UNIVERSIDADE
BEIRA INTERIOR

Virtual Networking in Virtual Data Centers and Clouds

Tecnologias de Virtualização e Centros de Dados

Mestrado em Engenharia Informática

Alexandre Fonte
alexandre.fonte@ubi.pt
(Professor Convidado)
Departamento de Informática

Ano Letivo 2023/2024

Sumário

- Virtual Networking in Virtual Data Centers
  - Overview of network virtualization
  - Overview of network that is virtualized
  - Virtualization tools that enable network virtualization
  - Benefits of network virtualization
  - VDC network infrastructure and components
  - Virtual LAN (VLAN) and Virtual SAN (VSAN) and their benefits

- Estes slides são parcialmente baseados em alguns documentos públicos da EMC2.

Versão: 29 abril de 2022

Network Virtualization

Network Virtualization

It is a process of logically segmenting or grouping physical network(s) and making them operate as single or multiple independent network(s) called "Virtual Network(s)".

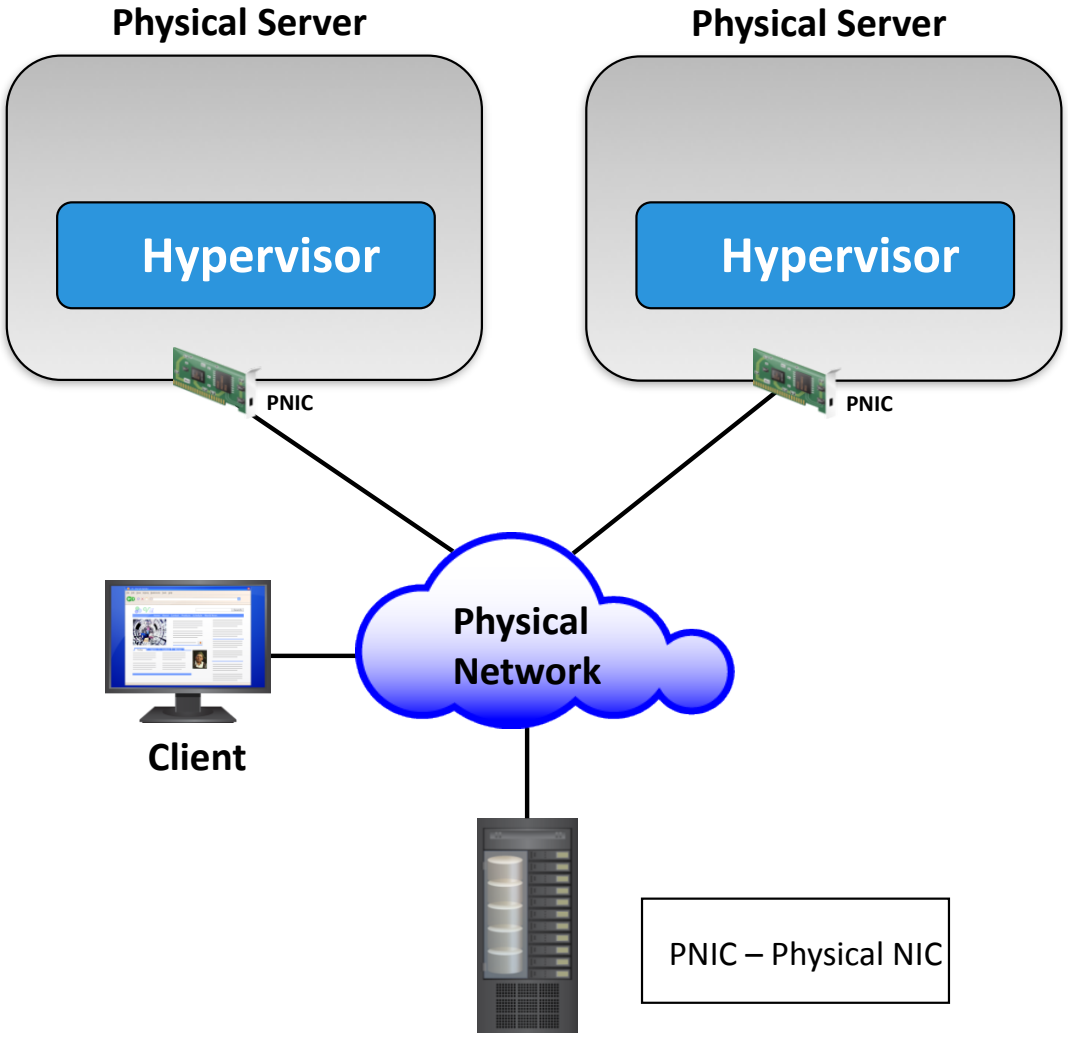
- Enables virtual networks to share network resources
- Allows communication between nodes in a virtual network without routing of frames
- Enforces routing for communication between virtual networks
- Restricts management traffic, including 'Network Broadcast', from propagating to other virtual network
- Enables functional grouping of nodes in a virtual network

Network Virtualization in VDC

- Involves virtualizing physical and VM networks

Physical Network

- Consists of following physical components:
  - Network adapters, switches, routers, bridges, repeaters, and hubs
- Provides connectivity
  - Among physical servers running hypervisor
  - Between physical servers and clients
  - Between physical servers and storage systems

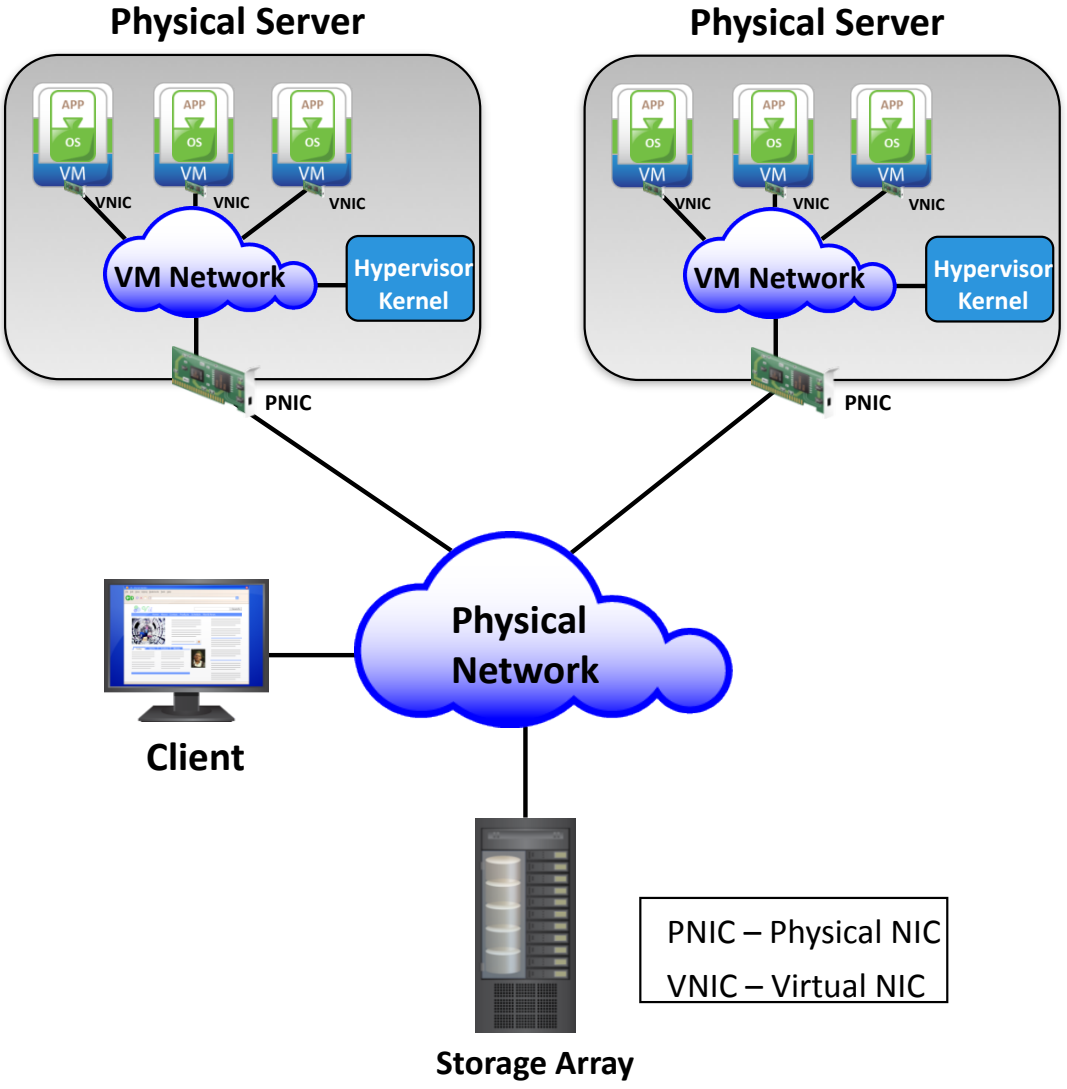


Network Virtualization in VDC (contd.)

