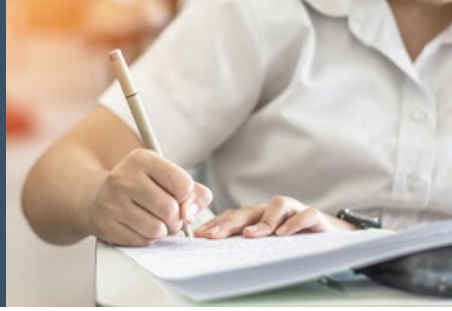
IBM Security Engineer
Study Guide



This study guide will help prepare you for the IBM **Security Engineer** Certification Examination.

What's in the Study Guide

This study guide covers:

- Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud

How to Use this Study Guide

1) **Read the content.**

2) **Take notes.**

3) **Answer practice questions.**

Preparation

Thorough study is essential to a successful outcome on the exam.

- Clear your schedule.
- Find a quiet place to study.
- Focus on the content.

- Open the associated on-line course for reference.
- Locate the Study Guide.
- Download the Study Guide.

- Print a copy of the Study Guide.
- Take notes.

Modules and Objectives

Modules

1. Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud

Objectives

- Articulate the security requirements for and implications of connecting to resources and services
- Configure VPN settings for a VPC
- Identify features and limitations of hardware firewall (Fortigate) in securing Classic resources
- Identify and assess the security ramifications of multi-region deployments
- Articulate how to connect on premise VMWare environments with IBM Cloud VMWare solutions
- Articulate how to connect using Juniper vSRX

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud

Introduction and Objectives

In Module 1 of the Study Guide the subject matter:

- Explains security requirements for connecting to VPC resources, VPN settings, hardware firewalls, multi-region deployments, connecting on premise VMWare environments with VMWare solutions in IBM Cloud, and Juniper vSRX.

Lessons

- Connecting Securely to Resources and Services
- VPN settings for a VPC
- Securing Classic Resources with a Hardware Firewall
- Multi-Region Deployments
- Connecting On Premise VMWare Environments with IBM Cloud VMWare solutions
- Juniper vSRX Connections
- Module Summary
- Knowledge Check Questions

Objectives

- Articulate the security requirements for and implications of connecting to resources and services
- Configure VPN settings for a VPC
- Identify features and limitations of hardware firewall (Fortigate) in securing Classic resources
- Identify and assess the security ramifications of multi-region deployments
- Articulate how to connect on premise VMWare environments with IBM Cloud VMWare solutions
- Articulate how to connect using Juniper vSRX

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud
Security Group Guidelines

Security Groups Guidelines
Consider the following guidelines when working with IBM™ Cloud Security Groups.

Rules
- Each security group defines different sets of network rules that define the incoming and outgoing traffic for a virtual server instance. You can specify rules for both IPv4 and IPv6.
- When a new security group is created by using the IBM Cloud console, the default behavior is to create a single rule that allows all outbound traffic from the virtual server instance. You must clear the "Create group with a default rule to allow all outbound traffic" check box to create the security group with no rules. A security group with no rules blocks all traffic (both inbound and outbound).
- To allow inbound traffic, outbound traffic, or both, you must add at least one security group that includes security group rules that allow traffic.
- Security group rules only can be permissive. Traffic is blocked by default.
- Users with the Manage Security Groups privilege can add, edit, or delete rules in a security group.
- Changes to security group rules are automatically applied and can be modified at any time.
- The order of rules within a security group does not matter. The priority always falls to the least restrictive rule.
- Rules are stateful. Connections established prior to a security group change are not altered. New connections abide by rules that exist at the time connectivity is established.
- Security groups do not override operating system firewalls on the virtual server. Even if a more restrictive firewall exists on the operating system than what is applied by the security group, the operating system rules will still be enforced.
- If your virtual server needs access to internal services, such as an update server, network attached storage (NAS), or advanced monitoring, ensure that the security group rules accommodate traffic for those internal services.

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud
Security Group Guidelines

Security Groups Guidelines Cont'd

Consider the following guidelines when working with IBM™ Cloud Security Groups.

