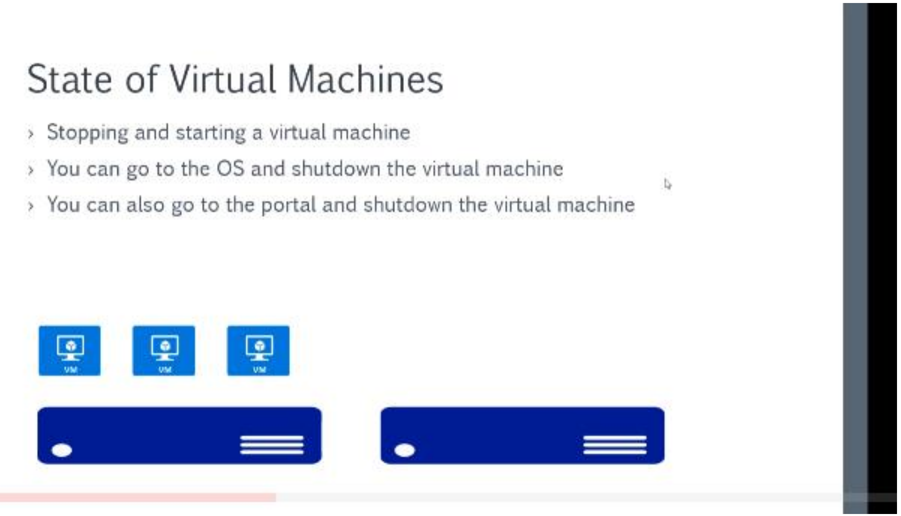
Cloud n Loud

(C)LOUD YOUR DREAMS

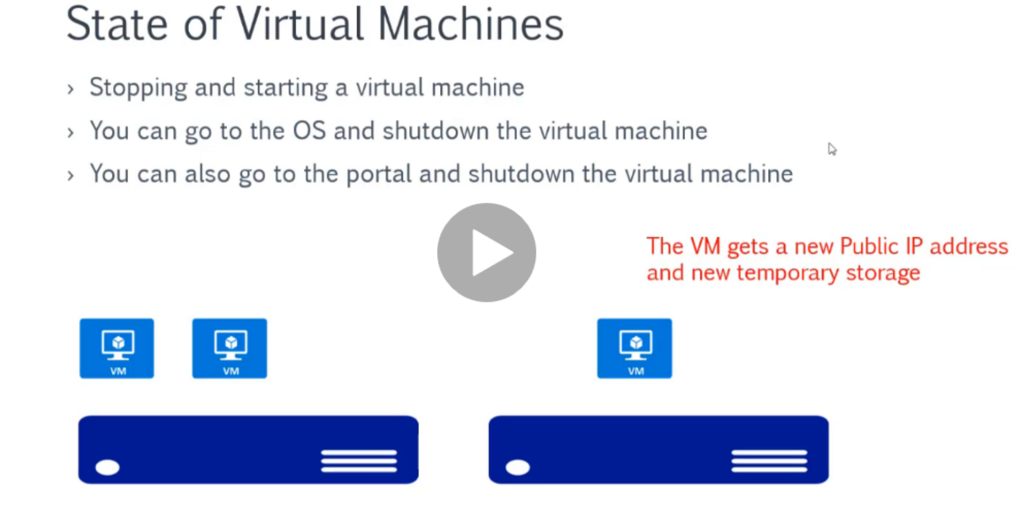
Want to Loud in AZURE Cloud

PRESENTED BY: Cloudnloud Team



State of Virtual Machines

- Stopping and starting a virtual machine
- You can go to the OS and shutdown the virtual machine
- You can also go to the portal and shutdown the virtual machine



