Infrastructure Security

By Ahsan Farooqui

Setup

- ❏ Overview
- ❏ Network
- ❏ Compute Workload
- ❏ Data/Storage Security & Encryption (covered in separate domain)

Introduction

- Infrastructure security is the foundation for operating securely in the cloud. “Infrastructure” is the glue of computers and networks that we build everything on top of.
- Compute and networking security
- Storage security is also core to infrastructure
- Infrastructure security encompasses the lowest layers of security, from physical facilities through the consumer’s configuration and implementation of infrastructure components.
- These are the fundamental components that everything else in the cloud is built from, including compute (workload), networking, and storage security.

Introduction

- we are focusing on cloud-specific aspects of infrastructure
- security.
- discusses two aspects:
  - cloud considerations for the underlying infrastructure,
  - and security for virtual networks and workloads.

Overview

- In cloud computing there are two macro layers to infrastructure:
  - The fundamental resources pooled together to create a cloud. This is the raw, physical and logical compute (processors, memory, etc.), networks, and storage used to build the cloud's resource pools. For example, this includes the security of the networking hardware and software used to create the network resource pool.
  - The virtual/abstracted infrastructure managed by a cloud user. That's the compute, network, and storage assets that they use from the resource pools. For example, the security of the virtual network, as defined and managed by the cloud user.
- Domain Focus is on macro layer 2 infrastructure security for the cloud user.
- Infrastructure security that's more fundamental for cloud providers, including those who manage private clouds, is well aligned with existing security standards for data centers.

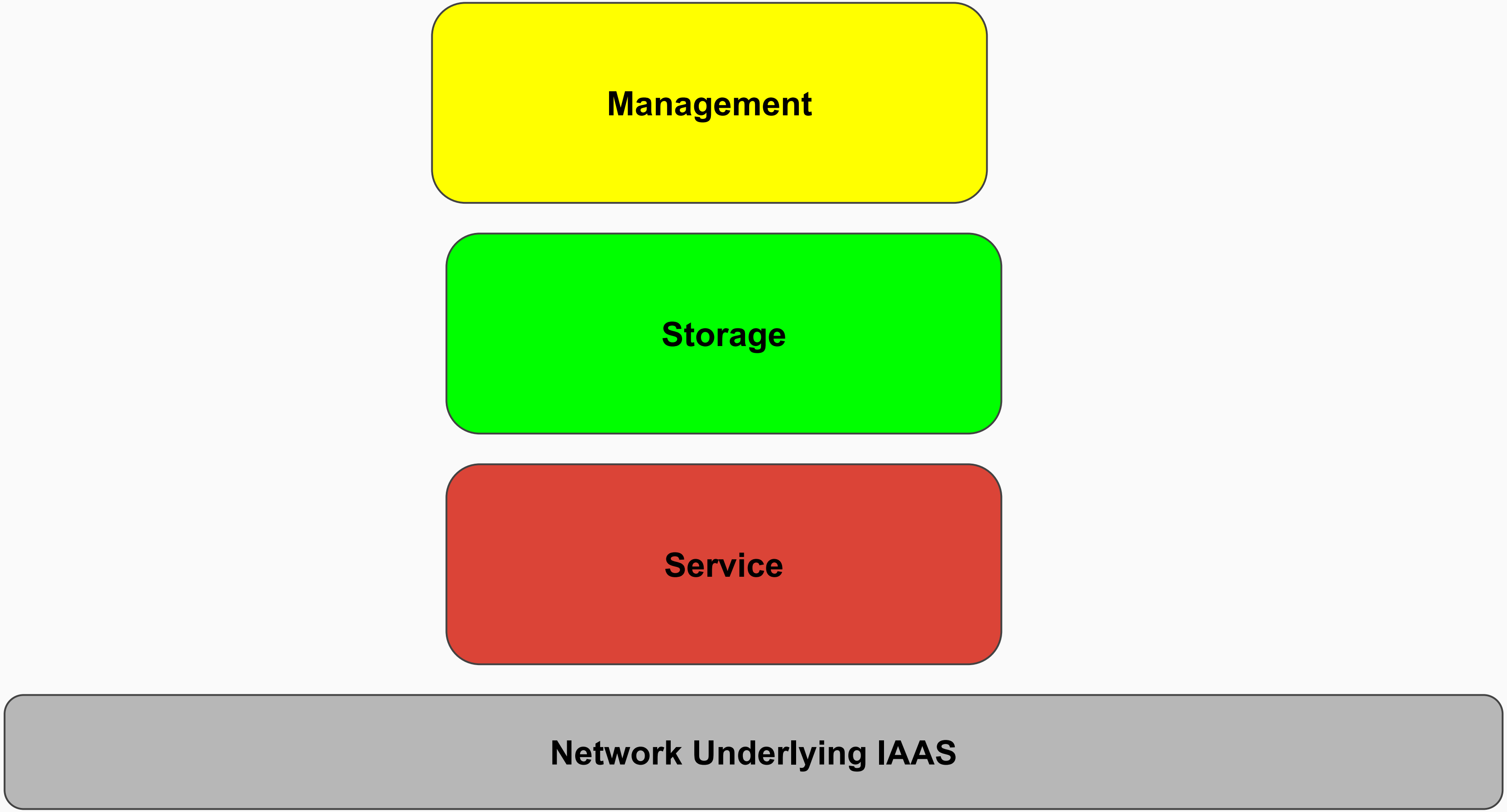
Cloud Network Virtualization

- All clouds utilize some form of virtual networking to abstract the physical network and create a network resource pool.
- Typically the cloud user provisions desired networking resources from this pool, which can then be configured within the limits of the virtualization technique used.
- For example,
    - some cloud platforms only support allocation of IP addresses within particular subnets, while others allow the cloud user the capability to provision entire Class B virtual networks and completely define the subnet architecture.