Interfaces

- A security group can be applied to a private network, a public network, or both network interface types.
- You can attach one or more security groups to the list of security groups that are assigned to a network interface. The security group rules of each security group apply to the associated virtual server instances.
- The first time that you assign an existing security group to a network interface (public or private), a restart is required for each interface. However, if the public and private interfaces were assigned to the security group at the same time, then only one restart is required. After a restart, changes are automatically applied.

Access

- All users within an account can read, attach, and detach security groups on the virtual server instances to which they have access. Only users with the Manage Security Groups privilege in Network Permissions can create, update and delete security groups.
- You cannot assign security groups to bare metal servers.

Deletion

- You cannot delete a security group that is assigned to one or more running virtual server instances.
- You cannot delete a security group that another security group is referencing in one of its rules.

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud

Working with ACLs and ACL rules

Working With ACLs And ACL Rules

You can use an access control list (ACL) to control all incoming and outgoing traffic in IBM Cloud® Virtual Private Cloud. An ACL is a built-in, virtual firewall, similar to a security group. In contrast to security groups, ACL rules control traffic to and from the *subnets*, rather than to and from the *instances*.

To make your ACLs effective, create rules that determine how to handle your inbound and outbound network traffic. You can create multiple inbound and outbound rules.
With inbound rules, you can allow or deny traffic from a source IP range, with specified protocols and ports.

- With outbound rules, you can allow or deny traffic to a destination IP range, with specified protocols and ports.
- ACL rules are prioritized and considered in sequence. Higher priority rules are evaluated first and override lower priority rules.
- Inbound rules are separated from outbound rules.
- If no rules are specified, then **implicit deny** is the default behavior.

Attaching an ACL to a subnet

You can attach an ACL to a subnet two different ways:

- You can create a new subnet, and specify an ACL to attach. If you don't specify an ACL, a default network ACL is attached. The default ACL allows all inbound traffic to this subnet, and all outbound traffic from this subnet.
- You can attach an ACL to an existing subnet. If another ACL is attached to this subnet already, that ACL is detached before the new ACL is attached.

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud

Setting up an IPsec VPN connection

Setting Up An Ipsec VPN Connection

What is IPsec VPN?

IPsec is a suite of protocols that are designed to authenticate and encrypt all IP traffic between two locations. It allows trusted data to pass through networks, which otherwise would be considered insecure. IPsec tunnel endpoints can be located anywhere and still provide access to your entire private network, or the networks you specify. IPsec tunnels are incompatible if you are using a zone, or cloud service endpoints.
IBM Cloud VPN access allows users to manage all servers remotely and securely over the IBM Cloud Private network. A VPN connection from your location to the private network gives you the capability for out-of-band management and server rescue through an encrypted VPN tunnel. With VPN access, you can:

- Establish a VPN connection to the private network through SSL or IPsec.
- Access your server by using its private 10.x.x.x IP address through SSH or RDP.
- Connect to your server's IPMI IP address for additional server management or rescue needs.

We provide the IPsec service to customers for management of their environments. It is not recommended for production workloads.

Negotiation parameters

You need to know the following information for the remote side of the IPsec VPN:

- Static IP address for VPN endpoint
- Preshared key (Password)
- Encryption algorithm (DES, 3DES, AES128, AES192, AES256)
- Authentication (MD5, SHA1, SHA256, for phase 1&2)
- Diffie-Hellman Group (for phase 1&2)
- Is Perfect Forward Secrecy (PFS) used?
- Key life time (for phase 1 & 2)
- After you have this information available, you can configure the basic negotiation parameters of the VPN connection.

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud

Setting up an IPsec VPN connection

Setting Up An Ipsec VPN Connection Cont'd

Protected networks

In the VPN connection properties, you must define the networks on the remote end of the tunnel and the local networks for the tunnel. In the “Protected Customer (Remote) Subnet”, enter the private IP address space in CIDR notation for the remote (Non-IBM) end of the IPsec tunnel.
For example, if your network on the remote end of the tunnel uses a single subnet 10.0.0.0 with a netmask of 255.255.255.0, you would enter IP address 10.0.0.0 / CIDR 24 for the “Protected Customer (Remote) Subnet” section.

Network Address Translation (NAT)

With the IPsec VPN, you also are allowed to define private IP addresses on the IBM Cloud network that will route traffic to remote subnets on the other end of the VPN connection. This allows you to have private internet traffic that is forwarded to one of your internal IP addresses of a system behind your VPN, without exposing the remote location to full internet access.

