FIREWALL PDF-FALGUNI MAM

VPN

VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in **real time**.

**How does a VPN work?**

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

**What are the benefits of a VPN connection?**

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.

**Secure encryption:** To read the data, you need an *encryption key* . Without one, it would take millions of years for a computer to decipher the code in the event of a [brute force attack](https://www.kaspersky.com/resource-center/definitions/brute-force-attack) . With the help of a VPN, your online activities are hidden even on public networks.

**Disguising your whereabouts** : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.

**Access to regional content:** Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With **VPN location spoofing** , you can switch to a server to another country and effectively “change” your location.

**Secure data transfer:** If you work remotely, you may need to access important files on your company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

**Why should you use a VPN connection?**

Your ISP usually sets up your connection when you connect to the internet. It tracks you via an IP address. Your network traffic is routed through your ISP's servers, which can log and display everything you do online.

Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.

This is especially important if you regularly connect to public Wi-Fi networks. You never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity.

**What should a good VPN do?**

You should rely on your VPN to perform one or more tasks. The VPN itself should also be protected against compromise. These are the features you should expect from a comprehensive VPN solution:

* **Encryption of your IP address:** The primary job of a VPN is to hide your IP address from your ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.
* **Encryption of protocols:** A VPN should also prevent you from leaving traces, for example, in the form of your internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.
* **Kill switch:** If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.
* **Two-factor authentication:** By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

**What is high performance computing?**

High performance computing (HPC) is the practice of aggregating computing resources to gain performance greater than that of a single workstation, server, or computer. HPC can take the form of custom-built supercomputers or groups of individual computers called clusters. HPC can be run on-premises, in the cloud, or as a hybrid of both. Each computer in a cluster is often called a node, with each node responsible for a different task. Controller nodes run essential services and coordinate work between nodes, interactive nodes or login nodes act as the hosts that users log in to, either by graphical user interface or command line, and compute or worker nodes execute the computations. Algorithms and software are run in parallel on each node of the cluster to help perform its given task. HPC typically has three main components: compute, storage, and networking.

HPC allows companies and researchers to aggregate computing resources to solve problems that are either too large for standard computers to handle individually or would take too long to process. For this reason, it is also sometimes referred to as supercomputing.

HPC is used to solve problems in academic research, science, design, simulation, and business intelligence. HPC’s ability to quickly process massive amounts of data powers some of the most fundamental aspects of today’s society, such as the capability for banks to verify fraud on millions of credit card transactions at once, for automakers to test your car’s design for crash safety, or to know what the weather is going to be like tomorrow.

Types of HPC clusters

High performance computing has three main components:

* Compute
* Network
* Storage

In basic terms, the nodes (compute) of the HPC system are connected to other nodes to run algorithms and software simultaneously, and are then connected (network) with data servers (storage) to capture the output. As HPC projects tend to be large and complex, the nodes of the system usually have to exchange the results of their computation with each other, which means they need fast disks, high-speed memory, and low-latency, high-bandwidth networking between the nodes and storage systems.

HPC can typically be broken down into two general design types: cluster computing and distributed computing.

Cluster computing

Parallel computing is done with a collection of computers (clusters) working together, such as a connected group of servers placed closely to one another both physically and in network topology, to minimize the latency between nodes.

Distributed computing

The distributed computing model connects the computing power of multiple computers in a network that is either in a single location (often on-premises) or distributed across several locations, which may include on-premises hardware and cloud resources.

In addition, HPC clusters can be distinguished between homogeneous vs heterogeneous hardware models. In homogenous clusters, all machines have similar performance and configuration, and are often treated as the same and interchangeable. In heterogeneous clusters, there is a collection of hardware with different characteristics (high CPU core-count, GPU-accelerated, and more), and the system is best utilized when nodes are assigned tasks to best leverage their distinct advantages.

How do HPC jobs work?

Workloads in an HPC environment typically come in two different types: loosely coupled and tightly coupled.