3 Dedicated Isolated Networks

- ❑ We see at-least three dedicated isolated networks on a dedicated hardware
- ❑ Service Network
  - ❑ The service network for communications between virtual machines and the Internet. This builds the network resource pool for the cloud users.
  - ❑ Internet to Compute nodes
  - ❑ Instances to Instance node
- ❑ Storage Network
  - ❑ The storage network to connect virtual storage to virtual machines.
  - ❑ Storage nodes(Volumes) to Compute nodes(Instances)
- ❑ Management Network
  - ❑ A management network for management and API traffic.
  - ❑ Management Plane to nodes

Dedicated Networks



Management

Storage

Service

Network Underlying IAAS

Two Categories of Network Virtualization

- **Virtual Local Area Networks (VLANs):**
  - **VLANs leverage existing network technology implemented in most network hardware. VLANs are extremely common in enterprise networks, even without cloud computing. They are designed for use in single-tenant networks (enterprise data centers) to separate different business units, functions, etc. (like guest networks). VLANs are not designed for cloud-scale virtualization or security and shouldn’t be considered, on their own, an effective security control for isolating networks. They are also never a substitute for physical network segregation.**

- **Software Defined Networking (SDN): A more complete abstraction layer on top of networking hardware, SDNs decouple the network control plane from the data plane (you can read more on SDN principles at this Wikipedia entry). This allows us to abstract networking from the traditional limitations of a LAN.There are multiple implementations, including standards-based and proprietary options.**

What is Software-Defined Networking (SDN)?

Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

This model differs from that of traditional networks, which use dedicated hardware devices (i.e., routers and switches) to control network traffic. SDN can create and control a virtual network – or control a traditional hardware – via software.

While network virtualization allows organizations to segment different virtual networks within a single physical network, or to connect devices on different physical networks to create a single virtual network, software-defined networking enables a new way of controlling the routing of data packets through a centralized server.

How does Software-Defined Networking (SDN) work?

In SDN (like anything virtualized), the software is decoupled from the hardware. SDN moves the control plane that determines where to send traffic to software, and leaves the data plane that actually forwards the traffic in the hardware. This allows network administrators who use software-defined networking to program and control the entire network via a single pane of glass instead of on a device by device basis.

There are three parts to a typical SDN architecture, which may be located in different physical locations:

- ❏ Applications, which communicate resource requests or information about the network as a whole
- ❏ Controllers, which use the information from applications to decide how to route a data packet
- ❏ Networking devices, which receive information from the controller about where to move the data

Physical or virtual networking devices actually move the data through the network. In some cases, virtual switches, which may be embedded in either the software or the hardware, take over the responsibilities of physical switches and consolidate their functions into a single, intelligent switch. The switch checks the integrity of both the data packets and their virtual machine destinations and moves the packets along.

What are the different models of SDN?

While the premise of centralized software controlling the flow of data in switches and routers applies to all software-defined networking, there are different models of SDN.

- ❑ Open SDN: Network administrators use a protocol like OpenFlow to control the behavior of virtual and physical switches at the data plane level.
- ❑ SDN by APIs: Instead of using an open protocol, application programming interfaces control how data moves through the network on each device.
- ❑ SDN Overlay Model: Another type of software-defined networking runs a virtual network on top of an existing hardware infrastructure, creating dynamic tunnels to different on-premise and remote data centers. The virtual network allocates bandwidth over a variety of channels and assigns devices to each channel, leaving the physical network untouched.
- ❑ Hybrid SDN: This model combines software-defined networking with traditional networking protocols in one environment to support different functions on a network. Standard networking protocols continue to direct some traffic, while SDN takes on responsibility for other traffic, allowing network administrators to introduce SDN in stages to a legacy environment.

How is SDN different from Traditional Networking?

The key difference between SDN and traditional networking is infrastructure: SDN is software-based, while traditional networking is hardware-based. Because the control plane is software-based, SDN is much more flexible than traditional networking. It allows administrators to control the network, change configuration settings, provision resources, and increase network capacity—all from a centralized user interface, without adding more hardware.

There are also security differences between SDN and traditional networking. Thanks to greater visibility and the ability to define secure pathways, SDN offers better security in many ways. However, because software-defined networks use a centralized controller, securing the controller is crucial to maintaining a secure network, and this single point of failure represents a potential vulnerability of SDN.

What are SDN Benefits?

Many of today’s services and applications, especially when they involve the cloud, could not function without SDN.

SDN allows data to move easily between distributed locations, which is critical for cloud applications.

- ❑ Additionally, SDN supports moving workloads around a network quickly. For instance, dividing a virtual network into sections, using a technique called network functions virtualization (NFV), allows telecommunications providers to move customer services to less expensive servers or even to the customer’s own servers. Service providers can use a virtual network infrastructure to shift workloads from private to public cloud infrastructures as necessary, and to make new customer services available instantly.
- ❑ SDN also makes it easier for any network to flex and scale as network administrators add or remove virtual machines, whether those machines are on-premises or in the cloud.
- ❑ Finally, because of the speed and flexibility offered by SDN, it is able to support emerging trends and technologies such as edge computing and the Internet of Things, which require transferring data quickly

Why SDN are important?