Network Address Translation/assigned static NAT subnets

To configure a remote VPN IP with a static NAT entry:

- Select the red arrow to display the subnet list in the **Assigned Static NAT subnets** section. Each IP in the subnet is displayed.
- Enter the IP on the remote end of the VPN connection under the **Customer IP** column and enter a name for the mapping under the **Name** column.
- Select the **Add/Modify Context Address Translations** and **Apply Configurations** to save and apply the configuration.

This action sets up a static one-to-one network translation for the return traffic, which is used by your hosts behind the IBM Cloud VPN concentrator to communicate with the hosts behind the remote VPN peer. For example, all traffic for IP 10.1.255.92 will be translated and forwarded to the customer's IP 192.168.10.15. This forwarding eliminates the need for more route entries on the IBM Cloud server.

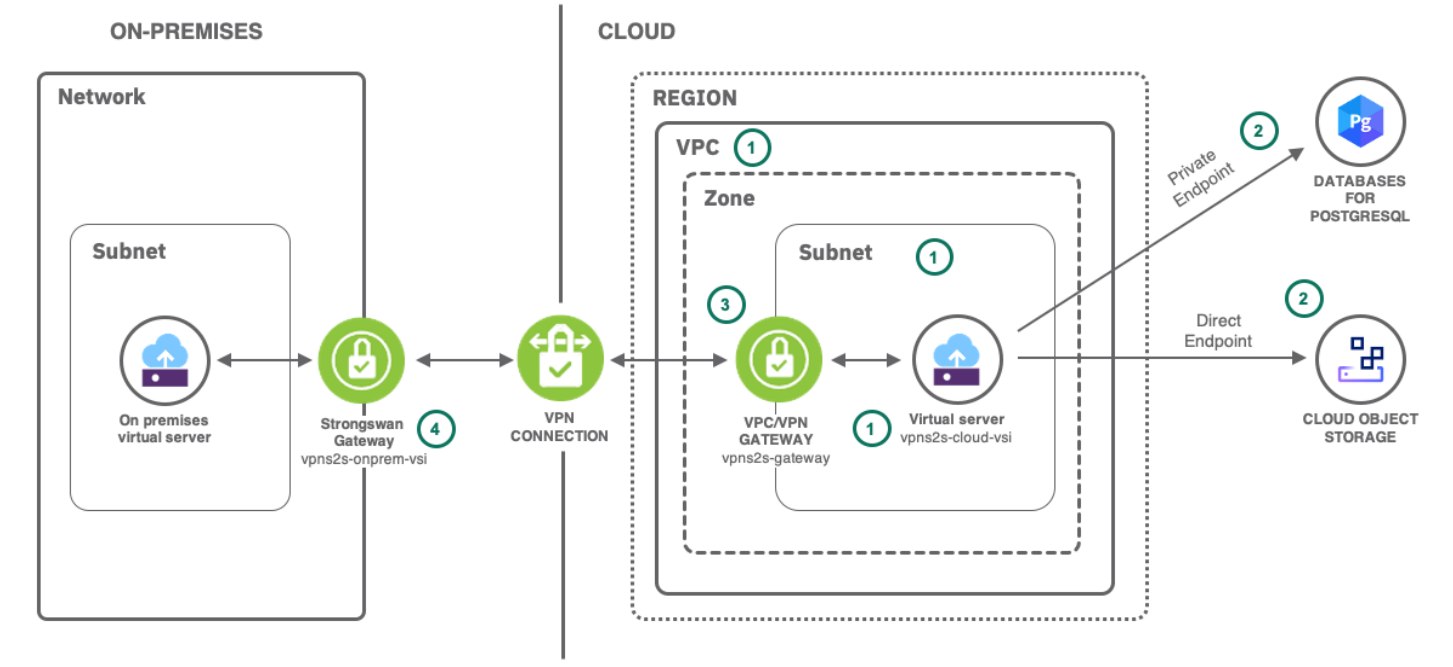
Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud
Use a VPC/VPN gateway for secure and private on-premises access to cloud resources

Use A VPC/VPN Gateway For Secure And Private On-premises Access To Cloud Resources

IBM offers a number of ways to securely extend an on-premises computer network with resources in the IBM Cloud. This allows you to benefit from the elasticity of provisioning servers when you need them and removing them when no longer required. Moreover, you can easily and securely connect your on-premises capabilities to the IBM Cloud services. There are many popular on-premises VPN solutions for site-to-site gateways available. In short, using a VPC you can

- connect your on-premises systems to services and workloads running in IBM Cloud,
- ensure private and low cost connectivity to IBM Cloud services,
- connect your cloud-based systems to services and workloads running on-premises.

