computing Services
Support Technology for Model-Based Design Targeted at a Cloud Environment
Cloud-based SI for Improving the Efficiency of SI in the Cloud Computing by Means of Model- Based Sizing and Configuration Management
Big Data Analytics in the Cloud - System Invariant Analysis Technology Pierces the Anomaly -

Case Studies
Using Cloud Computing to Achieve Stable Operation of a Remote Surveillance/Maintenance System Supporting More Than 1,100 Automated Vertical Parking Lots throughout Japan
Meiji Fresh Network's Core Business Systems are Transitioned to NEC Cloud IaaS NEC's Total Support Capability is Highly Evaluated.
Sumitomo Life Insurance Uses NEC's Cloud Infrastructure Service to Standardize IT Environments across the Entire Group and Strengthen IT Governance

Vol.9 No.2
June, 2015

Special Issue TOP

NEC Information

NEWS
2014 C&C Prize Ceremony