SDN represents a substantial step forward from traditional networking, in that it enables the following:

- ❏ Increased control with greater speed and flexibility:
  - ❏ Instead of manually programming multiple vendor-specific hardware devices, developers can control the flow of traffic over a network simply by programming an open standard software-based controller. Networking administrators also have more flexibility in choosing networking equipment, since they can choose a single protocol to communicate with any number of hardware devices through a central controller.
- ❏ Customizable network infrastructure:
  - ❏ With a software-defined network, administrators can configure network services and allocate virtual resources to change the network infrastructure in real time through one centralized location. This allows network administrators to optimize the flow of data through the network and prioritize applications that require more availability.
- ❏ Robust security:
  - ❏ A software-defined network delivers visibility into the entire network, providing a more holistic view of security threats. With the proliferation of smart devices that connect to the internet, SDN offers clear advantages over traditional networking. Operators can create separate zones for devices that require different levels of security, or immediately quarantine compromised devices so that they cannot infect the rest of the network.

Virtual Appliances Challenges in Cloud-1

Since physical appliances can’t be inserted (except by the cloud provider) they must be replaced by virtual appliances if still needed, and if the cloud network supports the necessary routing. This brings the same concerns as inserting virtual appliances for network monitoring:

- ❑ Virtual appliances thus become bottlenecks, since they cannot fail open, and must intercept all traffic.
- ❑ Virtual appliances may take significant resources and increase costs to meet network performance requirements.
- ❑ When used, virtual appliances should support auto-scaling to match the elasticity of the resources they protect. Depending on the product, this could cause issues if the vendor does not support elastic licensing compatible with auto-scaling.
- ❑ Virtual appliances should also be aware of operating in the cloud, as well as the ability of instances to move between different geographic and availability zones. The velocity of change in cloud networks is higher than that of physical networks and tools need to be designed to handle this important difference.
- ❑ Cloud application components tend to be more distributed to improve resiliency and, due to auto-scaling, virtual servers may have shorter lives and be more prolific. This changes how security policies need to be designed.

Virtual Appliances Challenges in Cloud-2

- ❑ This induces that very high rate of change that security tools must be able to manage (e.g., servers with a lifespan of less than an hour).
- ❑ IP addresses will change far more quickly than on a traditional network, which security tools must account for. Ideally they should identify assets on the network by a unique ID, not an IP address or network name.
- ❑ Assets are less likely to exist at static IP addresses. Different assets may share the same IP address within a short period of time. Alerts and the Incident Response lifecycle may have to be modified to ensure that the alert is actionable in such a dynamic environment. Assets within a single application tier will often be located on multiple subnets for resiliency, further complicating IP-based security policies. Due to auto-scaling, assets may also be ephemeral, existing for hours or even minutes. On the upside, cloud architectures skew towards fewer services per server, which improves your ability tod efine restrictive firewall rules. Instead of a stack of services on a single virtual machine — as on physical servers where you need to maximize the capital investment in the hardware — it is common to run a much smaller set of services, or even a single service,

SDM Security Benefits-1

- ❏ Isolation is easier. It becomes possible to build out as many isolated networks as you need without constraints of physical hardware. For example, if you run multiple networks with the same CIDR address blocks, there is no logical way they can directly communicate, dueto addressing conflicts. This is an excellent way to segregate applications and services of different security contexts. We discuss this microsegregation in more detail below.
- ❏ SDN firewalls (e.g., security groups) can apply to assets based on more flexible criteria thanhardware-based firewalls, since they aren't limited based on physical topology. (Note thatthis is true of many types of software firewalls, but is distinct from hardware firewalls). SDN firewalls are typically policy sets that define ingress and egress rules that can apply to single assets or groups of assets, regardless of network location (within a given virtual network).For example, you can create a set of firewall rules that apply to any asset with a particular tag. Keep in mind this gets slightly difficult to discuss, since different platforms use different terminology and have different capabilities to support this kind of capability, so we are trying to keep things at a conceptual level.

SDM Security Benefits-2

- ❑ Combined with the cloud platform’s orchestration layer, this enables very dynamic and granular combinations and policies with less management overhead than the equivalent using a traditional hardware or host-based approach. For example, if virtual machines in an auto-scale group are automatically deployed in multiple subnets and load balanced across them, then you can create a firewall ruleset that applies to these instances,regardless of their subnet or IP address. It is a key enabling feature of secure cloud networks that use architectures quite differently from traditional computing.
- ❑ Default deny is often the starting point, and you are required to open connections from there, which is the opposite of most physical networks.• Think of it as the granularity of a host firewall with the better manageability of a network appliance. Host firewalls have two issues: They are difficult to manage at scale, and if the system they are on is compromised, they are easy to alter and disable. On the other hand, it is cost-prohibitive to route all internal traffic, evenbetween peers on a subnet, through a network firewall. Software firewalls, such as security groups, are managed outside a system yet apply to each system, without additional hardware costs or complex provisioning needed. Thus, it is trivial to do things like isolate every single virtual machine on the same virtual subnet.