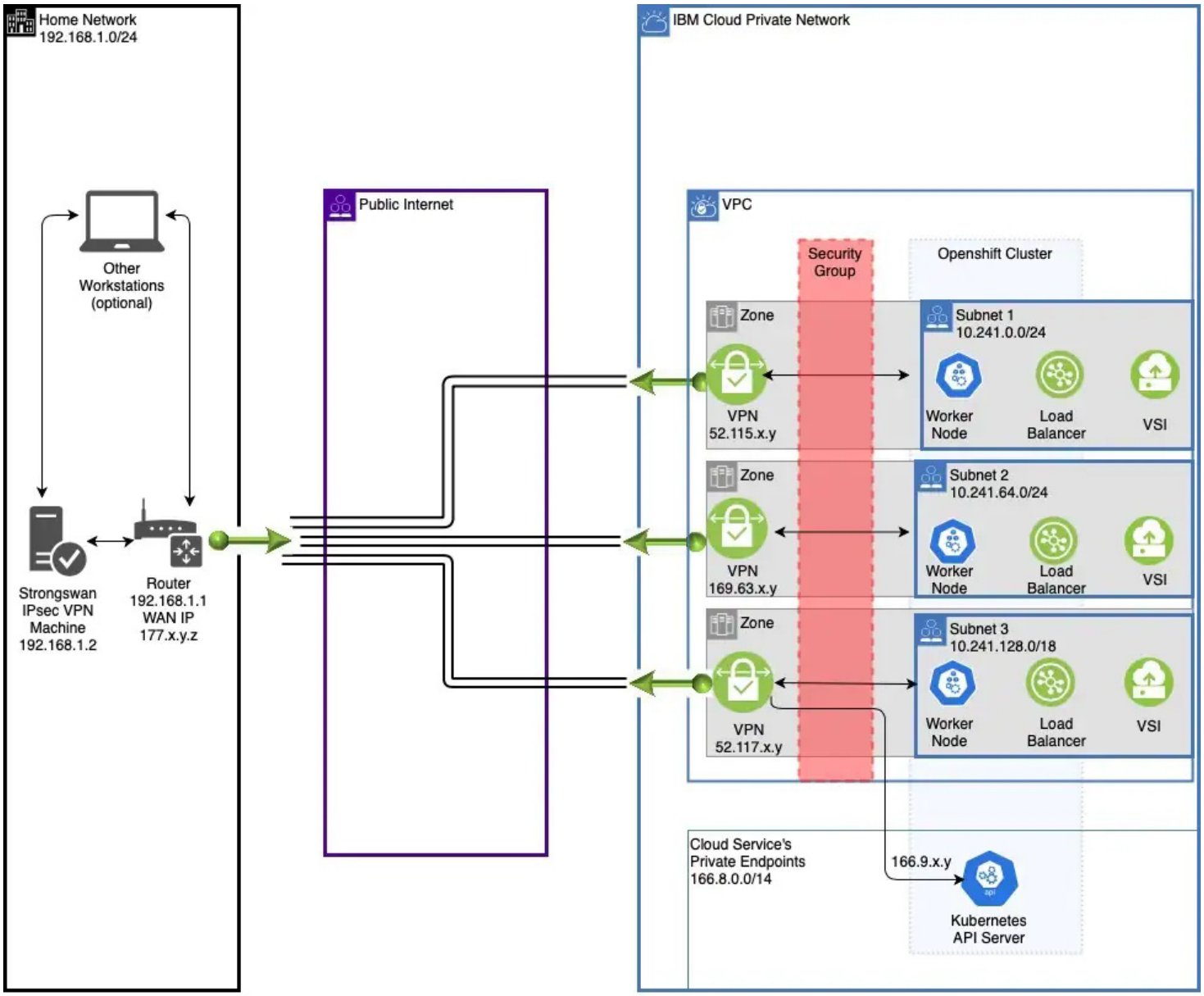
The following diagram shows the virtual private cloud containing an app server. The app server hosts a microservice interfacing with IBM Cloud services. A (simulated) on-premises network and the virtual cloud environment are connected via VPN gateways.



Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud
Setting Up a VPN Between IBM Cloud VPC and Your Home Office

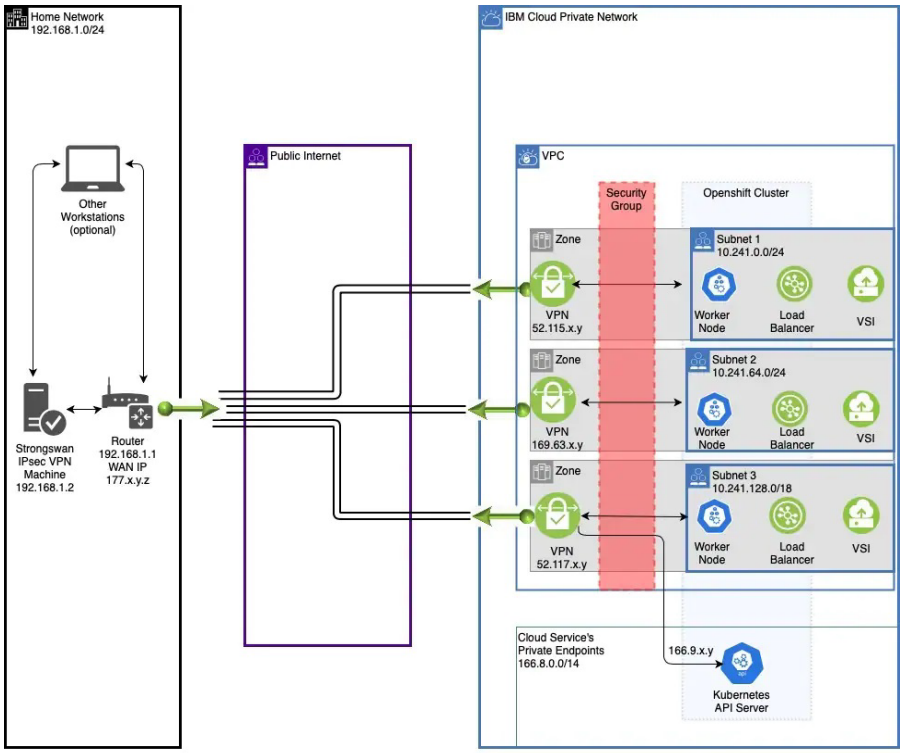
Setting Up a VPN Between IBM Cloud VPC and Your Home Office Overview

A VPC gives an enterprise the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private and secure place on the public cloud.



Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud
Setting Up a VPN Between IBM Cloud VPC and Your Home Office

Setting Up a VPN Between IBM Cloud VPC and Your Home Office Overview Cont'd



Home network (the left side)

Prerequisites:

Before you begin, you will need access to your home router.

1. Typically, in a home network, machines are assigned IP addresses via DHCP by the router. However, we don't want the machine running the VPN's IP address to change because that IP address is part of the configuration. Use the home router settings to give the machine a static IP address of 192.168.1.2.
2. Obtain the WAN IP address of your home router. This IP address can usually be found in the WAN section of the router settings. This IP address is typically assigned dynamically by your internet service provider.

IBM Cloud VPC network (the right side)

Prerequisites:

- IBM Cloud VPC
- VPC subnets
- A Kubernetes or OpenShift cluster in the VPC
- Your home network CIDR, which you typically find in the configuration settings of your home router

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud
Exploring Firewalls

Exploring Firewalls

IBM Cloud® offers several firewalls to choose from. The following table compares the firewall solutions to help you choose the one that's right for you.