Loosely coupled workloads (often called parallel or high throughput jobs) consist of independent tasks that can be run at the same time across the system. The tasks may share common storage, but they are not context-dependent and thus do not need to communicate results with each other as they are completed. An example of a loosely coupled workload would be rendering Computer Generated Imagery (CGI) in a feature film, where each frame of the video is rendered independently of the other frames, despite them sharing the same input data like backgrounds and 3D models.

Tightly coupled workloads consist of many small processes, each handled by different nodes in a cluster, which are dependent on each other to complete the overall task. Tightly coupled workloads usually require low-latency networking between nodes and fast access to shared memory and storage. Interprocess communication for these workloads is handled by a Message Passing Interface (MPI), using software such as OpenMPI and Intel MPI. An example of a tightly coupled workload would be weather forecasting, which involves physics-based simulation of dynamic and interdependent systems involving temperature, wind, pressure, precipitation, and more. Here, each cluster node may compute partial solutions to different weather factors, contributing to the overall forecast.

HPC in the cloud

HPC can be performed on-premises with dedicated equipment, in the cloud, or a hybrid of each.

HPC in the cloud offers the benefit of flexibility and scalability without having to purchase and maintain expensive dedicated supercomputers. HPC in the cloud provides all the necessary infrastructure needed to perform large, complex tasks such as data storage, networking solutions, specialized compute resources, security, and artificial intelligence applications. Workloads can be performed on demand, which means that organizations can save money on equipment and time on computing cycles, only using the resources they need, when they need them.

Some common considerations when choosing to run HPC in the cloud include:

**Latency and bandwidth:**With the amount of data running in HPC workloads, cloud providers need to provide robust networking capabilities (>100 GB/s) with low latency.

**Performance:** HPC in the cloud works best with providers that constantly update systems to optimize performance, especially in computer processors, storage solutions, and networking capabilities.

**Sustainability:** HPC is a resource intensive form of computing, requiring much more electricity than normal workloads. On-premises high performance computers can cost millions of dollars a year in energy. [Public clouds](https://cloud.google.com/learn/what-is-public-cloud) that prioritize renewable energy—[such as Google Cloud](https://cloud.google.com/sustainability)—can mitigate the energy impacts of HPC.

**Storage:** Given the size of most HPC tasks, scalable data storage is an important consideration when running HPC workloads. Cloud providers that can easily store and manage large amounts of data (such as through Cloud Storage [Filestore High Scale](https://cloud.google.com/filestore/docs/service-tiers" \l "high_scale_ssd_tier" \t "_blank), or [DDN EXAScaler](https://console.cloud.google.com/marketplace/details/ddnstorage/exascaler-cloud?pli=1)) have an advantage in HPC.

**Security:**A cloud provider with a privately managed global infrastructure ensures that data and applications are the least exposed to the public internet. Virtual private cloud (VPC) networks enable connectivity between nodes and can configure firewalls for HPC applications. [Confidential Computing](https://cloud.google.com/confidential-computing) features allow encryption in use, as well as encryption at rest and in flight.

Benefits of HPC in the cloud

**Speed and performance**

High performance computing can process data and tasks much faster than a single server or computer. Tasks that could take weeks or months on a regular computing system can take hours in HPC.

**Flexibility and efficiency**

With HPC in the cloud, workloads can be scaled up or down depending on need. With a robust internet connection, HPC can be accessed from anywhere on the globe.

**Cost savings**

Because of the speed, flexibility, and efficiency of HPC in the cloud, organizations can save time and money on computing resources and labor hours.

**Fault tolerance**

If one node of an HPC cluster fails, the system is resilient enough that the rest of the system does not come crashing down. Given the large and complex tasks performed by HPC, fault tolerance is a big advantage.

**Accelerated R&D**

HPC provides an advantage to companies performing research and development by speeding up the results of data-intensive projects, such as pharmaceutical modeling, designing new machines and parts, or simulating experiments to reduce physical testing.

**Initial cost**

On-premises HPC clusters and supercomputers have high initial costs. On-premises HPC would be out of reach for most organizations after factoring in the cost of equipment, labor, software, and configuration.