- Involves virtualizing physical and VM networks

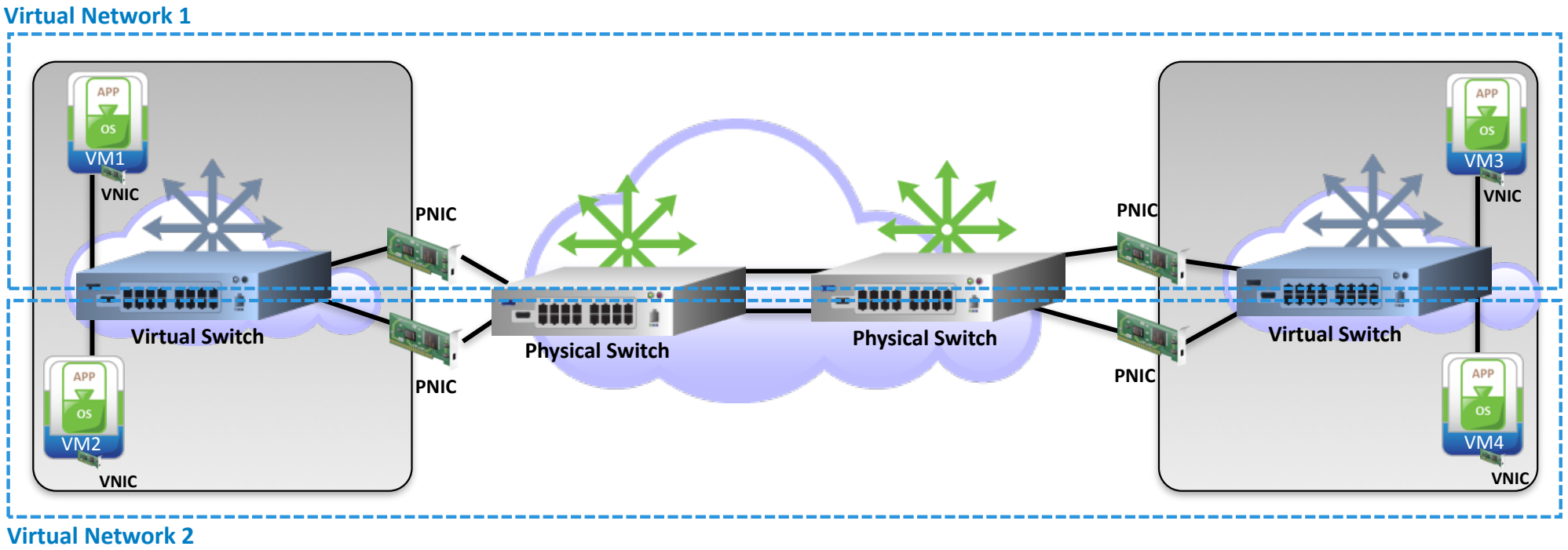
VM Network

- Resides inside physical server
- Consists of logical switches called “virtual switches”
- Provides connectivity among VMs inside a physical server
- Provides connectivity to Hypervisor kernel
- Connects to physical network



Network Virtualization in VDC (contd.)

- VM and physical networks are virtualized to create virtual networks; for example: virtual LAN, virtual SAN



Network Virtualization tools

- Physical switch Operating System (OS)
  - OS must have network virtualization functionality
- Hypervisor
  - Uses built-in networking and network virtualization functionalities
    - To create virtual switch and configuring virtual networks on it
  - Or, uses third-party software for providing networking and network virtualization functionalities
    - Third-party software is installed onto the hypervisor
    - Third-party software replaces the native networking functionality of the hypervisor

Benefits of Network Virtualization

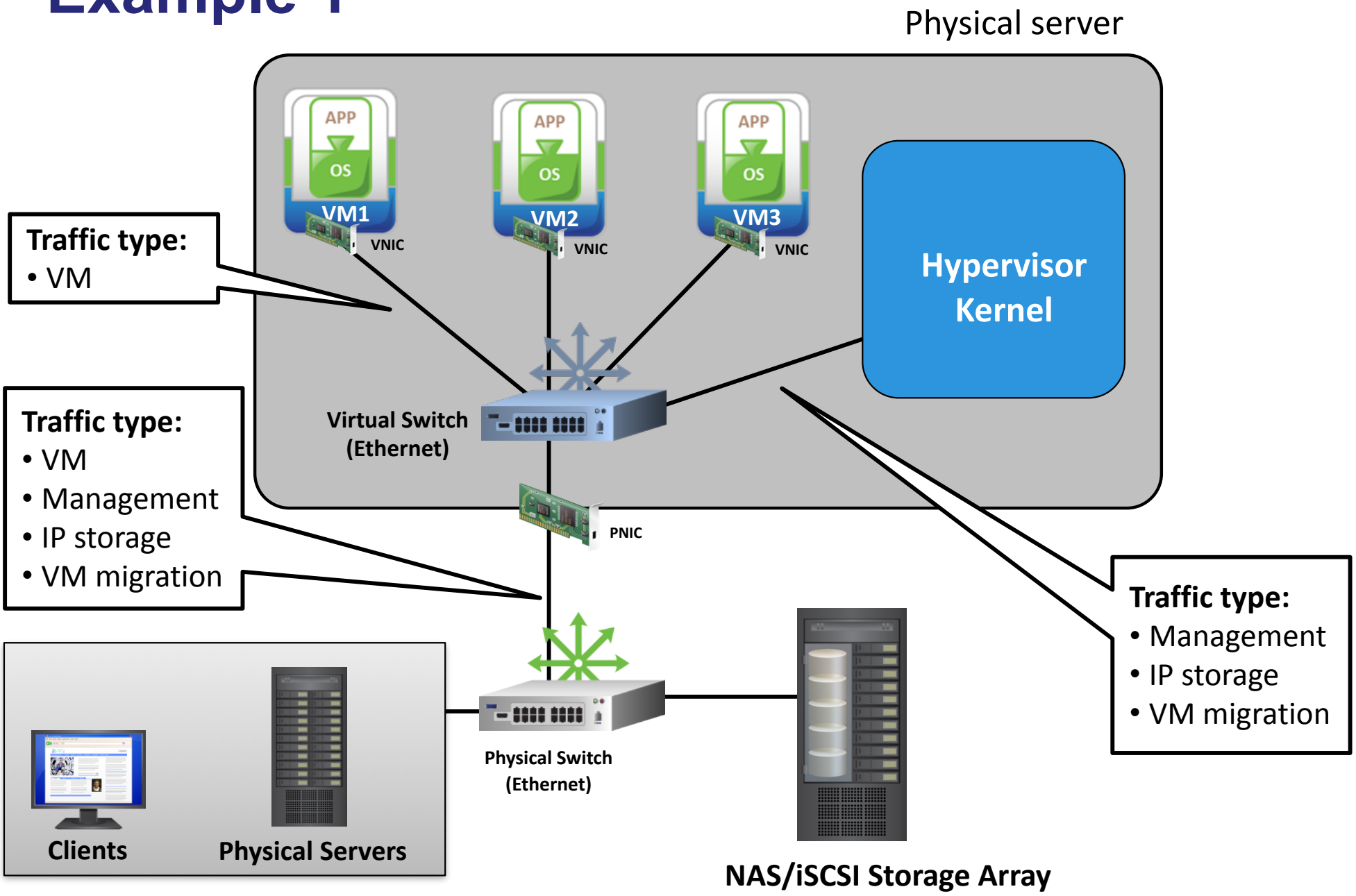
Benefit	Description
Enhances security	• Restricts access to nodes in a virtual network from another virtual network • Isolates sensitive data from one virtual network to another
Enhances performance	• Restricts network broadcast and improves virtual network performance
Improves manageability	• Allows configuring virtual networks from a centralized management workstation using management software • Eases grouping and regrouping of nodes
Improves utilization and reduces CAPEX	• Enables multiple virtual networks to share the same physical network, which improves utilization of network resource • Reduces the requirement to setup separate physical networks for different node groups

VDC Network Infrastructure

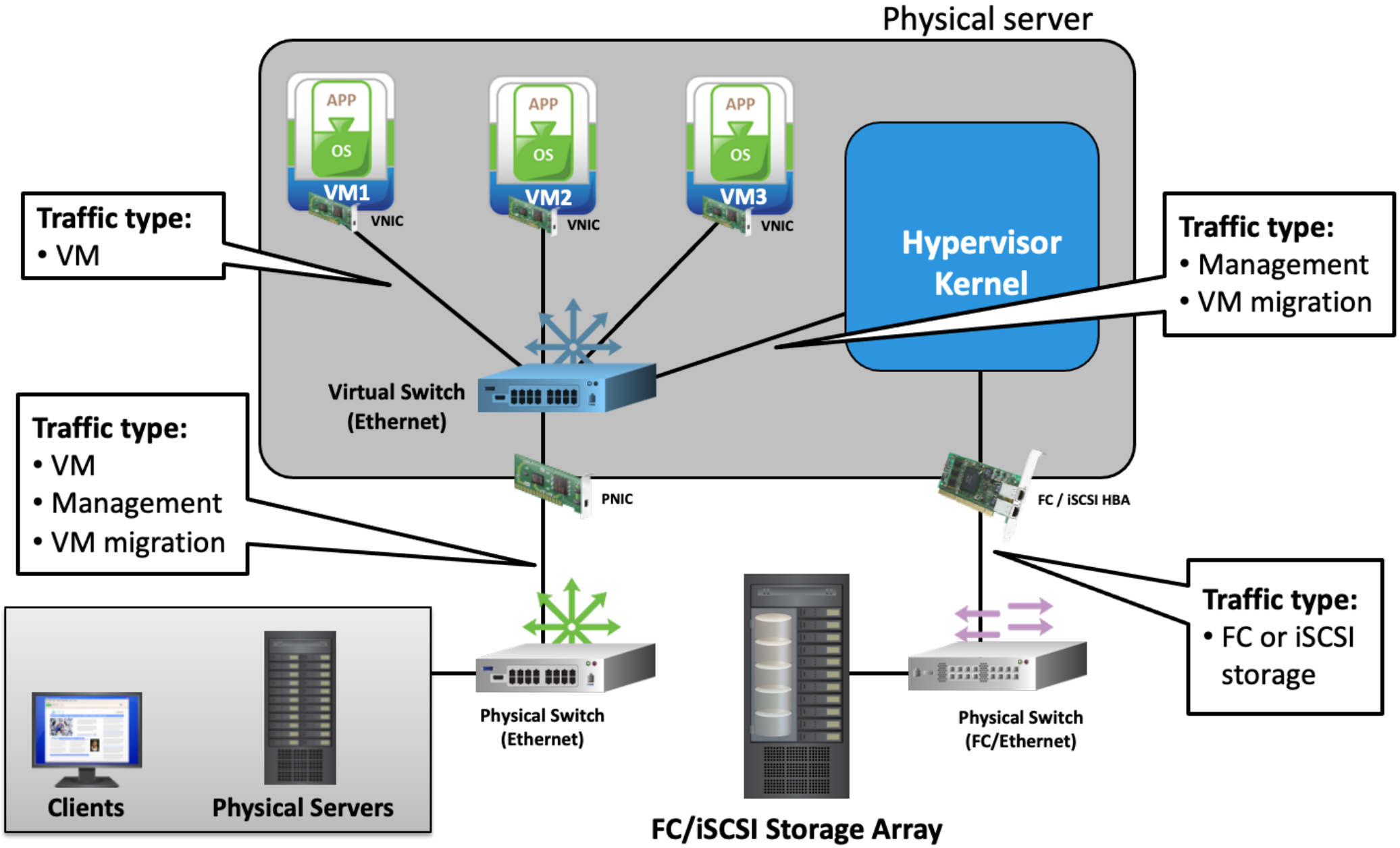
- Components of VDC Network Infrastructure
  - -VDC network infrastructure includes both virtual and physical network components
  - -Components are connected to each other to enable network traffic flow