SDM Security Benefits-3

- As briefly mentioned above, firewall rules can be based on other criteria, such as tags. Note, that while the potential is there, the actual capabilities depend on the platform. Just because a cloud network is SDN-based doesn’t mean it actually conveys any security benefits.
- Many network attacks are eliminated by default (depending on your platforms), such as ARP spoofing and other lower level exploits, beyond merely eliminating sniffing.This is due to the inherent nature of the SDN and application of more software-based rules and analysis in moving packets.
- It is possible to encrypt packets as they are encapsulated.
- As with security groups, other routing and network design can be dynamic and tied to the cloud’s orchestration layer, such as bridging virtual networks or connecting to internal PaaS services.
- Additional security functions can potentially be added natively.

Microsegmentation Software defined perimeter

- Microsegmentation (also sometimes referred to as hypersegregation) leverages virtual network topologies to run more, smaller, and more isolated networks without incurring additional hardware costs that historically make such models prohibitive. Since the entire networks are defined in software without many of the traditional addressing issues, it is far more feasible to run these multiple, software-defined environments.
- A common, practical example leveraging this capability is running most, if not all, applications on their own virtual network and only connecting those networks as needed. This dramatically reduces the blast radius if an attacker compromises an individual system. The attacker can no longer leverage this foothold to expand across the entire data center.
- Although there are no increases in capital expenses since cloud microsegmentation is based on software configurations, it can increase operational expenses in managing multiple overlappingnet works and connectivity.

Software defined perimeter(SDP) Components

❑ The CSA Software Defined Perimeter Working Group has developed a model and specification that combines device and user authentication to dynamically provision network access to resources and enhance security. SDP includes three components:

  ❑ An SDP client on the connecting asset (e.g. a laptop).

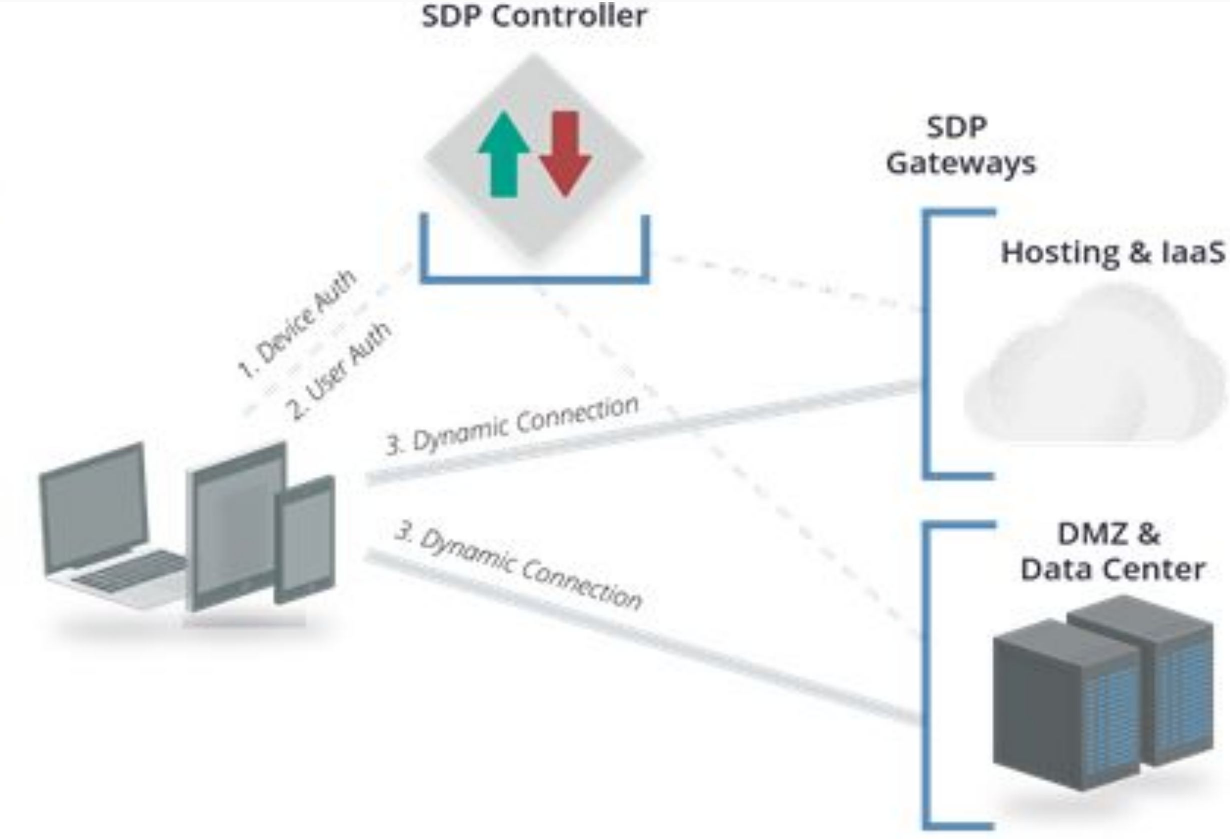
  ❑ The SDP controller for authenticating and authorizing SDP clients and configuring the connections to SDP gateways.

  ❑ The SDP gateway for terminating SDP client network traffic and enforcing policies in communication with the SDP controller.

❑ Network security decisions can thus be made on a wider range of criteria than just IP packets. Especially combined with SDNs this potentially offers greater flexibility and security for evolving network topologies.

