Interconnection between the Windows Azure Virtual Network and SEIL Series VPN

Updated: January 17, 2014

Author: Internet Initiative Japan, Inc.

SEIL (http://www.seil.jp/) is an access router for companies developed by the ISP Internet Initiative Japan (IIJ). It allows for the interconnection between the Windows Azure virtual network and IPsec based VPN. By setting up a VPN, users can use LAN computers to easily access virtual machines on Windows Azure.

Index

Advance Preparations

To begin, subscribe to Windows Azure. Also complete set up procedures as shown below. Then set up SEIL, which will become the VPN gateway for the LAN side, so that it can connect to the internet in advance.

Item	Example	Notes
Virtual Network Address Space	10.0.0.0/8	
Virtual Network Subnet for Use with VPN	10.0.0.0/11	
Windows Azure VPN Gateway Address (global address)	Automatically Created	Checked after setting up virtual network
IKE Pre-Shared Key	Automatically Created	Checked after setting up virtual network
SEIL Global IP Address	203.0.113.1	
SEIL Private Address Space for Use with VPN	192.168.10.0/24	

Windows Azure Set Up

1. Network Management

Open up “NETWORKS”, then click “CREATE A VIRTUAL NETWORK.”

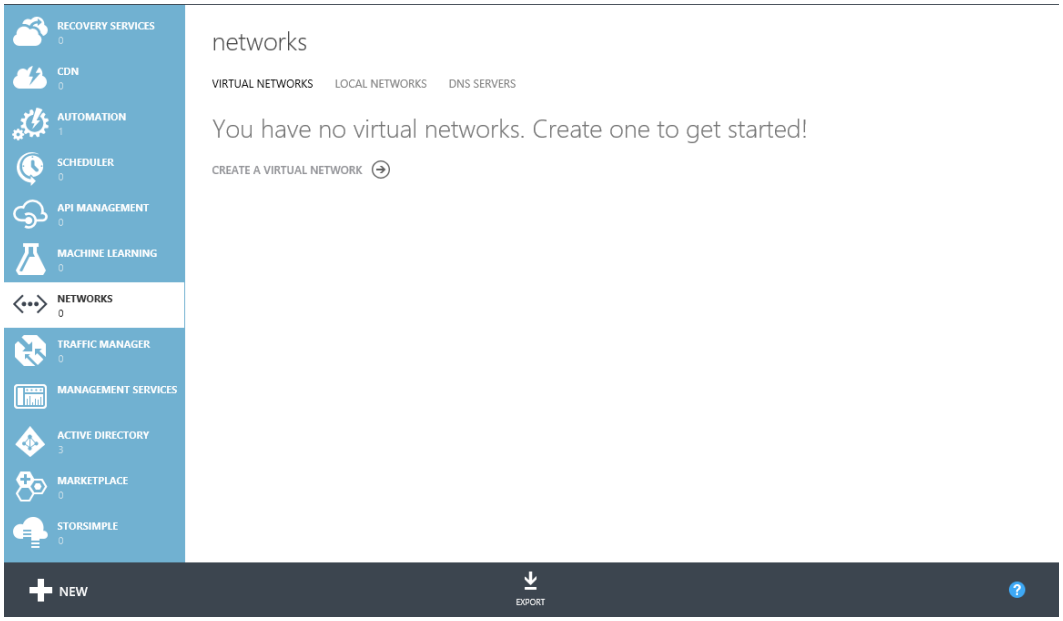

Figure 1

2. Virtual Network Creation

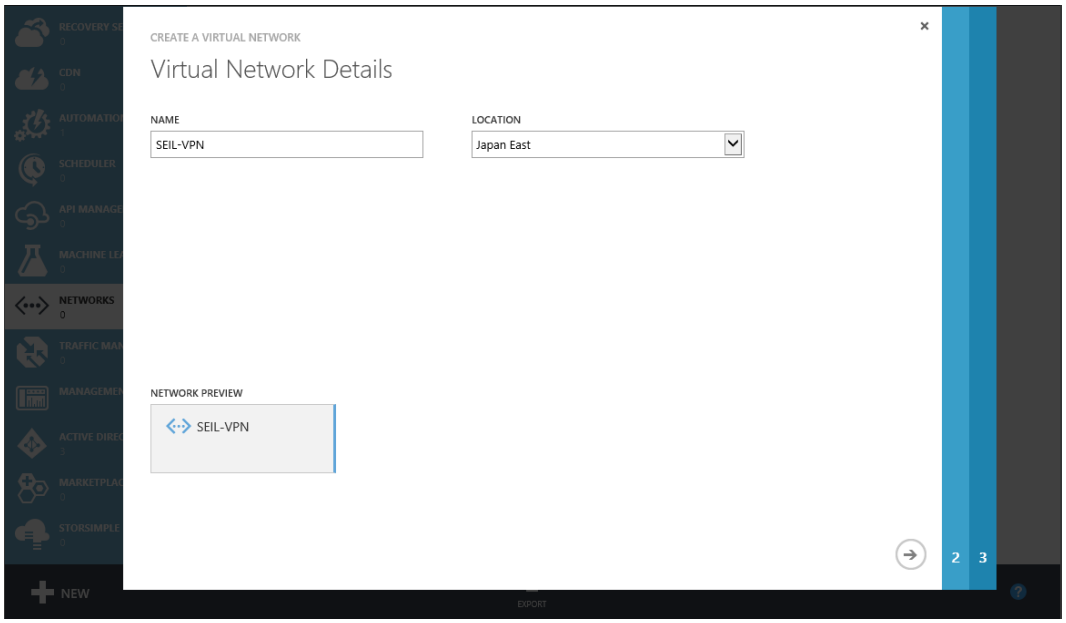

Figure 2

- **NAME**: Enter your chosen name.
- **LOCATION:** Enter your chosen location.

3. Gateway Setup

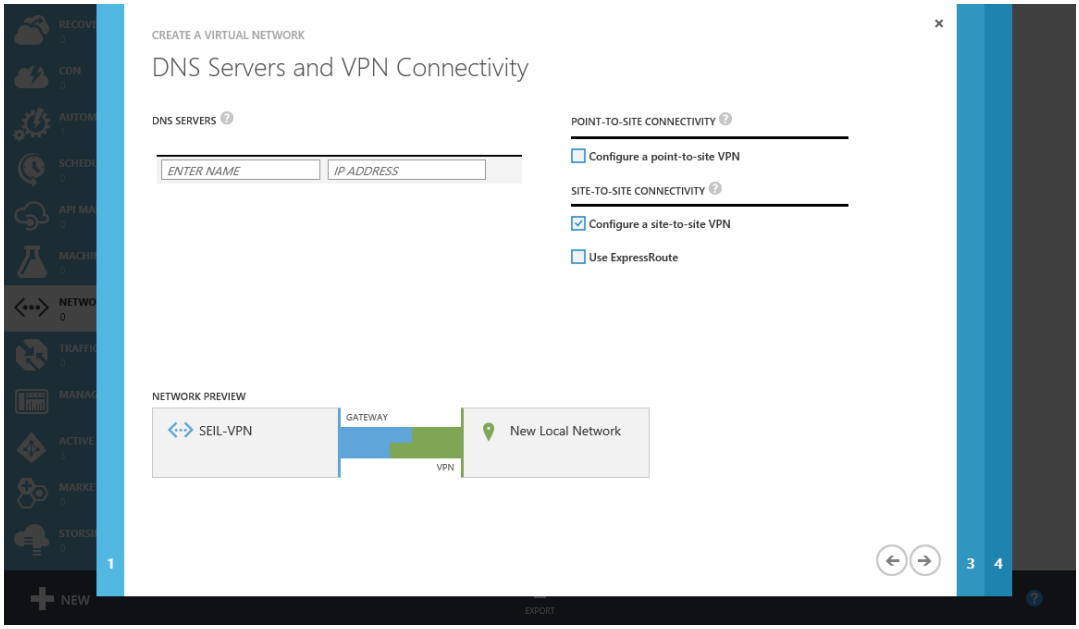

Figure 3

Select the “Configure a site-to-site VPN.”