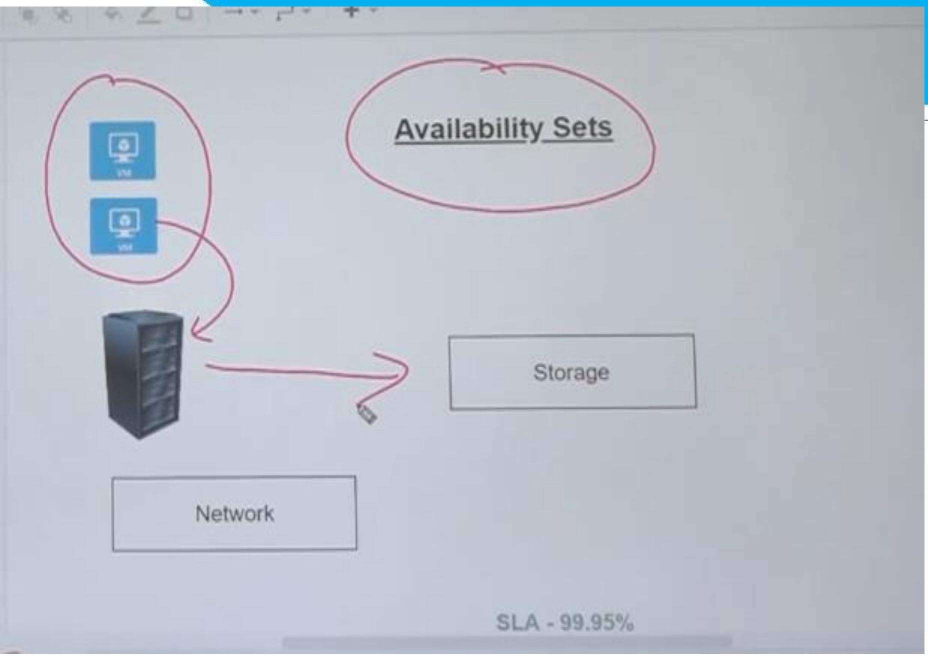
State of Virtual Machines

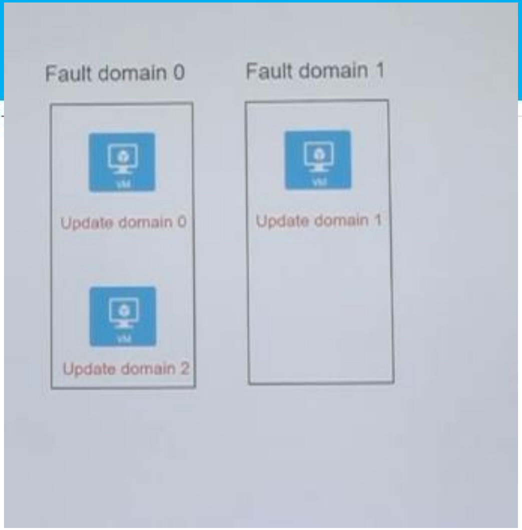
- Stopping and starting a virtual machine
- You can go to the OS and shutdown the virtual machine
- You can also go to the portal and shutdown the virtual machine

The VM gets a new Public IP address and new temporary storage

If you shutdown the machine via portal.azure.com then next time when u start it may start from different physical hosts and come with different public IP

If you go to OS and poweroff then the VM never go to any other physical host also public IP will be remain the same.