	Security Groups (VSI only)	IBM Cloud Juniper vSRX Standard	Virtual Router Appliance	FortiGate Security Applicance 10 Gbps	FortiGate Security Appliance 1 Gbps	Hardware Firewall	Cloud Internet Services
Stateful Packet Inspection	X	x	x	x	x	x	IP firewall only
Public Network Protection	X	x	x	x	x	x	x
Private Network Protection	X	x	x	x			
Ingress Rules	X	x	x	x	x	x	IP Firewall only
Egress Rules	X	x	x	x	x		
Single Tenant Appliance		x	x	x	x		
VLAN Protection		x	x	x	x		
Multi-VLAN Support		x	x	x			
NAT Support		x	x	x	x		
SSL/IPsec VPN Termination		x	x	x	x		
Open VPN Termination			x				Only with single port on TCP/UDP
High Availability (HA) Option	N/A	x	x	x	x	Using range and load balancers	
Manage from API & Portal	Yes	Appliance GUI	Appliance GUI	Appliance GUI	Appliance GUI	Yes	Yes
10 Gbps Support	N/A	x	x	x			
NGFW Add-ons (IPS, AV, WF)		x		x	x		TLS encryption, IP Firewall rules, and Proxy Protocol v1

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud
IBM Cloud Transit Gateway

IBM Cloud Transit Gateway

IBM Cloud Transit Gateway enables you to connect IBM Cloud VPCs and classic infrastructure to transit gateways, allowing you to build global networks of multiple VPCs and classic infrastructure resources across IBM Cloud regions to keep up with your business needs. IBM Cloud Transit Gateway works across IBM Cloud VPCs as well as IBM classic networks.

Here are some ways that you can implement the IBM Cloud Transit Gateway service:

- Use case 1: Interconnect two or more VPCs in the same Multi-Zone Region (MZR)
  - Connect two VPCs in the same region with a local transit gateway.
- Use case 2: Interconnect two or more VPCs across multiple MZRs
  - Connect VPCs in multiple regions using a global transit gateway.
- Use case 3: Interconnect one or more VPCs in the same MZR and an IBM classic network
  - Connect VPCs in the same region with IBM Cloud classic through a local transit gateway.
- Use case 4: Interconnect VPCs and an IBM classic network to access all your resources across all MZRs
  - Connect VPCs from multiple regions with IBM Cloud classic through a global transit gateway.
- Use case 5: Interconnect VPCs across accounts
  - Connect VPCs in the same region owned by different IBM Cloud accounts through a local transit gateway.
- Use case 6: Connect networks (VPC and classic) to multiple local gateways
  - It keeps your local traffic on a local transit gateway, which reduces latency.
  - Classic infrastructure transit gateway connections are required to be in the same account as the transit gateway owner.
- Use case 7: Interconnect networks (VPC and classic) across accounts
  - Connect cross-account IBM Cloud classic accounts to one or more transit gateways.

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud
VMware HCX

VMware HCX Overview

The VMware HCX™ service extends the networks of on-premises data centers into IBM Cloud®, and it helps you migrate virtual machines (VMs) to and from the IBM Cloud without any conversion or change. HCX creates an abstraction layer that enables application mobility and infrastructure hybridity through securely stretched networks. You can modernize your VMware® environment from VMware vSphere® 5.1 to the most recent vSphere version without needing to refactor or modify your existing application, as HCX enables this seamless transformation. With HCX, you can bring your IP subnet ranges into IBM Cloud ensuring the IP consistency through a hybrid deployment and by providing high-level security with end-to-end Suite B encryptions.

A VMware vCenter Server® instance with HCX is limited to three simultaneous connections from on-premises sites.

- For vCenter Server with NSX-T™ instances, HCX is supported for NSX-T 3.1 or later and for VMware vSphere 7.0.
- For vCenter Server with NSX-V instances, HCX is supported for vSphere 6.7.

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud
NSX Edge Services Gateway Design

NSX Edge Services Gateway Design

The NSX Edge Services Gateway on IBM Cloud® solution provides VMware® technology that is deployed within IBM Cloud data centers across the globe.