**Energy consumption**

The energy costs of on-premises supercomputer installations can be large. For environmentally and cost conscious companies, HPC energy consumption can be sustainable by running HPC [on the world’s cleanest cloud](https://cloud.google.com/sustainability).

**Maintenance**

HPC runs best when on the latest generation of hardware and optimized software. Keeping an on-premises HPC cluster or supercomputer up to date to ensure optimal performance can quickly become a large and ongoing expense.

**Cloud Computing** and **Grid Computing** are two model in distributed computing. They are used for different purposes and have different architectures. Cloud Computing is the use of remote servers to store, manage, and process data rather than using local servers while Grid Computing can be defined as a network of computers working together to perform a task that would rather be difficult for a single machine.

## ****What is Cloud Computing?****

Cloud Computing is a Client-server computing architecture.[**Cloud Computing**](https://www.geeksforgeeks.org/cloud-computing/)means storing and accessing the data and programs on remote servers that are hosted on the internet instead of the computer’s hard drive or local server. Cloud computing is also referred to as Internet-based computing, it is a technology where the resource is provided as a service through the Internet to the user. The stored data can be files, images, documents, or any other storable document.

## Advantages of Cloud Computing

* One of the advantages of cloud computing is scalability.
* Cloud computing provide on demand self service.
* Cloud Computing is cost effective.
* Cloud services are accessible from anywhere with an[internet](https://www.geeksforgeeks.org/introduction-to-internet/) connection.
* Cloud Computing provide rapid elasticity.

## Disadvantages of Cloud Computing

* Dependence on Internet Connectivity
* Security Concerns
* Cloud computing require constant and high speed internet.
* Users have less control over the underlying infrastructure and configurations.

## ****What is Grid Computing?****

[Grid Computing](https://www.geeksforgeeks.org/grid-computing/) is a [Distributed computing](https://www.geeksforgeeks.org/what-is-distributed-computing/) architecture. In grid computing, resources are used in collaborative patterns, and also in grid computing, the users do not pay for use.

## ****Advantages of Grid Computing****

* Grid Computing provide high resources utilization.
* Grid Computing allow parallel processing of task.
* Grid Computing is designed to be scalable.

## ****Disadvantages of Grid Computing****

* The software of the grid is still in the evolution stage.
* Grid computing introduce Complexity.
* Limited Flexibility
* Security Risks

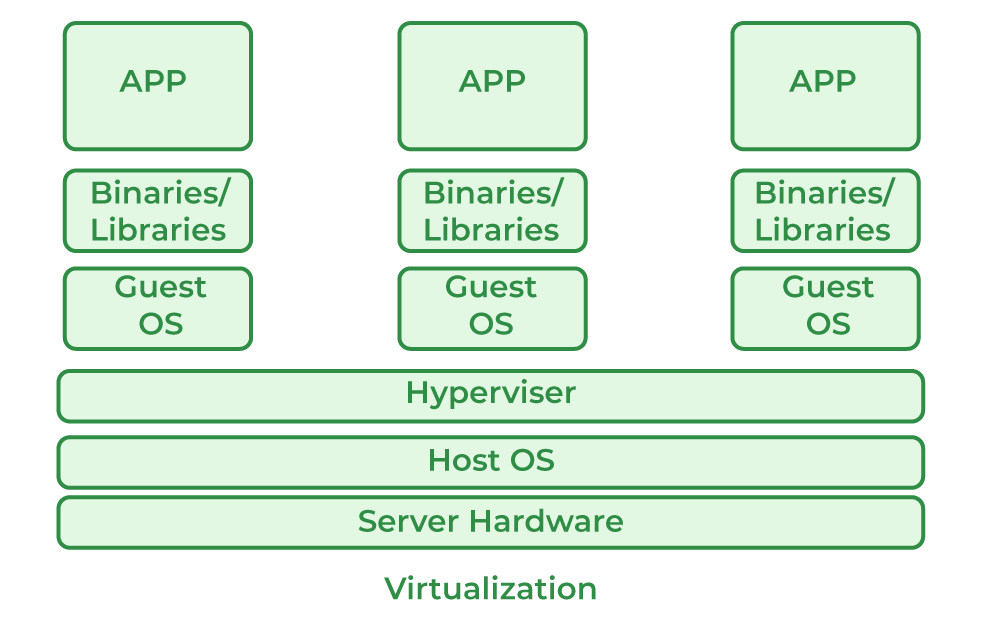
## Difference between Cloud Computing and Grid Computing