Software defined perimeter(SDP) Components

More information on SDP is available from the CSA at https://cloudsecurityalliance.org/group/software-defined-perimeter/#_overview



Additional Consideration for Cloud Provider or Private Cloud

- ❑ **Providers must maintain the core security of the physical/traditional networks that the platform is built on. A security failure at the root network will likely compromise the security of all customers.And this security must be managed for arbitrary communications and multiple tenants, some of which must be considered adversarial.**
- ❑ **It is absolutely critical to maintain segregation and isolation for the multitenant environment. There will thus be additional overhead to properly enable, configure, and maintain the SDN security controls. While an SDN is more likely to provide needed isolation once it is up and running, it is important to take the extra time to get everything set up properly in order to handle potentially hostile tenants. We aren't saying your users are necessarily hostile, but it is safe to assume that, at some point, something on the network will be compromised and used to further an attack.**
- ❑ **Providers must also expose security controls to the cloud users so they can properly configure and manage their network security.**
- ❑ **Finally, providers are responsible for implementing perimeter security that protects the environment, but minimizes impact on customer workloads, for example, Distributed Denial of Service Protection (DDoS) and baseline IPS to filter out hostile traffic before it affects the cloud's**

  consumers. Another consideration is to ensure that any potentially sensitive information is *scrubbed* when a virtual instance is released back to the hypervisor, to ensure the information is not able to be read by another customer when the drive space is provisioned.

Hybrid Cloud Consideration

- ❑ Hybrid clouds connect an enterprise private cloud or data center to a public cloud provider, typically using either a dedicated Wide Area Network (WAN) link or VPN.
  Ideally the hybrid cloud will support arbitrary network addressing to help seamlessly extend the cloud user's network. If the cloud uses the same network address range as your on-premises assets,it is effectively unusable.
- ❑ The hybrid connection may reduce the security of the cloud network if the private network isn't at an equivalent security level. If you run a flat network in your data center, with minimal segregation from your employees' systems, someone could compromise an employee's laptop and then use that to scan your entire cloud deployment over the hybrid connection. A hybrid connection shouldn't effectively flatten the security of both networks. Separation should be enforced via routing, access controls, and even firewalls or additional network security tools between the two networks.
- ❑ For management and security reasons it is typically preferable to minimize hybrid connections. Connecting multiple disparate networks is complex, especially when one of those networks is software-defined and the other limited by hardware. Hybrid connections are often still necessary, but don't assume they are needed. They may increase routing complexity, can reduce the ability to run multiple cloud networks with overlapping IP ranges, and complicate security on both sides, due to the need to harmonize security controls.

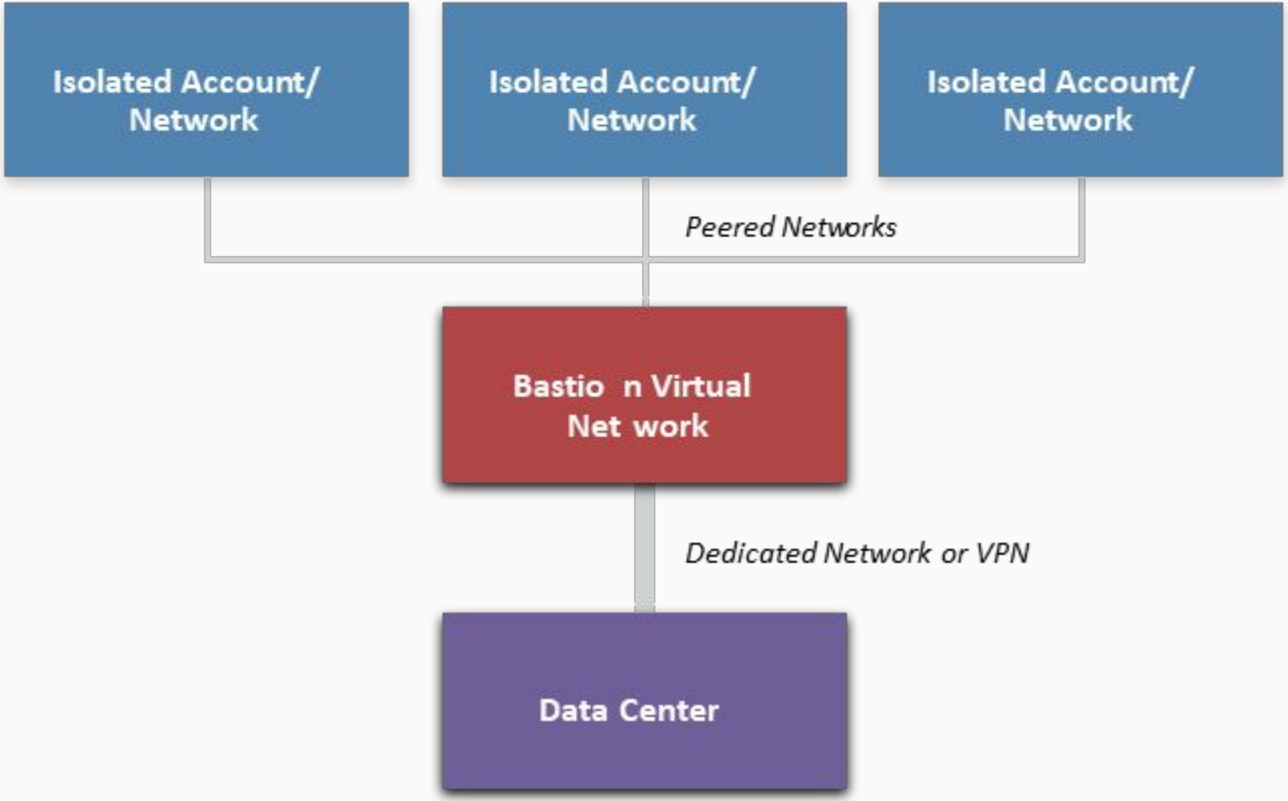
Bastion or Transit Hybrid Cloud Connectivity

One emerging architecture for hybrid cloud connectivity is “bastion” or “transit” virtual networks:

- ❑ This scenario allows you to connect multiple, different cloud networks to a data center using a single hybrid connection. The cloud user builds a dedicated virtual network for the hybrid connection and then peers any other networks through the designated bastion network.