4. SEIL Network Setup

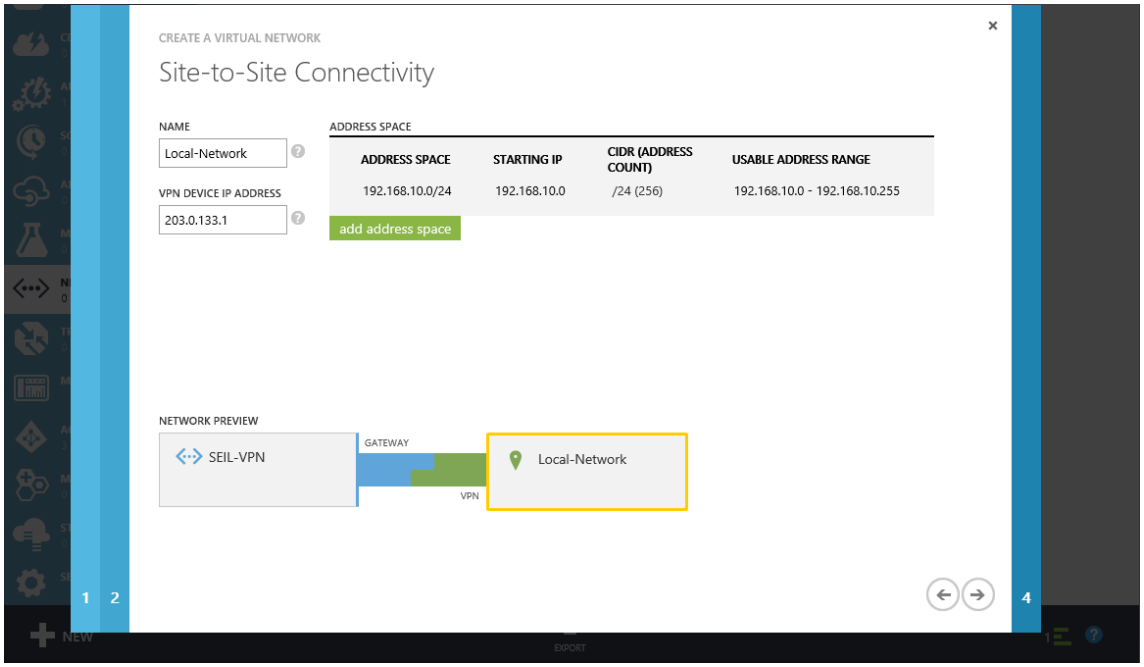

Figure 4

- **NAME:** Enter your chosen name.
- **VPN DEVICE IP ADDRESS:** Enter the global IP address used when SEIL connects to the internet.
- **ADDRESS SPACE:** Enter "STARTING IP" of the address space and "CIDR" of the address space.

Note:

"STARTING IP" is also known as "network address" and "CIDR" is also known as "prefix length". SEIL series often use the terms "network address" and "prefix length."