| **Cloud Computing** | **Grid Computing** |
| --- | --- |
| Cloud computing is a Client-server computing architecture. | While it is a Distributed computing architecture. |
| Cloud computing is a centralized executive. | While grid computing is a decentralized executive. |
| In cloud computing, resources are used in centralized pattern. | While in grid computing, resources are used in collaborative pattern. |
| It is more flexible than grid computing. | While it is less flexible than cloud computing. |
| In cloud computing, the users pay for the use. | While in grid computing, the users do not pay for use. |
| Cloud computing is a high accessible service. | While grid computing is a low accessible service. |
| It is highly scalable as compared to grid computing. | While grid computing is low scalable in comparison to cloud computing. |
| It can be accessed through standard web protocols. | While it is accessible through grid middleware. |
| Cloud computing is based on service-oriented. | Grid computing is based on application-oriented. |
| Cloud computing uses service like [IAAS](https://www.geeksforgeeks.org/difference-between-iaas-paas-and-saas/), PAAS, [SAAS](https://www.geeksforgeeks.org/software-as-a-service-saas/). | Grid computing uses service like distributed computing, [distributed pervasive](https://www.geeksforgeeks.org/introduction-to-pervasive-computing/#:~:text=), distributed information. |

**Virtualization in Cloud Computing and Types**

**Virtualization**is used to create a virtual version of an underlying service With the help of Virtualization, multiple operating systems and applications can run on the same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware. It was initially developed during the mainframe era.

It is one of the main cost-effective, hardware-reducing, and energy-saving techniques used by cloud providers. Virtualization allows sharing of a single physical instance of a resource or an application among multiple customers and organizations at one time. It does this by assigning a logical name to physical storage and providing a pointer to that physical resource on demand. The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for [cloud computing](https://www.geeksforgeeks.org/cloud-computing/). Moreover, virtualization technologies provide a virtual environment for not only executing applications but also for storage, memory, and networking.



*Virtualization*

* Host Machine: The machine on which the virtual machine is going to be built is known as Host Machine.
* Guest Machine: The virtual machine is referred to as a Guest Machine.

**Work of Virtualization in Cloud Computing**

Virtualization has a prominent impact on Cloud Computing. In the case of cloud computing, users store data in the cloud, but with the help of Virtualization, users have the extra benefit of sharing the infrastructure. Cloud Vendors take care of the required physical resources, but these cloud providers charge a huge amount for these services which impacts every user or organization. Virtualization helps Users or Organisations in maintaining those services which are required by a company through external (third-party) people, which helps in reducing costs to the company. This is the way through which Virtualization works in Cloud Computing.

**Benefits of Virtualization**

* More flexible and efficient allocation of resources.
* Enhance development productivity.
* It lowers the cost of IT infrastructure.
* Remote access and rapid scalability.
* High availability and disaster recovery.
* Pay peruse of the IT infrastructure on demand.
* Enables running multiple operating systems.

**Drawback of Virtualization**

* **High Initial Investment:**Clouds have a very high initial investment, but it is also true that it will help in reducing the cost of companies.
* **Learning New Infrastructure:** As the companies shifted from Servers to Cloud, it requires highly skilled staff who have skills to work with the cloud easily, and for this, you have to hire new staff or provide training to current staff.
* **Risk of Data:**Hosting data on third-party resources can lead to putting the data at risk, it has the chance of getting attacked by any hacker or cracker very easily.