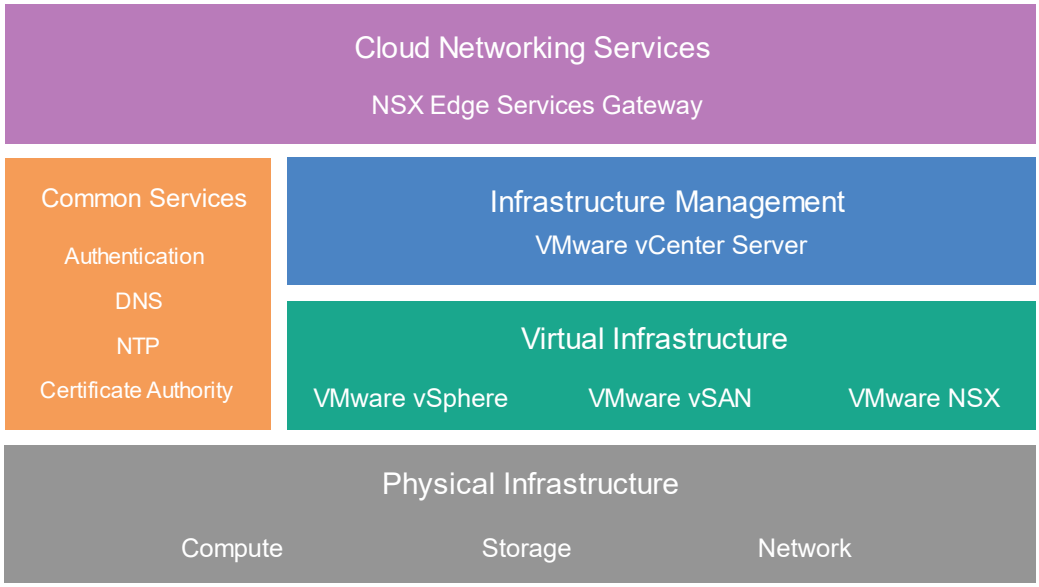
Internal architecture design

The internal architecture specifies the deployment of the necessary NSX Edge components in a resource pool in a VMware vCenter Server® cluster.

Dedicated architecture design

The dedicated architecture deploys the necessary NSX Edge components in a separate two-node vSphere cluster. This cluster is dedicated for the use of the NSX Edge and provides critical interaction with the physical network infrastructure. The dedicated architecture has the following characteristics and functions:

- Provides on-ramp and off-ramp connectivity to physical networks.
- Allows for communication with physical devices that are connected to VLANs in the physical networks through NSX L2 bridging and hosts the control virtual machine (VM) for Distributed Logical Router (DLR) routing.
- Can have centralized logical or physical services.
- NSX Controllers can be hosted in an edge services cluster when a dedicated vCenter is used to manage the compute and edge resources.
- Edge services cluster resources have an anti-affinity requirement to protect the active standby configuration or to maintain the bandwidth availability during failure.



Note: VMware vSAN™ is optional in the above figure.

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud Summary

Module Summary

- IBM Cloud security groups allow management of ingress and egress traffic.
- IBM Cloud Virtual Private Endpoints (VPEs) allow for Virtual Private Cloud (VPCs) connections which allow for a variety of services.
- Access Control Lists central all traffic to and from a VPC and its subnets, with its default setting in the console to allow outbound from the subnets.
- IPsec protocols create tunnels that are used to authenticate and encrypt traffic between two locations. These networks must be defined along with the local networks in the tunnel.
- Virtual Private Networks (VPNs) are one way to extend your on-premise resources. You can connect to the cloud through a VPC which allows you to use cloud services as well.
- There are limitations to VPN gateways that Cloud Security Engineers need to be aware of.
- FortiGate 10 GB is a hardware firewall service available for securing client assets.
- These firewalls reside in Virtual Local Area Network (VLANs). These are protected by the Frontend Customer Router (FCR) where the client's resources reside.
- Juniper vSRX is a virtual firewall that should be part of a CSE's consideration where firewalls are needed.
- Virtual Private Clouds have grown tremendously, and the easiest way to manage them is through the use of Cloud Transit Gateways.
- IBM Cloud Internet Services (CIS) has built-in settings for managing security in multi-regional deployments. These settings should be configured to the client's needs, as they are not customized.
- VMware NSX Edge Service Gateway (ESG) is a current offering from IBM that connects isolated networks to common gateway connections, allowing for the modernization of classic infrastructure to hybrid networks.
- Utilizing the VMware HCX service provides for a seamless transition of environments without needing to modify or refactor existing applications.

Module 1
Check Your Knowledge

Question 1.

A Security Engineer is contacted by a developer who needs a virtual server instance (VSI) that is only allowed to send outbound traffic; all ingress traffic should be blocked. The Security Engineer decides to use the IBM Cloud console to create security rules on VSI groups. Which additional modifications are required on this new security group to meet the stated requirements?