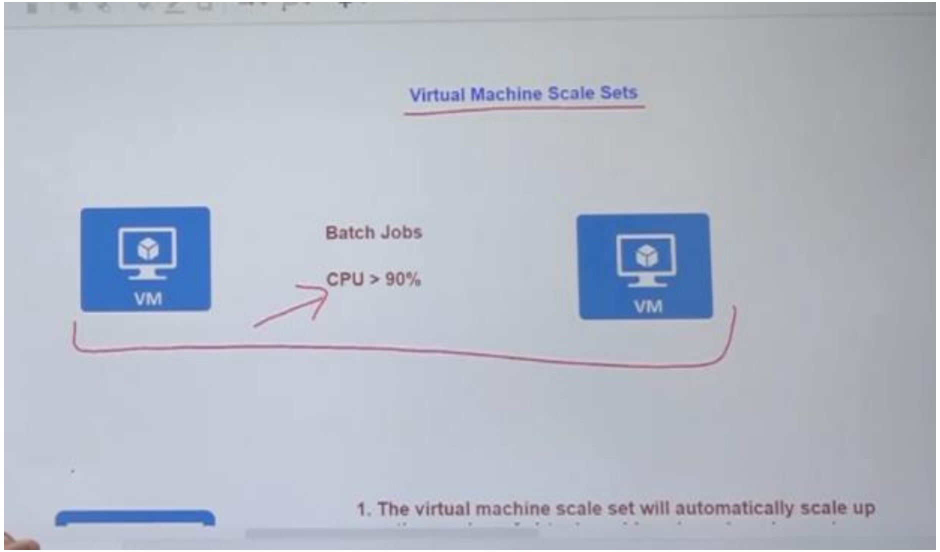


Availability set having 2 parts → 1. fault domain 2. Update domain

Fault domain is complete separate hardware

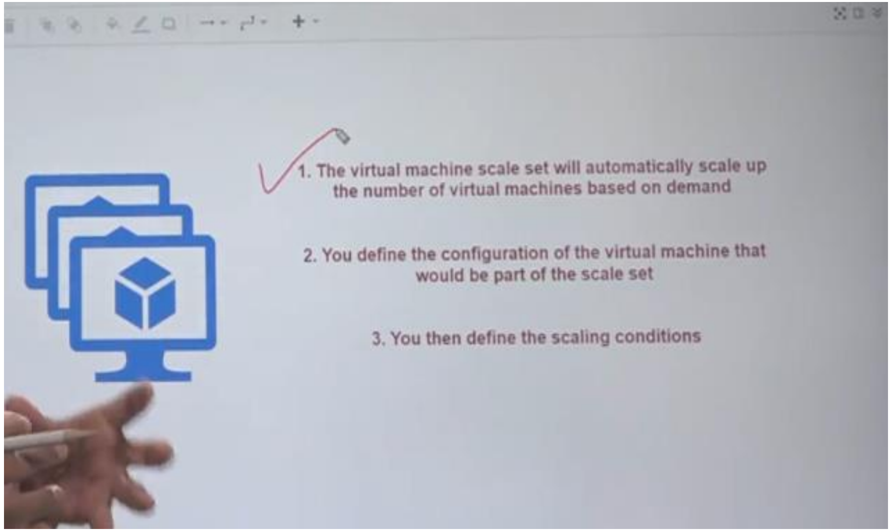
Update domain is logically separated for all maintenance purpose. Say for example if I patch in all servers in update domain 0 , once all fully completed then only next update domain will start.

Only during VM creation only I can associate which availability set I want to associate it in .once created I cant



Virtual Machine Scale Sets

1. The virtual machine scale set will automatically scale up



1. The virtual machine scale set will automatically scale up the number of virtual machines based on demand

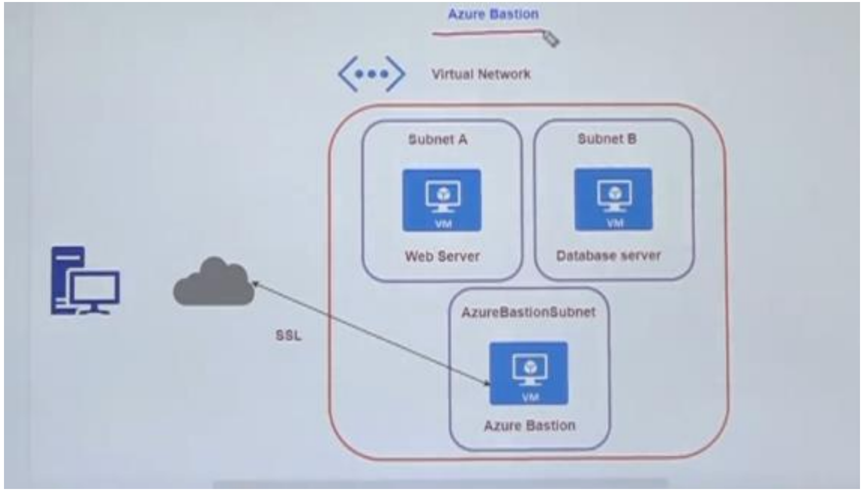
2. You define the configuration of the virtual machine that would be part of the scale set