For more benefits and drawbacks, you can refer to the [Pros and Cons of Virtualization.](https://www.geeksforgeeks.org/pros-and-cons-of-virtualization-in-cloud-computing/)

**Characteristics of Virtualization**

* **Increased Security:** The ability to control the execution of a guest program in a completely transparent manner opens new possibilities for delivering a secure, controlled execution environment. All the operations of the guest programs are generally performed against the virtual machine, which then translates and applies them to the host programs.
* **Managed Execution:** In particular, sharing, aggregation, emulation, and isolation are the most relevant features.
* **Sharing:** Virtualization allows the creation of a separate computing environment within the same host.
* **Aggregation:** It is possible to share physical resources among several guests, but virtualization also allows aggregation, which is the opposite process.

**Virtual Machine Security in Cloud**

The term **“Virtualized Security,”** sometimes known as “security virtualization,” describes security solutions that are software-based and created to operate in a virtualized IT environment. This is distinct from conventional hardware-based network security, which is static and is supported by equipment like conventional switches, routers, and firewalls.

Virtualized security is flexible and adaptive, in contrast to hardware-based security. It can be deployed anywhere on the network and is frequently cloud-based so it is not bound to a specific device.

In[Cloud Computing](https://www.geeksforgeeks.org/cloud-computing/)**,** where operators construct workloads and applications on-demand, virtualized security enables security services and functions to move around with those on-demand-created workloads. This is crucial for virtual machine security. It’s crucial to protect virtualized security in cloud computing technologies such as isolating multitenant setups in public cloud settings. Because data and workloads move around a complex ecosystem including several providers, virtualized security’s flexibility is useful for securing hybridand multi-cloud settings.

**Types of Hypervisors**

**Type-1 Hypervisors**

Its functions are on unmanaged systems. Type 1 hypervisors include **Lynx Secure, RTS Hypervisor, Oracle VM, Sun xVM Server, and Virtual Logic VLX**. Since they are placed on bare systems, type 1 hypervisor do not have any host operating systems.

**Type-2 Hypervisor**

It is a software interface that simulates the hardware that a system typically communicates with. Examples of Type 2 hypervisors include **containers, KVM, Microsoft Hyper V, VMWare Fusion, Virtual Server 2005 R2, Windows Virtual PC, and VMware workstation 6.0**.

**Type I Virtualization**

In this design, the**Virtual Machine Monitor (VMM)** sits directly above the hardware and eavesdrops on all interactions between the VMs and the hardware. On top of the VMM is a management VM that handles other guest VM management and handles the majority of a hardware connections. The Xen system is a common illustration of this kind of virtualization design.

**Type II virtualization**

In these architectures, like VMware Player, allow for the operation of the VMM as an application within the host operating system (OS). I/O drivers and guest VM management are the responsibilities of the host OS.

Securing virtual machines in the cloud is a top priority for DevOps teams. To learn more about integrating security best practices into your DevOps pipeline, the [**DevOps Engineering – Planning to Production**](https://gfgcdn.com/tu/S94/)**course** offers hands-on examples of securing cloud infrastructure.

**Service Provider Security**

The system’s virtualization hardware shouldn’t be physically accessible to anyone not authorized. Each VM can be given an access control that can only be established through the Hypervisor in order to safeguardit against unwanted access by Cloud administrators. The three fundamental tenets of access control, identity, authentication, and authorization**,** will prevent unauthorized data and system components from being accessed by administrators.

**Hypervisor Security**

The Hypervisor’s code integrity is protected via a technology called Hyper safe. Securing the write-protected memory pages, expands the hypervisor implementation and prohibits coding changes. By restricting access to its code,it defends the Hypervisor from control-flow hijacking threats**.** The only way to carry out a VM Escape assault is through a local physical setting. Therefore, insider assaults must be prevented in the physical Cloud environment. Additionally, the host OS and the interaction between the guest machines need to be configured properly.