- ❑ Second-level networks connect to the data center through the bastion network, but since they aren’t peered to each other they can’t talk to each other and are effectively segregated. Also, you can deploy different security tools, firewall rulesets, and Access Control Lists in the bastion network to further protect traffic in and out of the hybrid connection.

Bastion or Transit Hybrid Cloud Connectivity-Diagram


Isolated Account/ Network
Isolated Account/ Network
Isolated Account/ Network
Peered Networks
Bastio n Virtual Net work
Dedicated Network or VPN
Data Center

Cloud Compute and Workload Security

- A workload is a unit of processing, which can be in a virtual machine, a container, or other abstraction. Workloads always run somewhere on a processor and consume memory. Workloads include a very diverse range of processing tasks, which range from traditional applications running in a virtual machine on a standard operating system, to GPU- or FPGA-based specialized tasks. Nearly every one of these options is supported in some form in cloud computing.

- It's important to remember that every cloud workload runs on a hardware stack, and the integrity of this hardware is absolutely critical for the cloud provider to maintain. Different hardware stacks also support different execution isolation and chain of trust options. This can include hardware-based supervision and monitoring processes that run outside the main processors, secure execution environments, encryption and key management enclaves, and more.
- The range and rapidly changing nature of these options exceeds our ability to provide proscriptive guidance at this time, but in a general sense there are potentially very large gains in security by selecting and properly leveraging hardware with these advanced capabilities.

Multiple Compute Types

AT here are multiple compute abstraction types, each with differing degrees of segregation and isolation:

- **Virtual machines:** Virtual machines are the most-well known form of compute abstraction, and are offered by all IaaS providers. They are commonly called instances in cloud computing since they are created (or cloned) off a base image. The Virtual Machine Manager (hypervisor) abstracts an operating system from the underlying hardware. Modern hypervisors can tie into underlying hardware capabilities now commonly available on standard servers (and workstations) to reinforce isolation while supporting high-performance operations.
- Virtual machines are potentially open to certain memory attacks, but this is increasingly difficult due to ongoing hardware and software enhancements to reinforce isolation. VMs on modern hypervisors are generally an effective security control, and advances in hardware isolation for VMs and secure execution environments continue to improve these capabilities.
- **Containers:** Containers are code execution environments that run within an operating system (for now), sharing and leveraging resources of that operating system. While a VM is a full abstraction of an operating system, a container is a constrained place to run segregated processes while still utilizing the kernel and other capabilities of the base OS.
- Multiple containers can run on the same virtual machine or be implemented without the use of VMs at all and run directly on hardware.
- The container provides code running inside a restricted environment with only access to the processes and capabilities defined in the container configuration. This allows containers to launch incredibly rapidly, since they don't need to boot an operating system or launch many (sometimes any) new services; the container only needs access to already-running services in the host OS and some can launch in milliseconds.
- Containers are newer, with differing isolation capabilities that are very platform-dependent. They are also evolving quickly with different management systems, underlying operating systems, and container technologies.

Multiple Compute Types -Cond

- ❑ **Platform-based workloads:**
  - ❑ **This is a more complex category that covers workloads running on a shared platform that aren't virtual machines or containers, such as logic/procedures running on a shared database platform. Imagine a stored procedure running inside a multitenant database, or a machine-learning job running on a machine-learning Platform as a Service. Isolation and security are totally the responsibility of the platform provider, although the provider may expose certain security options and controls.**
- ❑ **• Serverless computing:**
  - ❑ **Serverless is a broad category that refers to any situation where the cloud user doesn't manage any of the underlying hardware or virtual machines, and just accesses exposed functions. For example, there are serverless platforms for directly executing application code. Under the hood, these still utilize capabilities such as containers, virtual machines, or specialized hardware platforms. From a security perspective, serverless is merely a combined term that covers containers and platform-based workloads, where the cloud provider manages all the underlying layers, including foundational security functions and controls.**

How cloud Change Workload Security

- **Workload Isolation**
  Any given processor and memory will nearly always be running multiple workloads, often from different tenants. Multiple tenants will likely share the same physical compute node, and there is a range of segregation capabilities on different hardware stacks. The burden to maintain workload isolation is on the cloud provider and should be one of their top priorities.

- **Dedicated or Private Tenancy or workload Isolation**
  In some environments dedicated/private tenancy is possible, but typically at a higher cost. With this model only designated workloads run on a designated physical server. Costs increase in public cloud as a consumer since you are taking hardware out of the general resource pool, but also in private cloud, due to less efficient use of internal resources.

- Cloud users rarely get to control where a workload physically runs, regardless of deployment model, although some platforms do support designating particular hardware pools or general locations to support availability, compliance, and other requirements.