Component	Description
Virtual NIC	• Connects VMs to the VM network • Sends/receives VM traffic to/from VM network
Virtual HBA	• Enables a VM to access FC disk/LUN assigned to the VM
Virtual switch	• Is an Ethernet switch that forms VM network • Provides connection to virtual NICs and forwards VM traffic • Provides connection to hypervisor kernel and directs hypervisor traffic: management, storage, VM migration
Physical adapter: NIC, HBA, CNA	• Connects physical servers to physical network • Forwards VM and hypervisor traffic to/from physical network
Physical switch, router	• Forms physical network that supports Ethernet/FC/iSCSI/FCoE • Provides connections among physical servers, between physical servers and storage systems, and between physical servers and clients

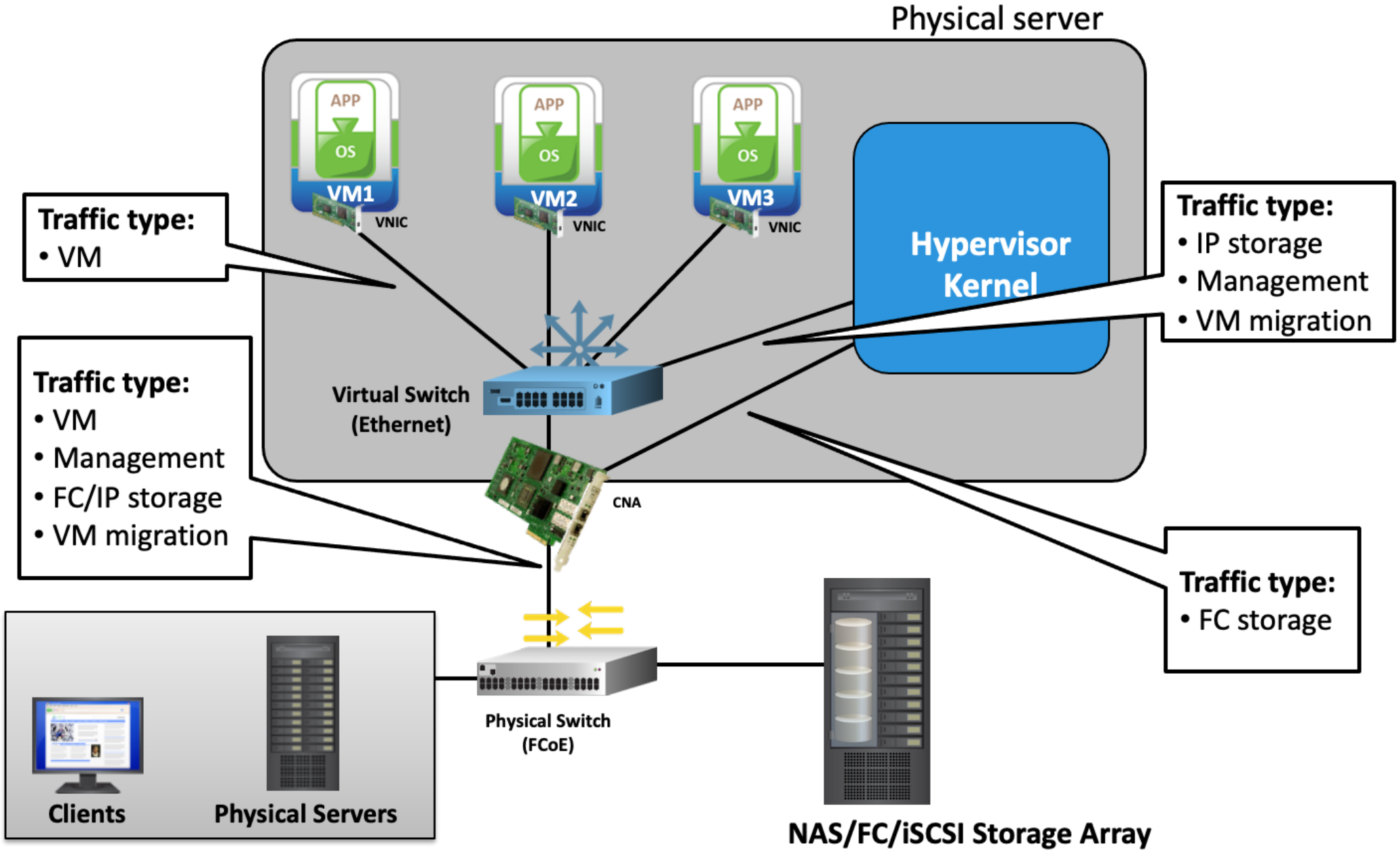
Network Connectivity and Traffic Flow: Example 1



Network Connectivity and Traffic Flow: Example 2



Network Connectivity and Traffic Flow: Example 3

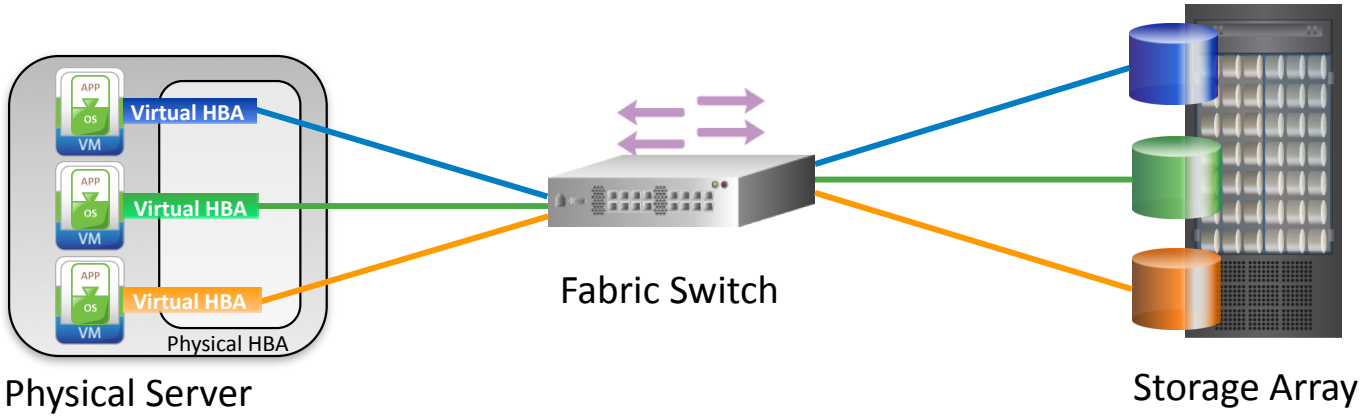


Virtual Network Component: Virtual NIC

- Connects VMs to virtual switch
- Forwards Ethernet frames to virtual switch
- Has unique MAC and IP addresses
- Supports Ethernet standards similar to physical NIC

Virtual Network Component: Virtual HBA

- Enables a VM to access FC disk/LUN assigned to the VM

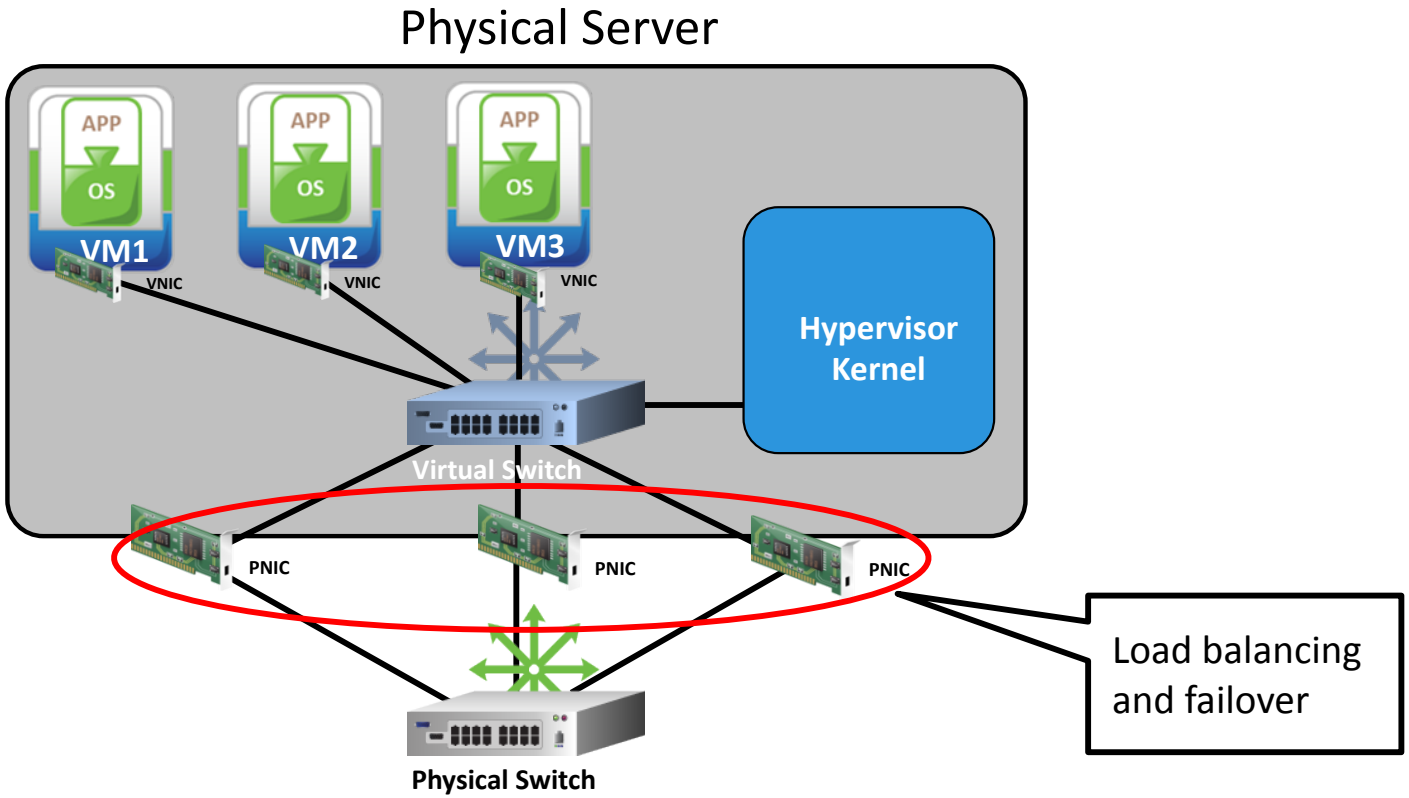


Virtual Network Component: Virtual Switch

- Is a logical OSI layer 2 switch that supports Ethernet protocol
- Resides inside a physical server
- Is created and configured using hypervisor
- Maintains MAC address table for frame forwarding
- Directs network traffic to/from VMs and hypervisor kernel
  - -VM to VM within physical server
  - -VM to physical network
  - -Hypervisor kernel: IP storage, VM migration, and management