5. Virtual Network Information Setup

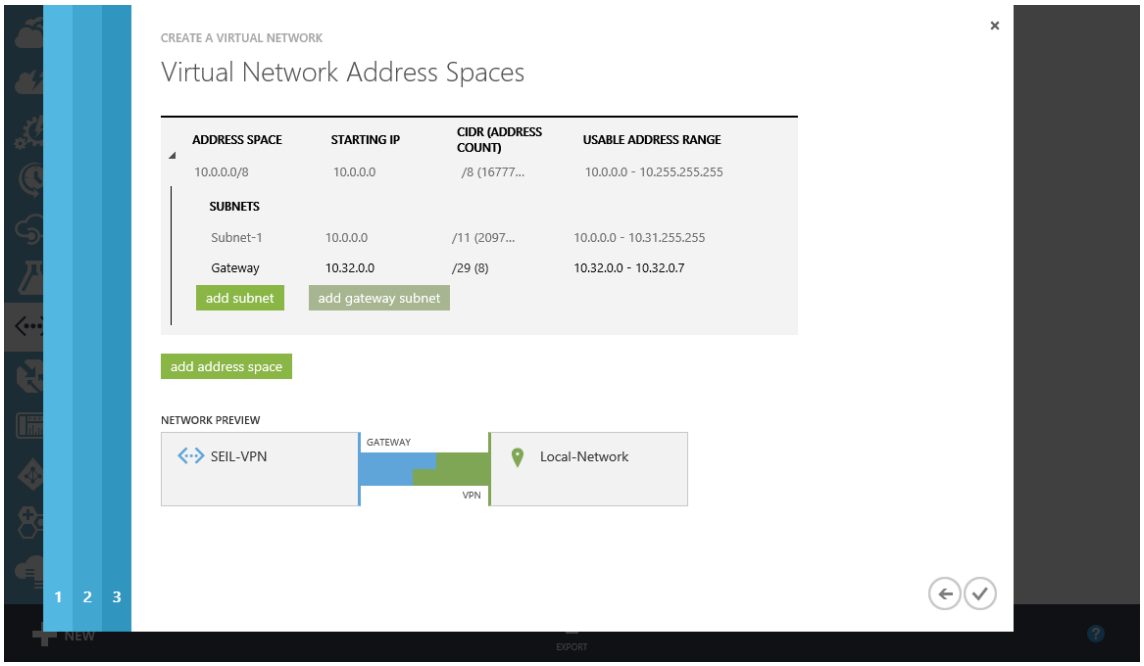

Figure 5

Click the “add gateway subnet” button.

6. Checking Created Virtual Network

Check to see whether the virtual network has been correctly created.

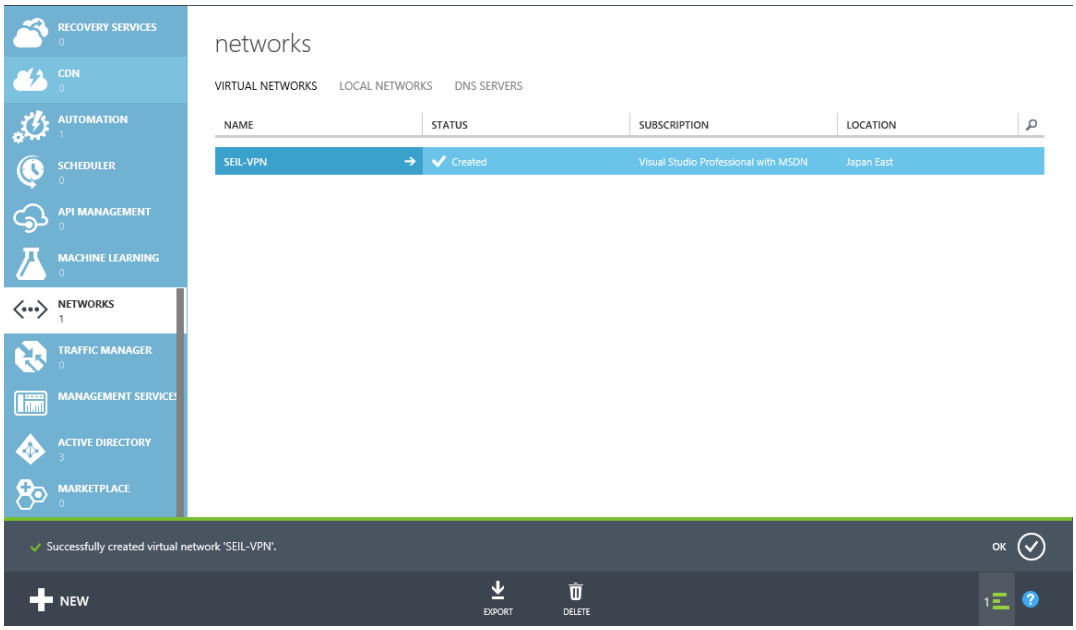

Figure 6

7. Obtaining Gateway IP Address

Open the added virtual network and obtain a Windows Azure gateway IP address.