A. Add a rule to permit all egress traffic
B. No additional modifications are required
C. Apply the security group to the Public Gateway
D. Remove the default rule allowing all ingress traffic

➞ Answer B. No additional modifications are required

Module 1
Check Your Knowledge

Question 2.

What type of information is required for an IPsec policy creation on an IBM Cloud VPC?

A. Encryption algorithm, IBM Cloud service endpoints, and Preshared key
B. Authentication algorithm, IKE Version, Key Lifetime, and Delegate-VPC
C. Authorization algorithm, IKE Version, Delegate-VPC, and Preshared key
D. Authentication algorithm, Encryption algorithm, Diffie-Hellman group, and Key Lifetime

Answer D. Authentication algorithm, Encryption algorithm, Diffie-Hellman group, and Key Lifetime

Module 1
Check Your Knowledge

Question 3.

True or False: Security Groups apply at the VPC subnet level.

A. True
B. False

Answer B. ACLs apply at subnet, Security Groups apply to VSI instances

Module 1
Check Your Knowledge

Question 4.

A client wants to move their existing workloads to IBM Cloud VMware solutions, Bare Metal, Power servers and KVM. What is the value for client using VMware vSphere 7.0 and NSX-T on IBM Cloud?

A. Client can route traffic between VMware ESX, Bare Metal, PowerVS, and KVM servers using NSX-T
B. Client can route traffic between VMware ESX, Bare Metal, and KVM servers using NSX-T
C. Client can create Tier 0/1 gateway allowing traffic to flow between VMware servers
D. VMware solutions offer comprehensive migration capability for other workloads

Answer A. Client can route traffic between VMware ESX, Bare Metal, PowerVS, and KVM servers using NSX-T

Module 1
Check Your Knowledge

Question 5.

What can you do using a VPC? Select all that apply.

A. Connect your on-premises systems to services and workloads running in IBM Cloud,
B. Ensure private and low cost connectivity to IBM Cloud services,
C. Connect your cloud-based systems to services and workloads running on-premises.
D. Run a Juniper status check

Answer A,B, and C VPC allows you to connect your on-premises systems to services and workloads running in IBM Cloud, ensure private and low cost connectivity to IBM Cloud services, connect your cloud-based systems to services and workloads running on-premises.

Module 1
Check Your Knowledge

Question 6.

Which firewall has an HA (High Availability) option? Select all that apply.

A. Juniper vSRX Standard
B. FortiGate Security Applicance 10 Gbps
C. Virtual Router Appliance
D. Cloud Internet Services

Answer A,B, and C. Juniper vSRX Standard, FortiGate Security Applicance 10 Gbps, and Virtual Router Appliance.

Module 1
Check Your Knowledge

Question 7.

What are some ways that you can implement the IBM Cloud Transit Gateway service? Select all that apply.

A. Connect VPCs with Juniper vSRX Standard
B. Interconnect two or more VPCs in the same MZR
C. Interconnect two or more VPCs across multiple MZRs
D. Connect VPCs with Kubernetes

Answer B and C. Interconnect two or more VPCs in the same MZR and interconnect two or more VPCs across multiple MZRs

Module 1
Check Your Knowledge

Question 8.

A VMware vCenter Server instance with HCX is limited to how many simultaneous connections from on-premises sites?

A. One
B. Two
C. Five
D. Three

Answer D. A VMware vCenter Server® instance with HCX is limited to three simultaneous connections from on-premises sites.

Module 1
Check Your Knowledge

Question 9.

Which gateway design has an anti-affinity requirement to protect the active standby configuration or to maintain the bandwidth availability during failure?

A. VMware HCX
B. NSX Edge Services
C. Kubernetes
D. Satellite

Answer B. NSX Edge Services Gateway design provides on-ramp and off-ramp connectivity to physical networks.

Module 1
Check Your Knowledge

Question 10.

Fill in the blank: With the IPsec VPN, you are allowed to define _____ IP addresses on the IBM Cloud network that will route traffic to remote subnets on the other end of the VPN connection.

A. Satellite
B. Cloud
C. Private
D. Public

Answer C. With the IPsec VPN, you are allowed to define private IP addresses on the IBM Cloud network that will route traffic to remote subnets on the other end of the VPN connection.