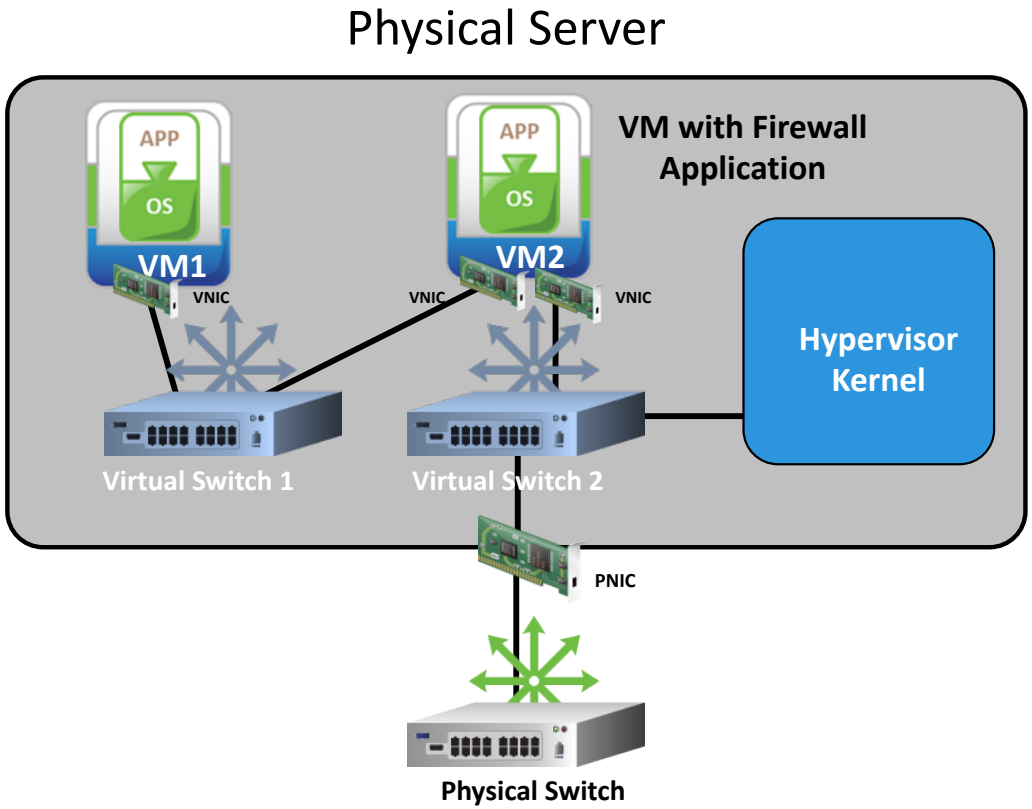
Virtual Network Component: Virtual Switch

- May connect to multiple physical NICs
  - Connection to multiple NICs performs load balancing and failover



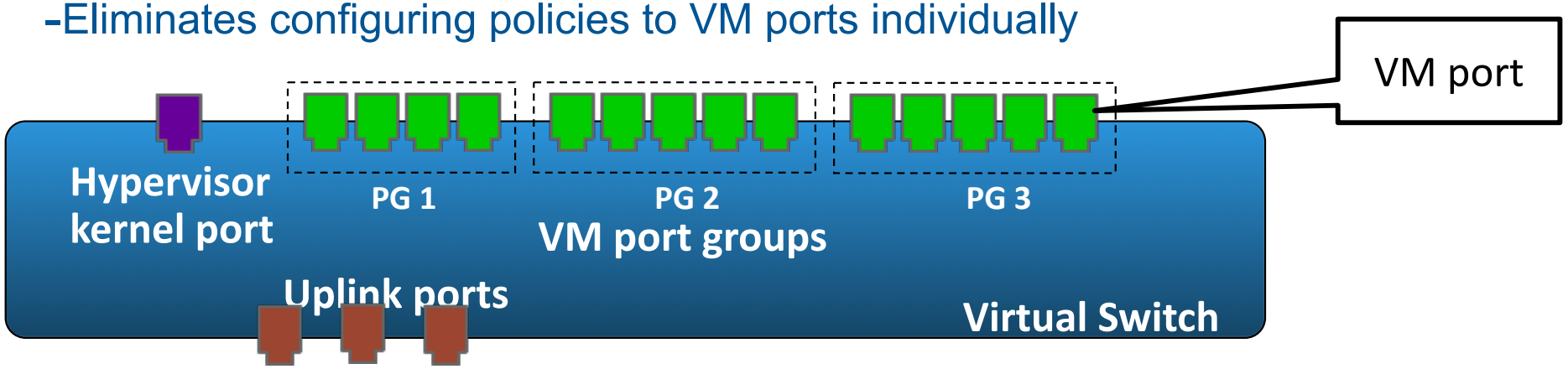
Virtual Network Component: Virtual Switch (contd.)

- May have no connection to any physical NIC
  - If virtual switch has no connection to physical NIC, it directs VM traffic within the physical server



Virtual Switch: Ports and Port Group

- Types of ports
  - -Hypervisor kernel port: Provides connectivity to hypervisor kernel
  - -VM port: Provides connectivity to virtual NICs
  - -Uplink port: Provides connectivity to physical NIC
- VM port group: Mechanism for applying uniform network policy settings to a group of VM ports
  - -Policy example: Security, load balancing, and failover across PNICs
- VMs connected to a VM port group share common configuration
  - -Eliminates configuring policies to VM ports individually

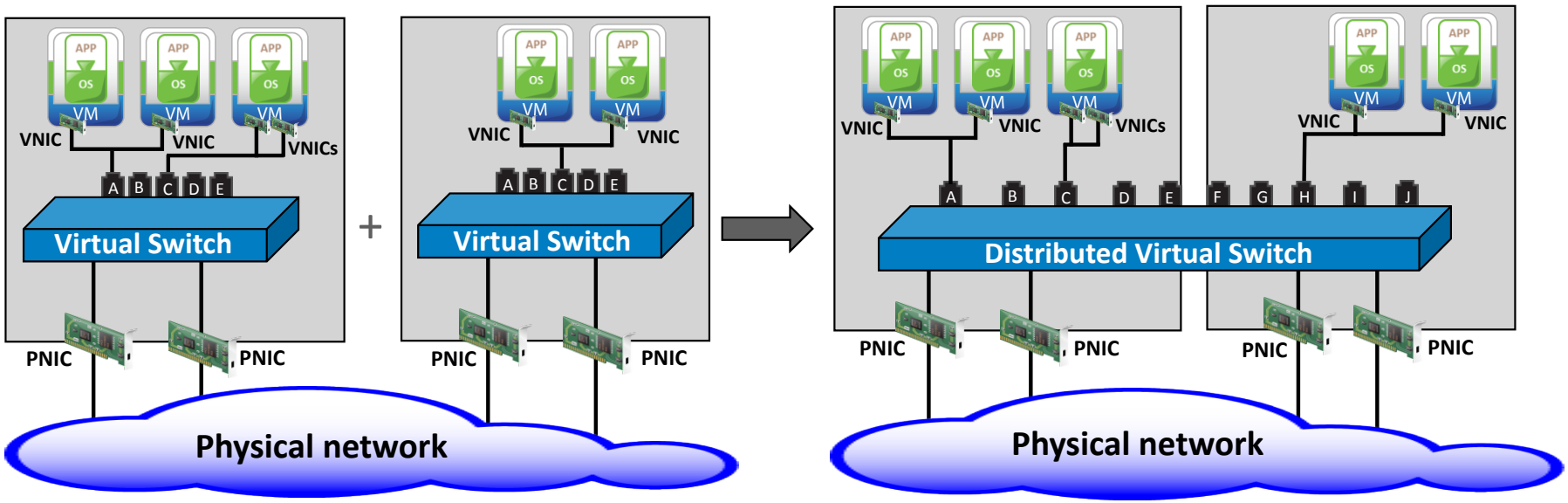


Distributed Virtual Switch

- Aggregation of multiple virtual switches distributed across multiple physical servers

Benefit

- Centralizes VM network management
- Maintains network policies during VM migration



Physical Network Component: NIC

- Physical NICs are used as inter-switch-links between virtual and physical Ethernet switches
  - -Transfer VM and hypervisor kernel traffic
- **Physical NICs are not addressable from network**
  - -IP address not assigned (prohibits OSI layer 3 access)
  - -MAC addresses not available (prohibits OSI layer 2 access)
- Virtual NIC and hypervisor kernel are addressable from network
  - -Have their own MAC and IP addresses
    - •Are used as source address in Ethernet frames
- Ethernet frames are transferred through physical NICs without modification

Physical Network Component: HBA and CNA

Type of Adapter	Description
iSCSI HBA	• Transfers hypervisor storage I/Os (SCSI I/Os) to iSCSI storage systems •Has built-in iSCSI initiator • Encapsulates SCSI I/O into iSCSI frames and then encapsulates iSCSI frames into Ethernet frames • Uses its own MAC and IP addresses for transmission of Ethernet frames over the Ethernet network • Offloads iSCSI processing (SCSI to iSCSI) from hypervisor
FC HBA	•Transfers hypervisor storage I/Os (SCSI I/Os) to FC storage systems • Encapsulates SCSI data into FC frame • Uses its own FC address for transmission of frames over FC network
CNA	•Hypervisor recognizes as an FC HBA and as an NIC ▸ NIC : Used as a link between virtual and physical switches ▸ FC HBA : Provides hypervisor access to the FC storage

Virtual Local Area Network (VLAN)

VLAN

A logical network, created on a LAN or across LANs consisting of physical and virtual switches, enabling communication among a group of nodes, regardless of their location in the network.

Benefit

- Controls broadcast activity and improves network performance
- Simplifies management
- Increases security levels
- Provides higher utilization of switch and reduces CAPEX

Configuring VLAN

- Define VLAN IDs on physical switch
  - Each VLAN is identified by a unique number: VLAN ID
- Choose necessary VLAN IDs from hypervisor's built-in VLAN ID pool
  - Required for virtual switches
- Assign VLAN ID to physical and virtual switch ports
  - To include switch ports to a VLAN
  - To enable grouping of switch ports into VLANs

Configuring VLAN (contd.)