Immutable Workload Enable Security

- **Immutable Virtual Machine**
  Auto-scaling and containers, by nature, work best when you run instances launched dynamically based on an image; those instances can be shut down when no longer needed for capacity without breaking an application stack. This is core to the elasticity of compute in the cloud. Thus, you no longer patch or make other changes to a running workload, since that wouldn't change the image, and, thus, new instances would be out of sync with whatever manual changes you make on whatever is running. We call these virtual machines immutable.

- To reconfigure or change an immutable instance you update the underlying image, and then rotate the new instances by shutting down the old ones and running the new ones in their place.

- There are degrees of immutable.
  - The pure definition is fully replacing running instances with a new image.
  - However, some organizations only push new images to update the operating system and use alternative deployment techniques to push code updates into running virtual machines. While technically not completely immutable, since the instance changes, these pushes still happen completely through automation and no one ever manually logs in to running systems to make local changes.

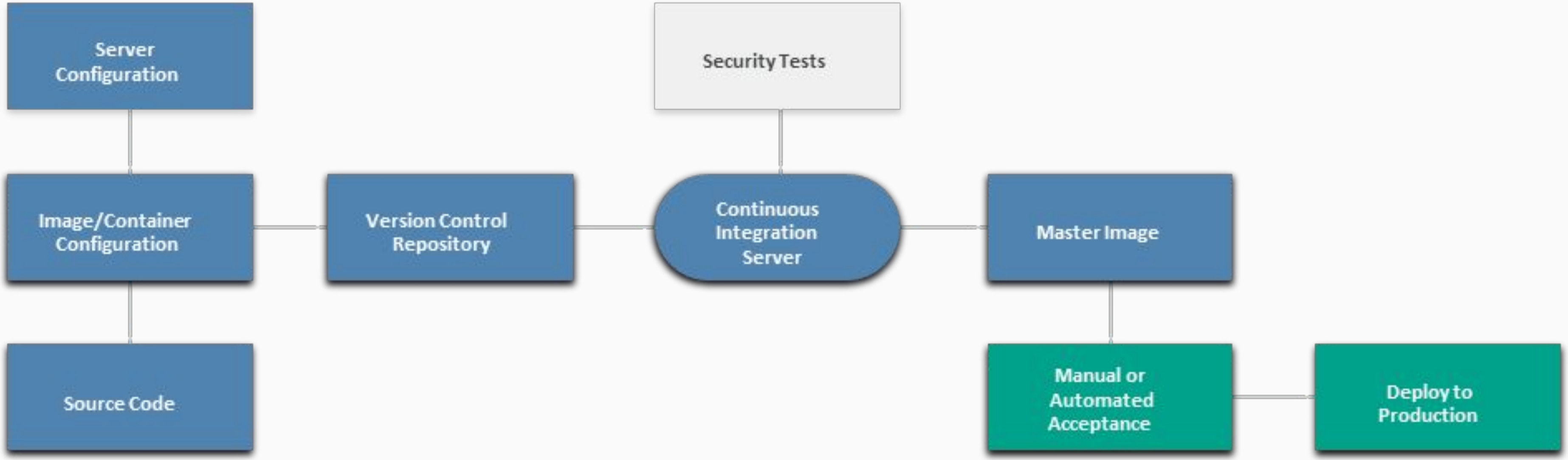
Immutable Workload Benefits

- Immutable workloads enable significant security benefits:
  - You no longer patch running systems or worry about dependencies, broken patch processes, etc. You replace them with a new gold master.
  - You can, and should, disable remote logins to running workloads (if logins are even an option). This is an operational requirement to prevent changes that aren’t consistent across the stack, which also has significant security benefits.
  - It is much faster to roll out updated versions, since applications must be designed to handle individual nodes going down (remember, this is fundamental to any auto-scaling). You are less constrained by the complexity and fragility of patching a running system. Even if something breaks, you just replace it.
  - It is easier to disable services and whitelist applications/processes since the instance should never change.
  - Most security testing can be managed during image creation, reducing the need for vulnerability assessment on running workloads since their behavior should be completely known at the time of creation. This doesn’t eliminate all security testing for production workloads, but it is a means of offloading large portions of testing.

Immutable Additional Requirements

- **Immutable does add some requirements**
  - **You need a consistent image creation process and the automation to support updating deployments. These new images must be produced on a regular basis to account for patch and malware signature updates.**
  - **Security testing must be integrated into the image creation and deployment process, including source code tests and, if using virtual machines or standard containers, vulnerability assessments.**
  - **Image configurations need mechanisms to disable logins and restrict services before deploying the images and using them for production virtual machines.**
  - **You may want a process, for some workloads, to enable logins to workloads that aren't actively in the application stack for troubleshooting. This could be a workload pulled from the group but allowed to continue to run in isolation. Alternatively (and often preferred), send sufficiently detailed logs to an external collector so that there is never a need to log in.**
  - **There will be increased complexity to manage the service catalog, since you might createdozens, or even hundreds, of images on any given day.**

Image Creation For Immutable VMs


Server Configuration
Security Tests
Image/Container Configuration
Version Control Repository
Continuous Integration Server
Master Image
Source Code
Manual or Automated Acceptance
Deploy to Production

A deployment pipeline for creating images for immutable virtual machines or containers.