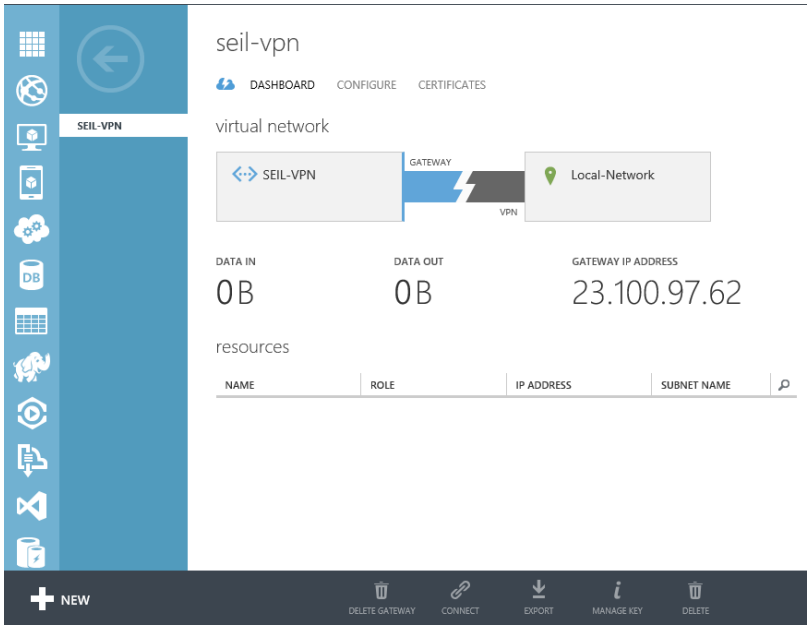

Figure 7

8. Obtaining Shared Key

Click “MANAGE KEY”, then obtain a shared key.

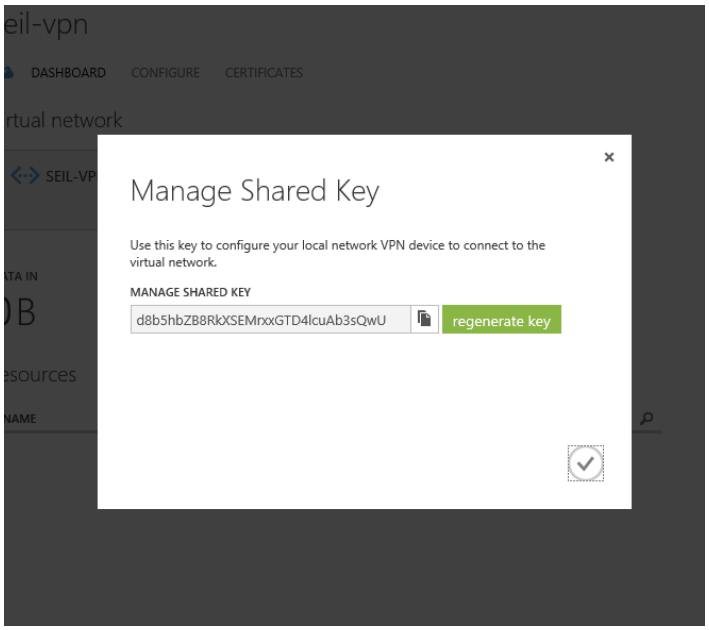

Figure 8

This completed Windows Azure setup. The following information covers SEIL setup procedures.

SEIL Setup

Log in and set up the SEIL using command shell. SEIL Series commands are not givin in detail on this document. Please contact "sales-seil@iij.ad.jp" for further details..

9. IKE Phase 1 Setup

```
ike preshared-key add "137.116.161.150" "fJ9hDVBf6sVar7bAZSYVSeFQKzAhjZVb"
ike proposal add Azure encryption aes256 hash sha1 authentication preshared-key dh-group modp1024 lifetime-of-time 08h
ike peer add Azure address 137.116.161.150 exchange-mode main proposals Azure nat-traversal enable responder-only on
```

- **ike preshared-key add**: Sets up a Windows Azure gateway IP address and shared key.
- **ike proposal add**: You need to set an encrypted algorithm or other such parameters to meet certain requests from Windows Azure. Complete set up as shown in the example.
- **ike peer add**: Sets up an access point for the Windows Azure gateway.

Note:

Set up a NAT Traversal regardless of whether the SEIL side is a NAT subordinate (turn "nat-traversal" enable).
Turn “responder-only” on so as to make Windows Azure the sole VPN connection initiator.

10. IKE Phase 2 Setup

```
ipsec security-association proposal add Azure authentication-algorithm hmac-sha1 encryption-algorithm aes256 lifetime-of-time 01h
ipsec security-association add Azure tunnel pppoe0 137.116.161.150 ike Azure esp enable
ipsec security-policy add Azure security-association Azure src 192.168.10.0/24 dst 10.0.0.0/8
```

- **ipsec security-association proposal add**: You may need to set an encrypted algorithm or other such parameters to meet certain requests from Windows Azure. Complete set up as shown in the example.
- **ipsec security-association add**: Sets the IPsec-SA to tunnel mode (tunnel), and sets a start and end point.

Note:

Set the start point as an interface set up for use in connecting SEIL to the internet (pppoe0 for example) or set a global IP address. Also make sure to set a security policy that requires use of a VPN between the SEIL private address space and the Windows Azure virtual network address space.