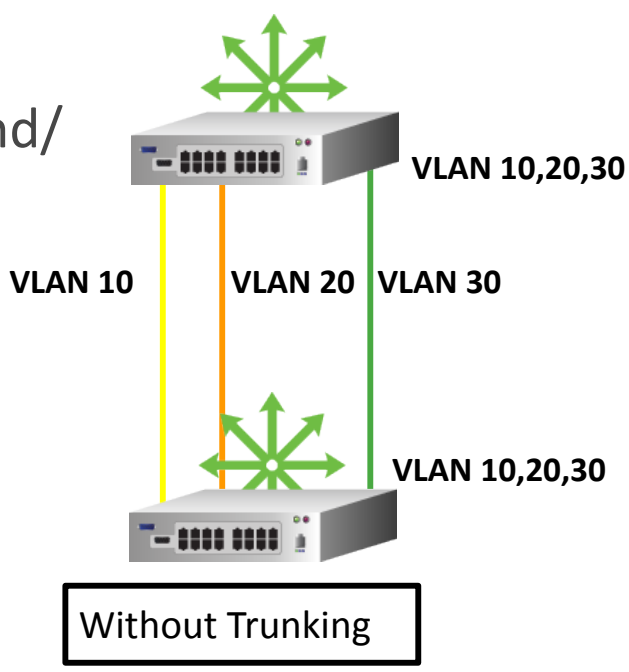
- Nodes become VLAN members when connected to VLAN ports
- Switch forwards frames between switch ports that belong to common VLAN
- VLAN traffic is transferred through routers
  - During inter VLAN communication
  - When VLAN spans different IP networks
- VM and storage systems may be members of multiple VLANs
  - Requires support of respective operating system

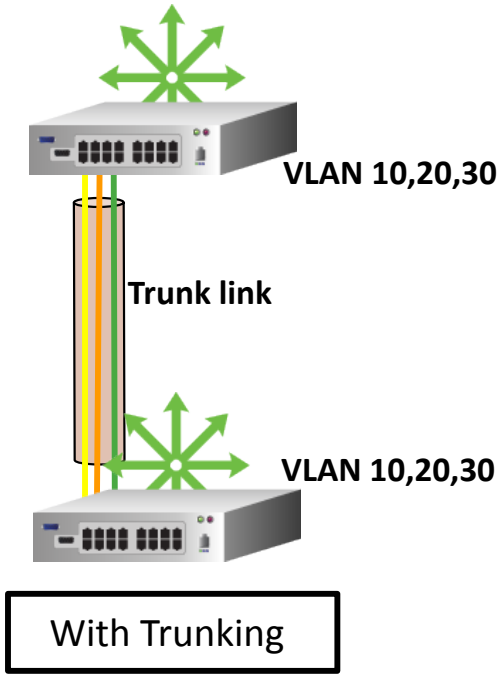
VLAN Trunking

VLAN Trunking

It is a technology that allows traffic from multiple VLANs to traverse a single network connection

- Single connection (Trunk link) carries multiple VLAN traffic
- Single port (Trunk port) to send/ receive multiple VLAN traffic over trunk link
- Trunk port is included to all VLANs
- VLAN trunking is enabled by tagging Ethernet frames





Benefits of VLAN Trunking

- Eliminates the need for dedicated network link(s) for each VLAN
- Reduces inter-device links when the devices have more than one VLAN
  - Reduces the number of virtual NICs, storage ports, and switch ports
  - Reduces management complexity

VLAN Tagging

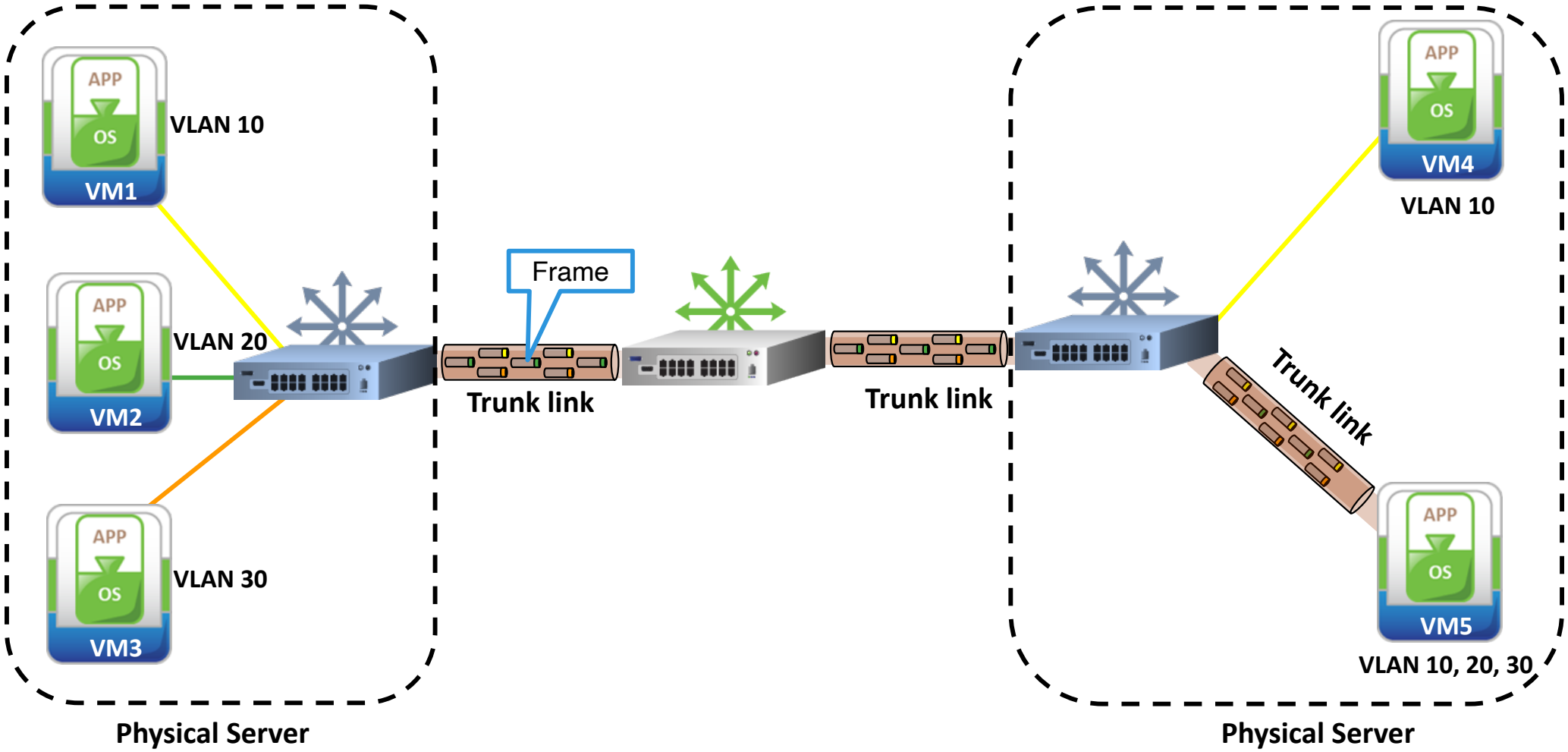
VLAN Tagging

It is a process of inserting or removing a marker (tag) with VLAN-specific information (VLAN ID) into the Ethernet frame

- Supported sending device inserts tag field in the Ethernet frame before sending to a trunk link
- Supported receiving device removes tag and forwards to the interface tied to a VLAN
- Trunk ports transfer and receive tagged frames

VLAN Tagging

- Sales group: Includes VM1, VM4, and VM5
- Finance group: Includes VM2 and VM5
- Marketing group: Includes VM3 and VM5



Sumário

- Redes Virtuais na Cloud
  - Principais Componentes

Referências:

https://devblogs.microsoft.com/premier-developer/differentiating-between-azure-virtual-network-vnet-and-aws-virtual-private-cloud-vpc/

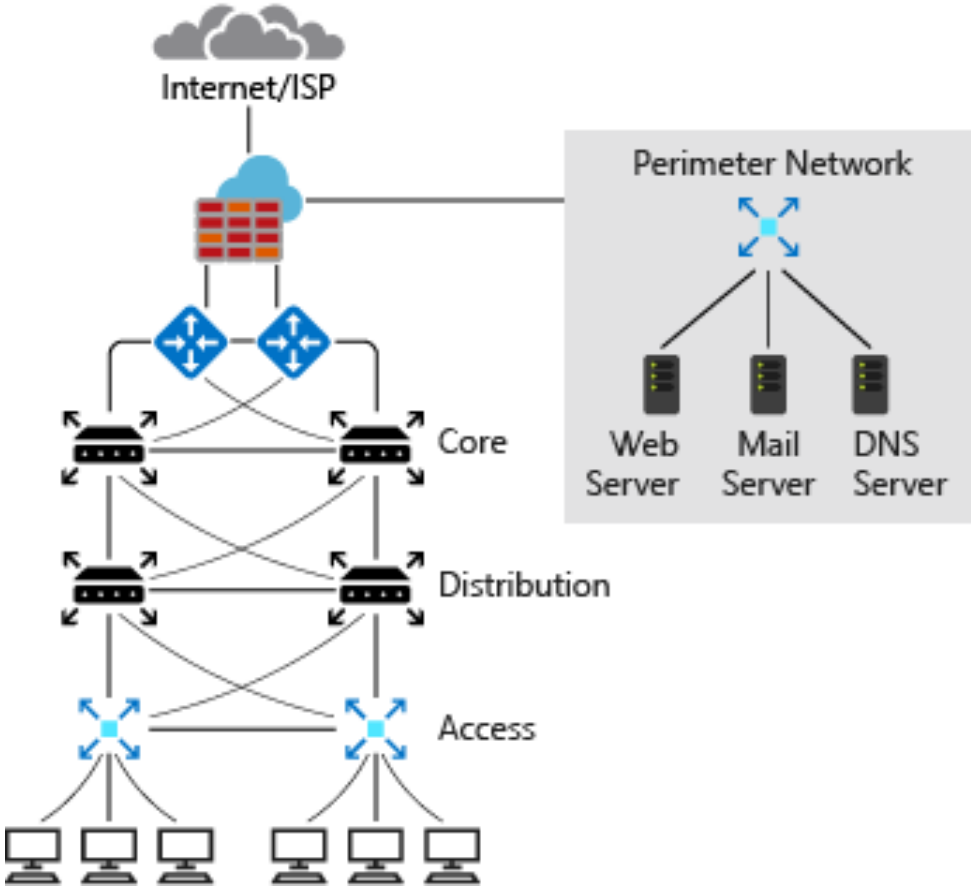
https://www.whizlabs.com/blog/amazon-elastic-load-balancer-vs-azure-load-balancer/