Impact of Cloud on Standard Workload Security Control

Some standard workload controls aren't as viable in cloud workloads (e.g. running antivirus inside some container types). Others aren't necessarily needed or need deep modification to maintain effectiveness in cloud computing:

- ❑ **You may lose the ability to run software agents for non-VM based workloads, such as those running in "serverless" provider-managed containers.**
- ❑ **"Traditional" agents may impede performance more heavily in cloud. Lightweight agents with lower compute requirements allow better workload distribution and efficient use of resources. Agents not designed for cloud computing may assume underlying compute capacity that isn't aligned with how the cloud deployment is designed. The developers on a given project might assume they are running a fleet of lightweight, single-purpose virtual machines. A security agent not attuned to this environment could significantly increase processing overhead, requiring larger virtual machine types and increasing costs.**
- ❑ **Agents that operate in cloud environments also need to support dynamic cloud workloads and deployment patterns like auto-scaling. They can't rely (on the agent or in the management system) on static IP addressing. While some cloud assets run on static IP addresses, it is far more common for the cloud to dynamically assign IP addresses at run time to enable elasticity. Thus, the agent must have the ability to discover the management/control plane and use that to determine what kind of workload it is running on and where.**

Impact of Cloud on Standard Workload Security Control

The management plane of the agent must itself also operate at the speed of auto-scaling and support elasticity (e.g., be able to keep up with incredibly dynamic IP addressing, such as the same address used by multiple workloads within a single hour). Traditional tools aren’t normally designed for this degree of velocity, creating the same issue as we discussed with network security and firewalls.

- ❑ **Agents shouldn’t increase attack surface due to communications/networking or other requirements that increase the attack surface. While this is always true, there is a greater likelihood of an agent becoming a security risk in cloud for a few reasons:**
- ❑ **We have a greater ability to run immutable systems, and an agent, like any piece of software, opens up additional attack surface, especially if it ingests configuration changes and signatures that could be used as an attack vector.**
- ❑ **In cloud we also tend to run fewer different services with a smaller set of networking ports on any given virtual machine (or container), as compared to a physical server. Some agents require opening up additional firewall ports, which increases the network attack surface.**
- ❑ **This doesn’t mean agents always create new security risks, but the benefits need to be balanced before simply assuming the security upside.**

Impact of Cloud on Standard Workload Security Control

- The File integrity monitoring can be an effective means of detecting unapproved changes to running immutable instances. Immutable workloads typically require fewer additional security tools, due to their hardened nature. They are locked down more than the usual servers and tend to run a smaller set of services. File integrity monitoring, which tends to be very lightweight, can be a good security control for immutable workloads since you should essentially have zero false positives by their unchanging nature.
- Long-running VMs that still run standard security controls may be isolated on the network, changing how they are managed. You might experience difficulty in connecting your management tool to a virtual machine running in a private network subnet. While you can technically run the management tool in the same subnet, this could increase costs significantly and be more difficult to manage.
- Cloud workloads running in isolation are typically less resilient than on physical infrastructure, due to the abstraction. Providing disaster recovery for these is extremely important.

Changes to Workload Security Monitoring and logging

- **Security logging/monitoring is more complex in cloud computing:**
  - **IP addresses in logs won't necessarily reflect a particular workflow since multiple virtual machines may share the same IP address over a period of time, and some workloads like containers and serverless may not have a recognizable IP address at all. Thus, you need to collect some other unique identifiers in the logs to be assured you know what the log entries actually refer to. These unique identifiers need to account for ephemeral systems, which may only be active for a short period of time.**
  - **Logs need to be offloaded and collected externally more quickly due to the higher velocity of change in cloud. You can easily lose logs in an auto-scale group if they aren't collected before the cloud controller shuts down an unneeded instance.**
  - **Logging architectures need to account for cloud storage and networking costs. For example, sending all logs from instances in a public cloud to on-premises Security Information and Event Management (SIEM) may be cost prohibitive, due to the additional internal storage and extra Internet networking fees.**

Changes to Workload Security Monitoring and logging

Vulnerability assessments in cloud computing need to account for both architectural and contractual limitations:

- ❑ **The cloud owner (public or private) will typically require notification of assessments and place limits on the nature of assessments. This is because they may be unable to distinguish an assessment from a real attack without prior warning.**
- ❑ **Default deny networks further limit the potential effectiveness of an automated network assessment, just as any firewall would. You either need to open up holes to perform the assessment, use an agent on the instance to perform the assessment, or assess knowing that a lot of tests are blocked by the firewall rules.**
- ❑ **Assessments can be run during the image creation process for immutable workloads. Since these aren’t in production, and the process is automated, they can run with fewer network restrictions, thus increasing the assessment surface.**
- ❑ **Penetration testing is less affected since it still uses the same scope as an attacker.**

Changes to Workload Security Monitoring and logging

Vulnerability assessments in cloud computing need to account for both architectural and contractual limitations:

- **The cloud owner (public or private) will typically require notification of assessments and place limits on the nature of assessments. This is because they may be unable to distinguish an assessment from a real attack without prior warning.**
- **Default deny networks further limit the potential effectiveness of an automated network assessment, just as any firewall would. You either need to open up holes to perform the assessment, use an agent on the instance to perform the assessment, or assess knowing that a lot of tests are blocked by the firewall rules.**
- **Assessments can be run during the image creation process for immutable workloads. Since these aren’t in production, and the process is automated, they can run with fewer network restrictions, thus increasing the assessment surface.**
- **Penetration testing is less affected since it still uses the same scope as an attacker.**