3. You then define the scaling conditions

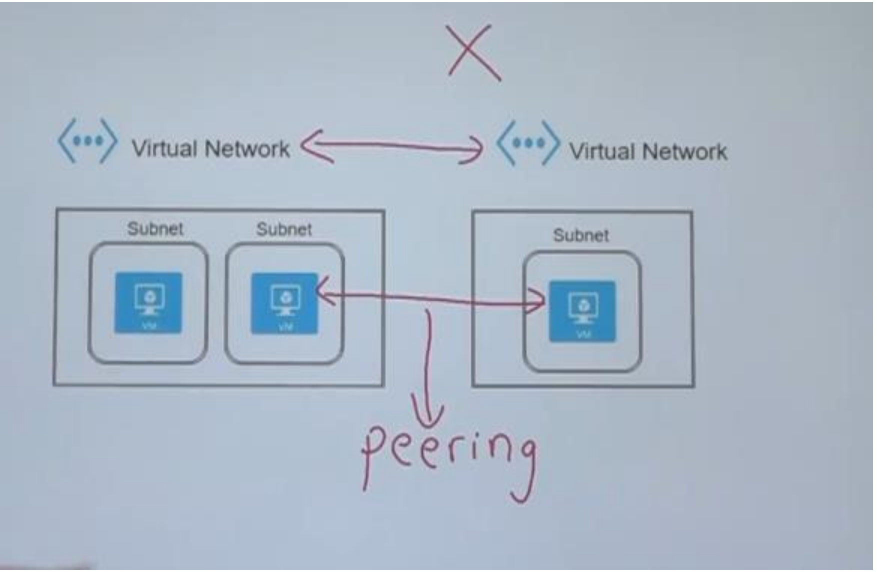
How to increase CPU load

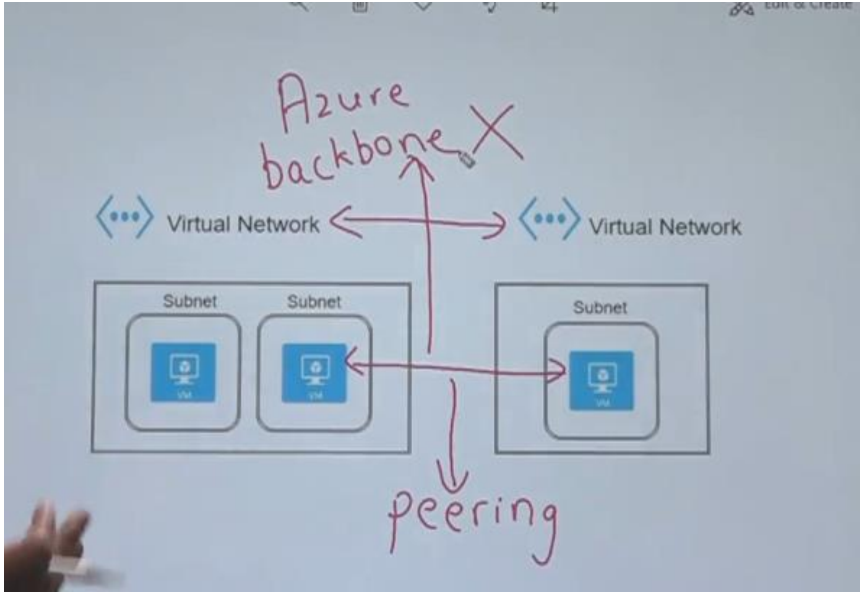
```
sudo stress --cpu 80
```

Bastion Host

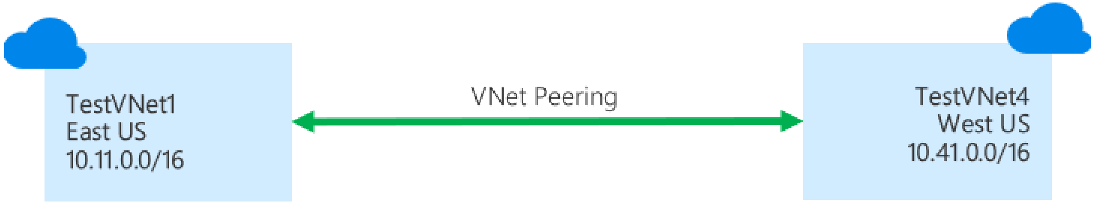


Virtual Peering





AZURE Vnet peering – between 2 virtual networks

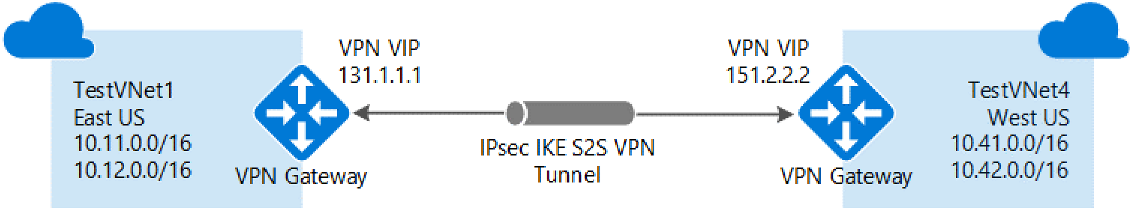


VNet Peering provides a low latency, high bandwidth connection useful in scenarios such as cross-region data replication and database failover scenarios. Since traffic is completely private and remains on the Microsoft backbone, customers with strict data policies prefer to use VNet Peering as public internet is not involved. Since there is no gateway in the path, there are no extra hops, ensuring low latency connections.

VNet peering enables you to seamlessly connect Azure virtual networks. Once peered, the VNets appear as one, for connectivity purposes. The traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, much like traffic is routed between virtual machines in the same VNet, through *private* IP addresses only. No public internet is involved. You can peer VNets across Azure regions, too – all with a single click in the Azure Portal.

- VNet peering - connecting VNets within the **same Azure region**
- Global VNet peering - connecting VNets **across Azure regions**

