

# Networking



## Networking Implementation

### 1.8.2 - Cloud Connectivity Options

**What are different connectivity options for the cloud?**

#### **Overview**

The student will summarize cloud concepts and connectivity options

#### **Grade Level(s)**

10, 11, 12

#### **Cyber Connections**

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

*This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).*

## Teacher Notes:

# CompTIA N10-008 Network+ Objectives

## Objective 1.8

- Summarize cloud concepts and connectivity options
  - Connectivity options
    - Virtual private network (VPN)
    - Private-direct connection to cloud provider
  - Multitenancy
  - Elasticity
  - Scalability
  - Security implications

---

## Cloud Connectivity Options

### Connectivity Options

By default, traffic in and out of our public cloud traverses the Internet. If we require additional security features when accessing cloud resources and exchanging data, we have a couple of options.

The first, a *virtual private network (VPN)*, sends data securely over the Internet. Most cloud providers offer site-to-site VPN options allowing us to establish a secure and protected network connection across the public Internet. This connection verifies both ends of the connection are legitimate and the establishes encrypted tunnels to route traffic from our data center to our cloud resources.

The second option is installing a private non-Internet connection and then configuring a direct connection. This *private-direct connection* is a dedicated circuit installed between our data center and an interconnection provider or directly to the cloud provider. Because of this, we have a secure, low latency connection with predictable performance. Direct connection speeds typically range from 1 Gbps to 10 Gbps, but we can aggregate them together to provide a larger total aggregate bandwidth.

We have a few options for connecting to a virtual server in a cloud environment: remote desktop, FTP and SFTP, and VMware remote console to name a few.

## Teacher Notes:

### Multitenancy, Elasticity, and Scalability

In cloud computing, *multitenancy* means that multiple customers of a cloud vendor are using the same computing resources. The classic definition of multitenancy was a single software instance serving multiple users or tenants. This term has taken a broader meaning with cloud computing. Even though resources are being shared, cloud customers are not aware of each other and their data is kept separate. Multitenancy is essential for cloud computing because without it, cloud services like IaaS, PaaS, and SaaS would be far less practical.

A cloud-based infrastructure has the ability to change and move whenever the conditions require it. *Elasticity* is one where you would add new resources as they are needed and remove them when they are not needed. Host availability allows you to implement this elasticity with the click of a button. *Scalability* is the ability to easily add or subtract compute or storage resources. In 'the old days' of on-premises data centers, scalability was incredibly costly, slow, and difficult to manage. Back then, scaling up meant buying new server hardware and disk arrays. With the cloud, another click of a button allows you to scale up or down as needed.

### Security is Implied

For the Network+ exam, there are some specific security implications that need to be recognized when it comes to the cloud. These include:

- Technicians falling victim to phishing attacks like that of salesforce.com that compromised customer passwords
- Customers failing to ensure the provider keeps their data safe in multitenant environments
- No specific standard has been developed to address a specific issue
- Data security varies greatly from country to country. Customers don't know where their data is located at any point in time