**Virtual Machine Security**

The administrator must set up a program or application that prevents virtual machines from consuming additional resources without permission. Additionally, a lightweight process that gathers logs from the VMs and monitors them in real-time to repair any **VM tampering must operate on a Virtual Machine**. Best security procedures must be used to harden the guest OS and any running applications. These procedures include setting up firewalls, host intrusion prevention systems (HIPS), anti-virus and anti-spyware programmers, online application protection, and log monitoring in guest operating systems.

**Guest Image Security**

A policy to control the creation, use, storage, and deletion of images must be in place for organizations that use virtualization. To find viruses, worms, spyware, and rootkits that hide from security software running in a guest OS, image files must be analyzed.

**Benefits of Virtualized Security**

Virtualized security is now practically required to meet the intricate security requirements of a virtualized network, and it is also more adaptable and effective than traditional physical security.

* **Cost-Effectiveness:**Cloud computing’s virtual machine security enables businesses to keep their networks secure without having to significantly raise their expenditures on pricey proprietary hardware. Usage-based pricing for cloud-based virtualized security services can result in significant savings for businesses that manage their resources effectively.
* **Flexibility:** It is essential in a virtualized environment that security operations can follow workloads wherever they go. A company is able to profit fully from virtualization while simultaneously maintaining data security thanks to the protection it offers across various data centers, in multi-cloud, and hybrid-cloud environments.
* **Operational Efficiency:**Virtualized security can be deployed more quickly and easily than hardware-based security because it doesn’t require IT, teams, to set up and configure several hardware appliances. Instead, they may quickly scale security systems by setting them up using centralized software. Security-related duties can be automated when security technology is used, which frees up more time for IT employees.
* **Regulatory Compliance:**Virtual machine security in cloud computing is a requirement for enterprises that need to maintain regulatory compliance because traditional hardware-based security is static and unable to keep up with the demands of a virtualized network.

**Virtualization Machine Security Challenges**

* As we previously covered, buffer overflows are a common component of classical network attacks. **Trojan horses, worms, spyware, rootkits, and DoS attacks**are examples of malware.
* In a cloud context, more recent assaults might be caused via VM rootkits, hypervisor malware, or guest hopping and hijacking. Man-in-the-middle attacks against VM migrations are another form of attack**.**Typically, passwords or sensitive information are stolen during passive attacks. Active attacks could alter the kernel’s data structures, seriously harming cloud servers.
* **HIDS or NIDS** are both types of IDSs. To supervise and check the execution of code, use programmed shepherding. The **RIO dynamic optimization infrastructure**, the v Safe and v Shield tools from VMware, security compliance for hypervisors, and Intel vPro technology are some further protective solutions.

**Four Steps to ensure VM Security in Cloud Computing**

**Protect Hosted Elements by Segregation**

To secure virtual machines in cloud computing, the first step is to segregate the newly hosted components. Let’s take an example where three features that are now running on an edge device may be placed in the cloud either as part of a private subnetwork that is invisible or as part of the service data plane, with addresses that are accessible to network users.

**All Components are Tested and Reviewed**

Before allowing virtual features and functions to be implemented, you must confirm that they comply with security standards as step two of cloud-virtual security. Virtual networking is subject to outside attacks, which can be dangerous, but insider attacks can be disastrous. When a feature with a backdoor security flaw is added to a service, it becomes a part of the infrastructure of the service and is far more likely to have unprotected attack paths to other infrastructure pieces.

**Separate Management APIs to Protect the Network**

The third step is to isolate service from infrastructure management and orchestration. Because they are created to regulate features, functions, and service behaviors, management APIs will always pose a significant risk. All such APIs should be protected, but the ones that keep an eye on infrastructure componentsthat service users should never access must also be protected.

**Keep Connections Secure and Separate**

The fourth and last aspect of cloud virtual network security is to make sure that connections between tenants or services do not cross over into virtual networks. **Virtual Networking is a fantastic approach to building quick connections to scaled or redeployed features,**but each time a modification is made to the virtual network, it’s possible that an accidental connection will be made between two distinct services, tenants, or feature/function deployments. A data plane leak, a link between the actual user networks, or a management or control leak could result from this, allowing one user to affect the service provided to another.