https://docs.microsoft.com/pt-pt/azure/virtual-network/

Versão: 29 abril de 2022

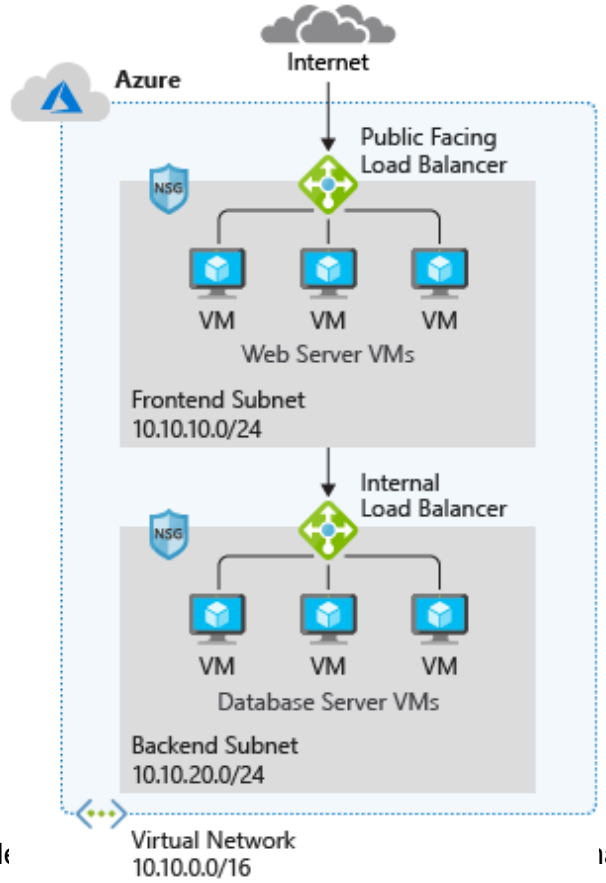
Modelo das Redes On-Premise (locais)

- Modelo Hierárquico organizados em 3 camadas
- Um esquema típico de rede local inclui os seguintes componentes:
  - Routers
  - Firewalls
  - Switches
  - VLANs (segmentação de rede)



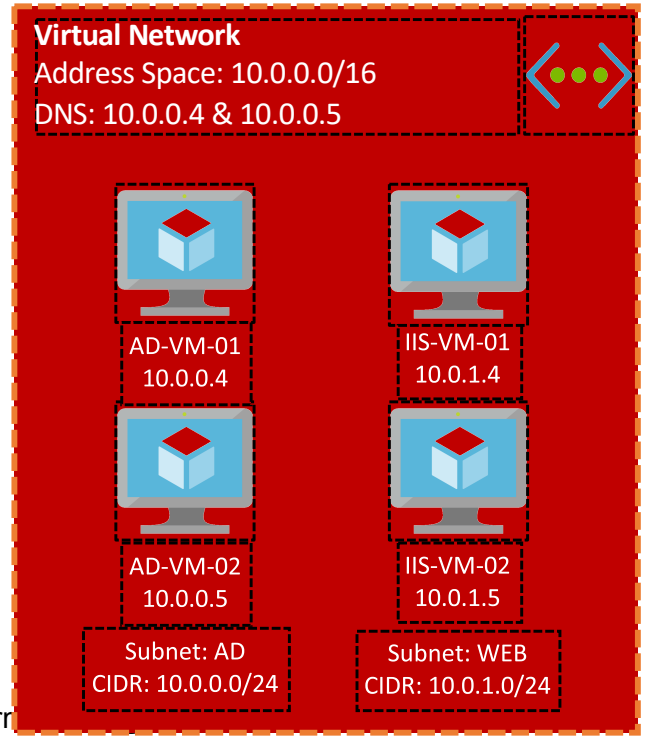
Modelo das Redes Virtuais em Cloud

- Uma Rede Virtual é um componente essencial para agrupar, isolar e proteger os recursos num ambiente de rede na Cloud.
- O design de rede tem recursos e funções semelhantes a uma rede local, mas a estrutura da rede é diferente.
- A rede em Cloud não seguem o design de rede hierárquica local típico.
- Não há dispositivos de hardware, como routers ou switches ou firewalls. Toda a infraestrutura de rede é virtual.



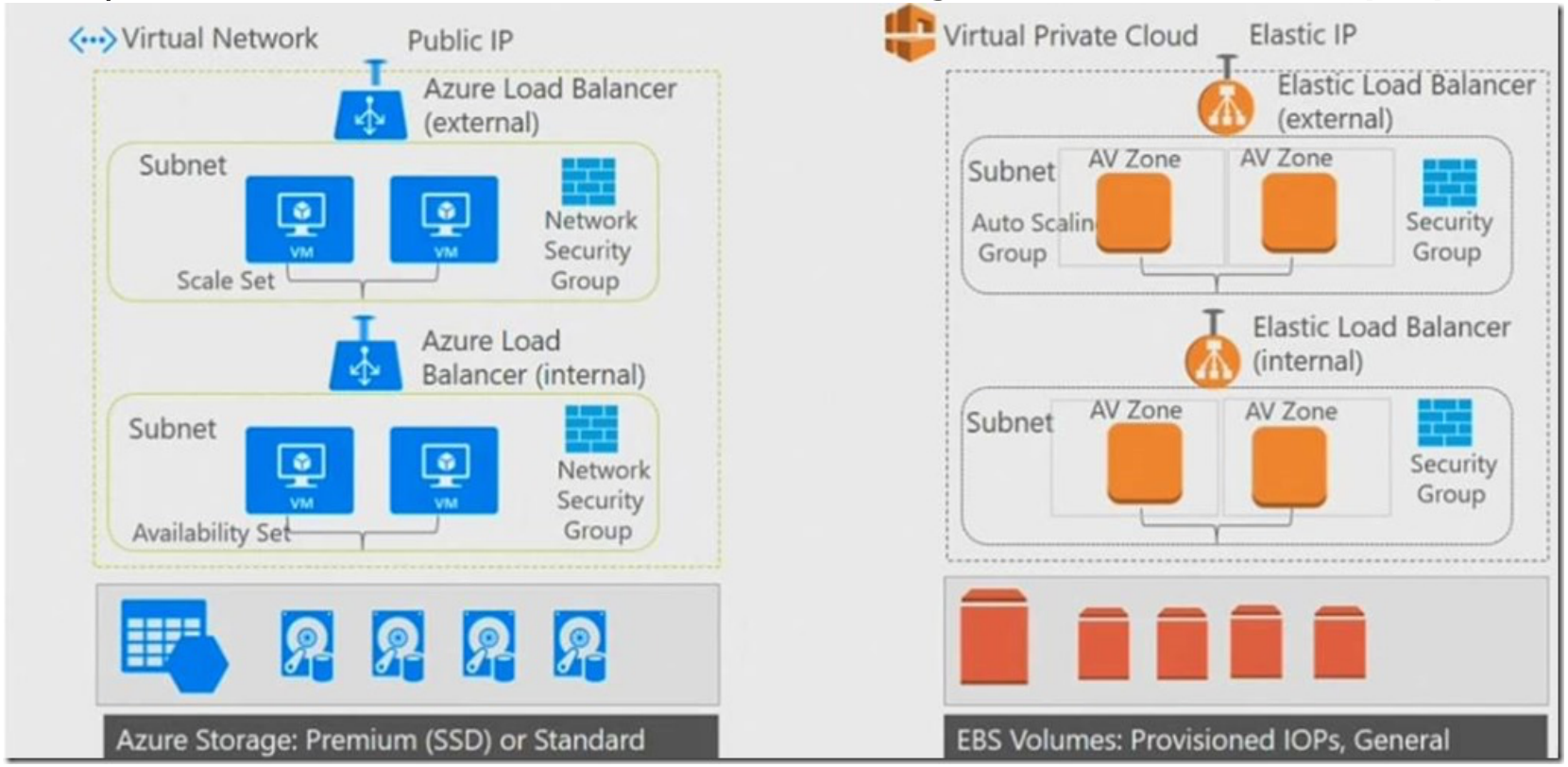
Redes Virtuais na Cloud

- Uma Rede Virtual é um componente essencial para agrupar, isolar e proteger os recursos num ambiente de rede na Cloud.
- Uma rede privada permite a ligação entre os recursos Cloud (e.g., VMs, EC2 ou Bases de Dados), à Internet e outras redes privadas.
  - Isolamento lógico com controle sobre a rede
  - Criação de sub-redes e isolamento do tráfego usando grupos de segurança de rede e appliances de segurança
  - Suporte para endereços IP estáticos
  - Suporte para balanceamento de carga
  - Suporte DNS
  - Suporte de conectividade híbrida
    - Site-to-Site
    - Point-to-Site



Virtual Private Networking entre recursos Cloud

- As VMs e os recursos computacionais Cloud devem poder comunicar com segurança uns com os outros.
- As plataformas Cloud devem oferecer este tipo de serviço de camada de Infraestrutura ou IaaS.
- Amazon Virtual Private Cloud (VPC) e Azure Virtual Network (VNet) são dois dos *cloud networking services* mais populares.



Sumário dos Principais Blocos Construtores das Redes Virtuais

- **Espaço de endereço:** ao criar uma AWS VPC ou VNet, é preciso especificar um espaço de endereço IP de uma gama globalmente não encaminhável CIDR especificada na RFC 1918.
- O Azure ou AWS atribui aos recursos (e.g., VM Windows) numa rede virtual um endereço IP privado do espaço de endereçamento definido.
- Por exemplo, ao implantar-se uma VM numa VNet com espaço de endereço, 10.0.0.0/16, a VM receberá do Azure um IP privado como 10.0.0.4. Nota: O Azure não permite a implantação de um servidor DHCP numa VNET.
- A menor subrede Azure é /29 enquanto a maior é /8. No caso da AWS o menor bloco é /28 e o maior é /16. As sub-redes IPv6 devem ter exatamente /64 de tamanho. Alguns endereços estão reservados (GW padrão, servidores DHCP e DNS).
- O Azure permite acesso direto aos recursos através de um endereço público; enquanto a AWS apenas através de um Internet Gateway (IGW).