This completes VPN set up. Start a connection from the Windows Azure side to check operations.

Checking SEIL Operations

11. Checking IKE Phase 1 Status

Run "show status ike" command.

```
# show status ike
IKE server: up
IKE Phase1 Sessions:
        203.0.113.1 137.116.161.150
        Cookies: 0xd865b141:0x6866c068
        Status: established
        Side: responder
        Phase2 Negotiations: 1
        Created Time: 2013-04-03 20:10:33
        Lifetime: 28800
        Identity (local): 203.0.113.1/32 (AddressPrefix)
        Identity (remote): 137.116.161.150/32 (AddressPrefix)
```

Note:

The ISAKMP security association (IKE Phase1) may not be held even when connecting to a VPN, depending on the timing.

12. Checking IKE Phase 2 Status

Run "show status ipsec-security-association" command.

```
# show status ipsec security-association
203.0.113.1[500] 137.116.161.150[500]
    ESP tunnel spi=969121498(0x39C39EDA)
    Encap: AES256 0x89EFABBC2DCA4CE1BD588E8BF08651CE
    Auth: HMAC-SHA1 0x6A49A675E847AED0F76F4F5960EDF5EEFC828246
    State: mature
    Add Time: 2013-04-03 20:10:33
    Use Time: (not used)
    Use Packets: 0
    Use Bytes: 0
    Lifetime (soft/hard): 2880/3600
    Lifebyte (soft/hard): 1422707840/1778384896

137.116.161.150[500] 203.0.113.1[500]
    ESP tunnel spi=151131169(0x09021421)
    Encap: AES256 0x212F0CFA9A054C047486BE9A5053D46C
    Auth: HMAC-SHA1 0x4E487AE60F4F99D49F574CF360D640F429A60F8E
    State: mature
    Add Time: 2013-04-03 20:10:33
    Use Time: 2013-04-03 20:12:42
    Use Packets: 13
    Use Bytes: 416
    Lifetime (soft/hard): 2880/3600
    Lifebyte (soft/hard): 1422707840/1778384896
```

Note:

Holds at least 2 IPsec security associations (IKE Phase 2) for both sending and receiving data when connected to a VPN.
Depending on the update timing, more than 2 associations may be held.

Checking Windows Azure Operations

13. Checking Connection Status

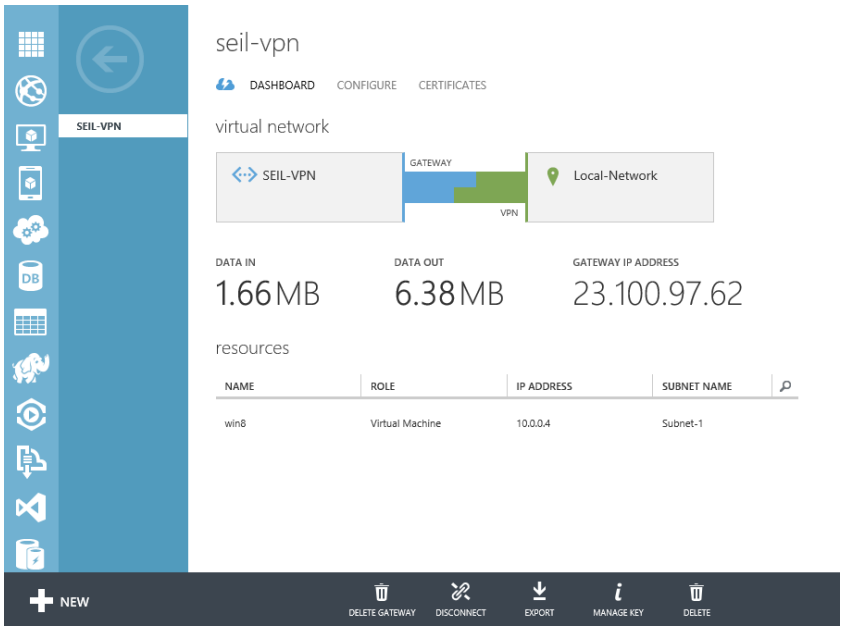

Figure 13

- **DATA IN/DATA OUT:** When data is sent to the virtual network, the sent/received data size in total is calculated.
- **resources:** By connecting a virtual machine to a virtual network, users can use remote desktops, etc., via a VPN.