Sumário dos Principais Blocos Construtores das Redes Virtuais

- **Sub-redes:** As redes virtuais VNET e AWS VPC podem ser segmentadas numa ou mais sub-redes, e ser-lhe alocadas parte do espaço de endereço da rede virtual para cada sub-rede.
- De seguida, pode-se então implantar recursos numa sub-rede específica. Isto melhora a eficiência da alocação de endereços e o controlo de recursos implementados na Cloud.
- A menor subrede Azure é /29 enquanto a maior é /8. No caso da AWS o menor bloco é /28 e o maior é /16. As sub-redes IPv6 devem ter exatamente /64 de tamanho. Alguns endereços estão reservados (GW padrão, servidores DHCP e DNS). Exemplo caso Azure 192.168.1.0/24 has the following reserved addresses:
  - 192.168.1.0 : Network address
  - 192.168.1.1 : Reserved by Azure for the default gateway
  - 192.168.1.2, 192.168.1.3 : Reserved by Azure to map the Azure DNS IPs to the VNet space
  - 192.168.1.255 : Network broadcast address.
- Uma AWS VPC abrange todas as Zonas de Disponibilidade (AZs) nessa região, pelo que as sub-redes no AWS VPC são mapeadas para as Zonas de Disponibilidade (AZs). Mas, uma sub-rede deve pertencer apenas a uma AZ e não pode abranger as AZs.
- Uma VNET Azure não precisa de explicitamente definir as zonas de disponibilidade.

Sumário dos Principais Blocos Construtores das Redes Virtuais

- **Routing Table –** AWS utiliza uma tabela de encaminhamento para especificar as rotas para o tráfego de saída da subrede. Todas as sub-redes criadas numa rede privada VPC são automaticamente associadas à tabela de encaminhamento principal AWS permitindo o tráfego entre sub-redes, a menos que as regras de segurança o neguem explicitamente.
- De forma semelhante, a Azure VNet utiliza uma tabela de encaminhamento de sistema para assegurar que todos os recursos ligados a qualquer sub-rede em qualquer VNet comunicam entre si por defeito.
- Em resumo, não é preciso configurar e gerir rotas visto que por omissão estas plataformas Cloud fornecem de forma automática encaminhamento entre VNETs, Subnets, e com redes on-premise, inserindo rotas pré-definidas.
- No entanto, há cenários em que se pode anular e sobrepor às rotas pré-definidas.
- Para tais cenários, podem-se implementar as rotas definidas pelo utilizador (UDR) ou/e rotas BGP para encaminhamento da VNet para a rede on-premise usando uma ligação baseada num Azure VPN Gateway ou no ExpressRoute.
- O UDR pode ser usado para fornecer uma camada de segurança desviando o tráfego para algum tipo de inspecção NVA. Network virtual appliances: Um dispositivo virtual de rede (appliance) é uma VM que executa uma função de rede, como firewall, otimização de WAN ou outra função de rede.

Sumário dos Principais Blocos Construtores das Redes Virtuais

- **Segurança - Filtragem de Tráfego: Pode-se proteger recursos em sub-redes usando grupos de segurança de rede ou grupos de segurança de aplicações**, os quais filtram o tráfego de rede à entrada ou saída das sub-redes ou das interfaces das VMs, ou então filtram o tráfego à entrada ou saída de um grupo de servidores aplicacionais.
- AWS VPC provides two levels of security for resources deployed to the network.
  - **Security Groups (SG):** The Security Group is a **stateful** object that is applied at the EC2 instance level. The response traffic is automatically allowed once a traffic is allowed.
  - **Network Access Controls (NACLs):** NACLs are **stateless** filtering rules that are applied at the subnet level. It's stateless because if an ingress traffic is allowed, the response is not automatically allowed unless explicitly allowed in the rule for the subnet. NACLs operates at the subnet level by examining the traffic entering and exiting the subnet. NACLs can be used to set both Allow and Deny rules.
  - The NACL rules are numbered and evaluated in order, starting with the lowest numbered rule, to determine whether traffic is allowed in or out of any subnet associated with the network ACL. The highest number that you can use for a rule is 32766. The last rule numbered is always an asterisk, and denies traffic to the subnet.
- Azure VNet provides **Network Security Groups (NSGs)** and it combines the functions of the AWS SGs and NACLs. NSGs are **stateful** and can be applied at the subnet or NIC level. Only one NSG can be applied to a NIC, but in AWS you can apply more than one Security Group (SG) to an Elastic Network Interface (ENI).
  - Network security groups: Network security groups e application security groups podem conter várias regras de segurança de entrada e saída que permitem filtrar o tráfego de e para recursos por endereço IP de origem e destino, porta e protocolo.

Gateways para Conectividade com a Internet

- **Gateways** – Both VNet and VPC offer different gateways for different connectivity purposes.
- AWS VPC uses mostly three gateways, four, if you add the NAT gateway. AWS allows one **Internet Gateway (IGW)** to provide connectivity to the internet via IPv4 and **Egress-only Internet Gateway** for internet connectivity to resources with IPv6. In AWS, any subnet without the IGW is regarded as private subnet and have no internet connectivity without **NAT gateway** or NAT instance (AWS recommends NAT Gateway for high availability and scalability). Another AWS gateway, **Virtual Private Gateway (VPG)** allows AWS to provide connectivity from AWS to other networks via VPN or Direct Connect.
- On the non-AWS network, AWS requires Customer Gateway (CGW) on the customer side to connect to AWS VPC.
- Azure VNet provides two types of gateway namely **VPN Gateway** and **ExpressRoute Gateway**. The VPN Gateway allows encrypted traffic for VNet to VNet or VNet to on-premises location across a public connection or across Microsoft's backbone in the case of VNet to VNet VPN. However, the ExpressRoute and VPN Gateway also require a gateway subnet. The gateway subnet contains the IP addresses that the virtual network gateway services use. Azure VNET to VNET can connect natively via VPN but in AWS, such VPC to VPC requires a 3rd party NVA if the VPCs are in different regions.
- Todos os recursos numa Azure VNet podem comunicar na direção outbound com a Internet, por omissão.
- É possível a comunicação com um recurso atribuindo-lhe um endereço IP público ou através de um Load Balancer público.

Balanceadores de Carga

- **Load balancers:** Load balancing is quite an important aspect of any cloud environment with a prominent contribution to ensuring the availability of cloud-based applications for customers, end-users, and business partners. **The process ensures the distribution of workloads throughout various servers**. As the name indicates, load balancing prevents overloading of any particular server and the risks of breaking down.
- **Load balancing not only provides the assurance of high availability but also profound support for scalability.** Cloud infrastructures are generally favored for the benefits of scalability, and scaling up generally involves spinning up various virtual servers alongside running different application instances. Load balancers serve as the primary network component for the distribution of traffic throughout the new instances.
- They can also detect unavailable servers and redirect traffic from them towards the operational servers.
- **Amazon Elastic Load Balancer e Azure Load Balancer** são dois dos cloud networking services mais populares

Balanceadores de Carga

- Amazon Elastic Load Balancer
  - Users can access four different load balancers such as:
    - Application load balancer - opera na camada 7 (HTTP/HTTPs)
    - Gateway load balancer - opera na camada 3
    - Classic load balancer - legado, opera na camada 4, a amazon recomenda o sudo de um GLB / ALB / NLB
    - Network load balancer - opera na camada 4
- Azure Load Balancer
  - Users could use two types of load balancers (camada 4 (UDP/TCP)) such as:
    - Public load balancer
    - Internal load balancers
  - Microsoft also provides other load balancing options:
    - Front Door (oferta Azure de redes CDN) basically serves as an application delivery network providing global load balancing alongside services for accelerating web applications.
    - Traffic Manager is basically a DNS-based traffic load balancer that supports optimal distribution of traffic.
    - Application Gateway (L7 LB) is a web traffic load balancer that enables you to manage traffic to your web applications. Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers.

Sumário dos Principais Blocos Construtores das Redes Virtuais - Interligação de Redes Virtuais

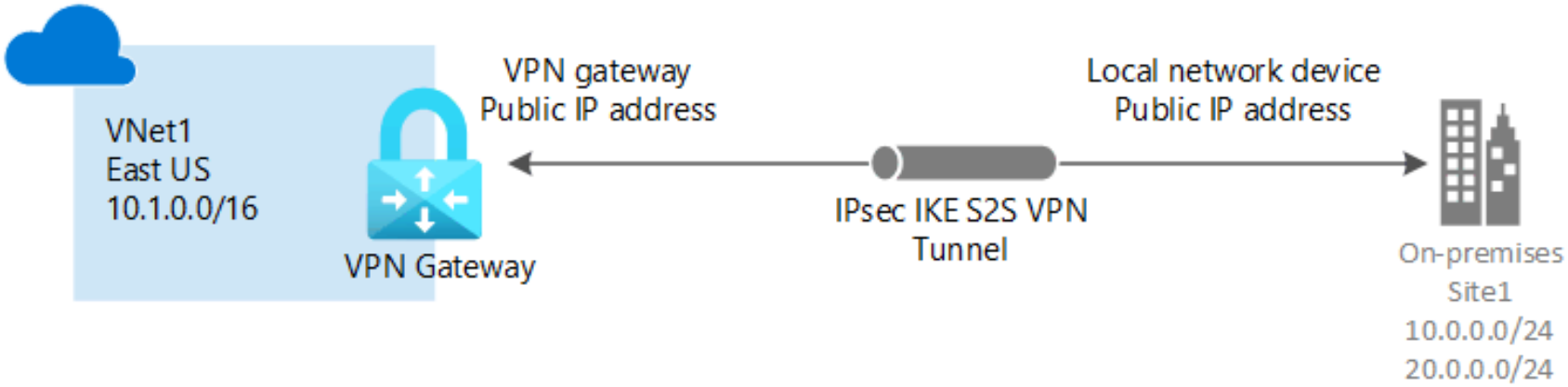
- No geral, as redes virtuais e subredes comunicam através da rede de backbone de alta velocidade (e.g., Azure ou AWS)
- **AWS**
  - **VPC peering** connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.
  - Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).
- **Azure**
  - **VNet Peering**: Podemos ligar redes virtuais entre si, permitindo que recursos numa qualquer rede virtual comuniquem entre si, usando peering de rede virtual. As redes virtuais a interligar podem estar na mesma ou em regiões diferentes do Azure.

Conectividade Híbrida entre VNETs/VPCs e os recursos on-premise

- É possível ligar os seus computadores e redes locais com uma rede virtual usando qualquer combinação das seguintes opções
- **Azure**

  -Site-to-site (S2S) VPN: Estabelecido entre seu dispositivo VPN local e um Gateway VPN do Azure que é implantado numa rede virtual. Este tipo de ligação permite que qualquer recurso local que você autorize a aceder a uma rede virtual. A comunicação entre seu dispositivo VPN local e um gateway de VPN do Azure é enviada por meio de um túnel criptografado pela Internet.

  -

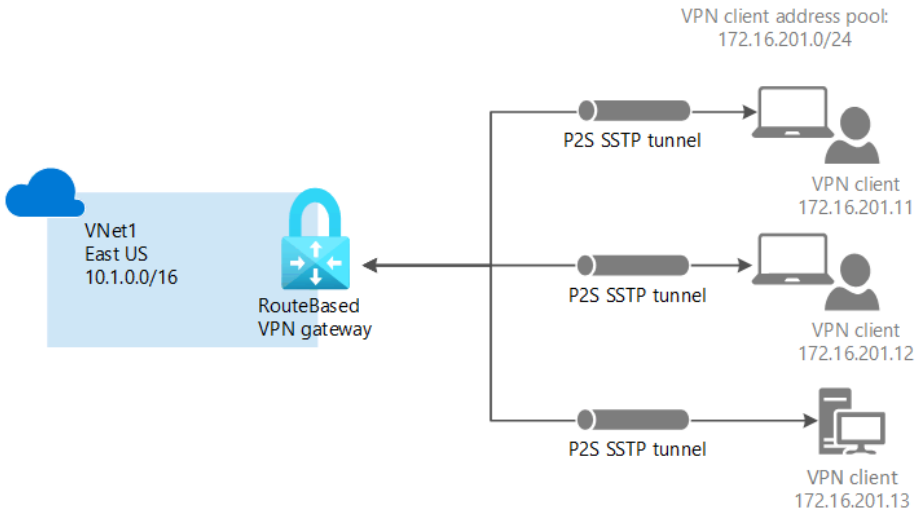


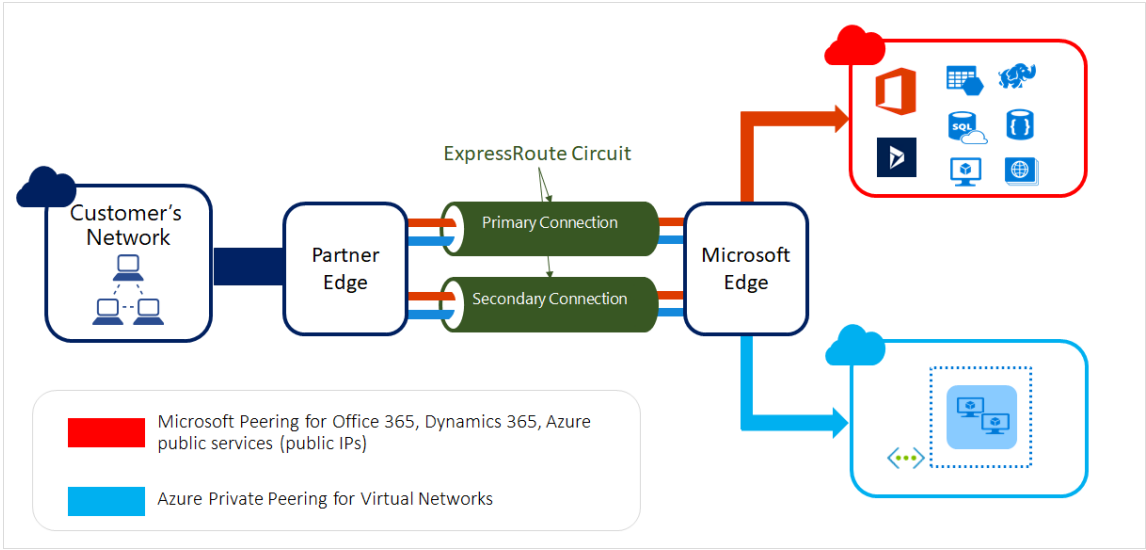
Conectividade Híbrida entre VNETs/VPCs e os recursos on-premise

- É possível ligar os seus computadores e redes locais com uma rede virtual usando qualquer combinação das seguintes opções
- **Azure**

  -Point-to-site (P2S) virtual private network (VPN): Estabelecido entre uma rede virtual e um computador. Este tipo de ligação é óptimo se estiver apenas a começar com o Azure, ou para programadores, porque requer poucas ou nenhumas alterações à sua rede existente. A comunicação entre o seu computador e uma rede virtual é enviada através de um túnel encriptado através da Internet.

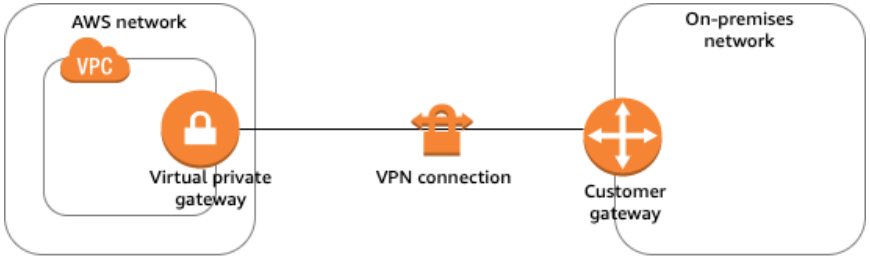
  -Azure ExpressRoute: Estabelecida entre sua rede e o Azure, por meio de um parceiro ExpressRoute. Esta ligação é privada. O tráfego não passa pela Internet. Para saber mais, consulte ExpressRoute.

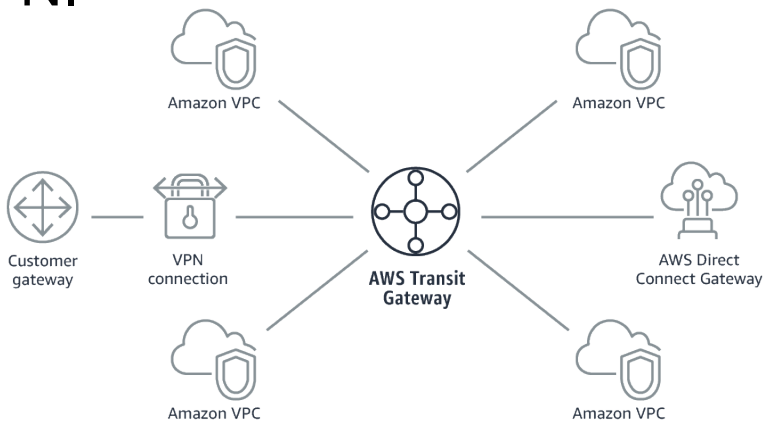




Conectividade Híbrida entre VNETs/VPCs e os recursos on-premise

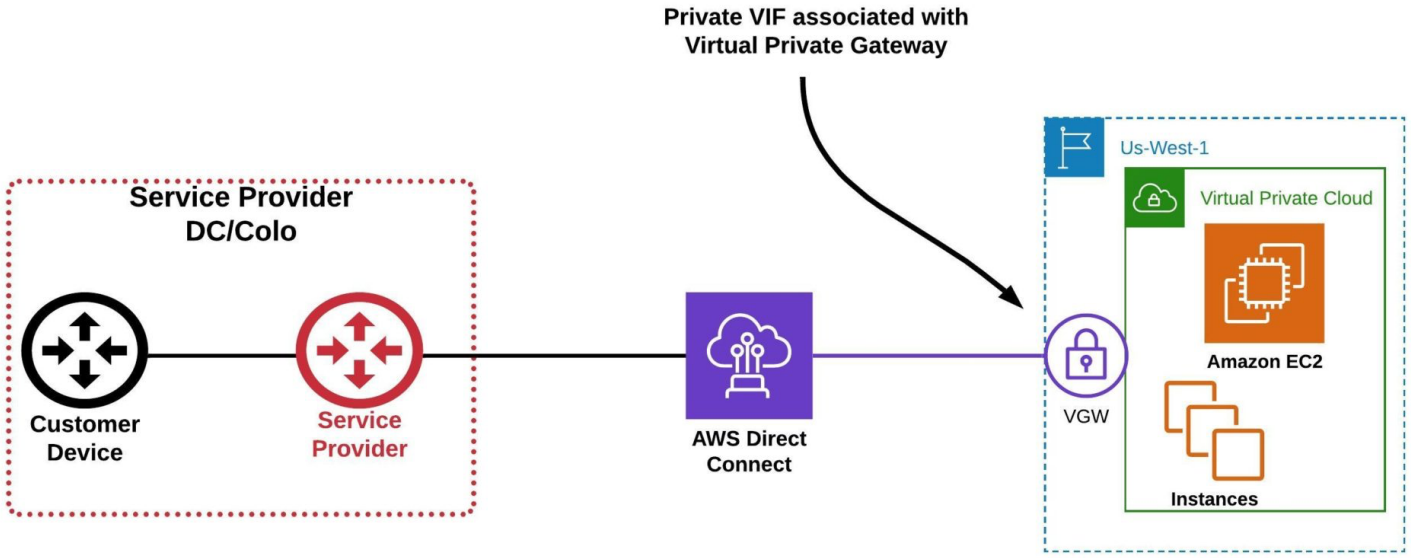
- **AWS**
- Virtual Private Gateway (VPG) allows AWS to provide connectivity from AWS to other networks via VPN or Direct Connect.
- On the non-AWS network, AWS requires Customer Gateway (CGW) on the customer side to connect to AWS VPC.
- Um solução que facilita a gestão de múltiplas ligações é a utilização de um AWS transit gateway que permite a conectividade através de um Hub Central.
- A AWS disponibiliza também uma soluções de conectividade P2S usando o AWS VPN Client ou OpenVPN.





Conectividade Híbrida entre VNETs/VPCs e os recursos on-premise

- **AWS (Cont.)**
- A AWS disponibiliza também uma solução de conectividade semelhante ao Azure ExpressRoute, a AWS Direct Connect



Pricing Azure VNETs, AWS VPCs and VNET peering / VPC Peering

- *Pricing*
  - Não há cobrança pode usar a VNet do Azure, é gratuita. Até um máximo de 50 por subscrição.
  - VNET peering é taxada pelas transferências inbound e outbound nas extremidades.
  - Não há qualquer custo para criar uma VPC ou uma ligação de peering VPC. Tal como no Azure, há uma taxa pela transferência de dados através de ligações de peering.

Questões