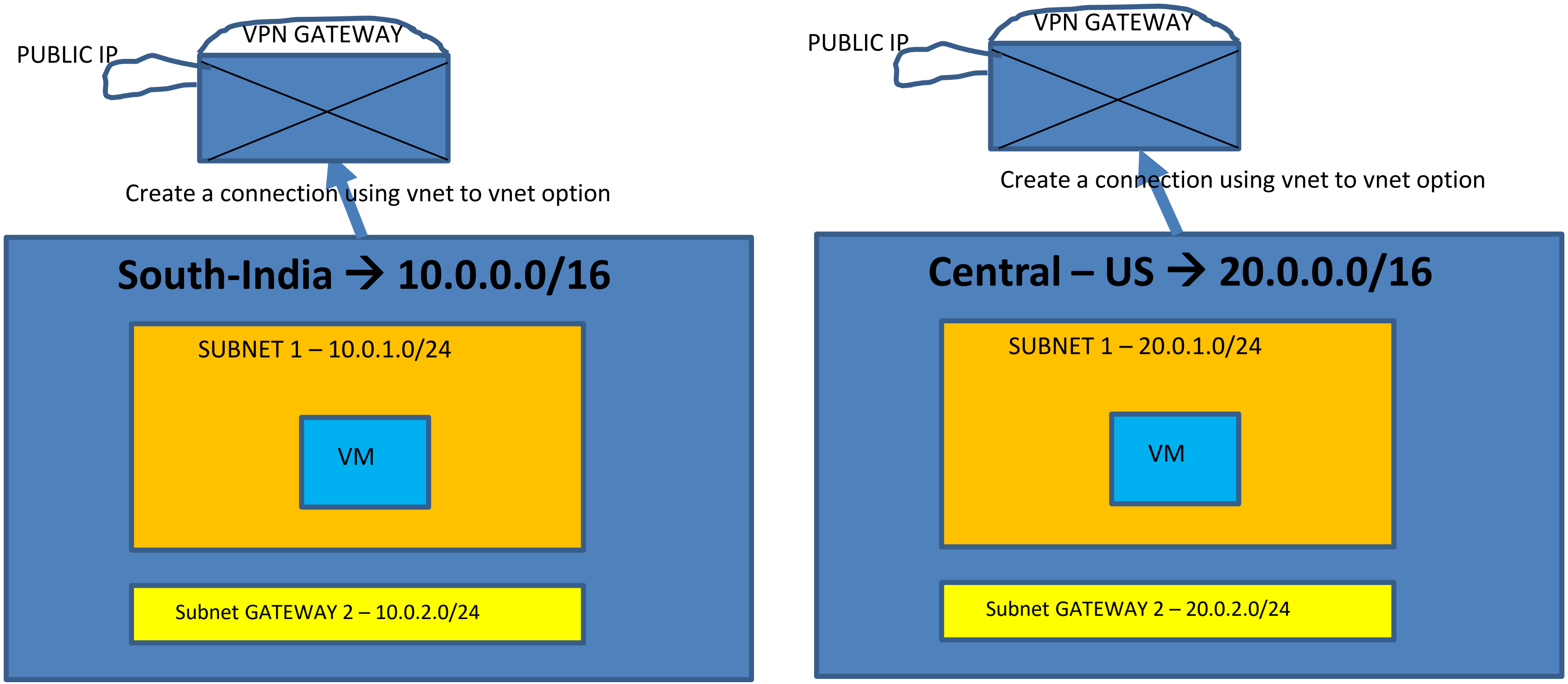
AZURE VPN Gateway to VPN Gateway



A VPN gateway is a specific type of VNet gateway that is used to send traffic between an Azure virtual network and an on-premises location over the public internet. You can also use a VPN gateway to send traffic between VNets. Each VNet can have only one VPN gateway.

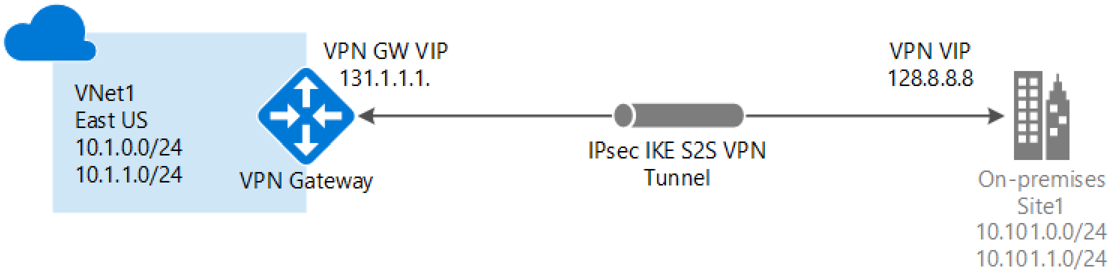
VPN Gateways provide a limited bandwidth connection and is useful in scenarios where encryption is needed, but bandwidth restrictions are tolerable. In these scenarios, customers are also not as latency-sensitive.

VPN to VPN → Azure to AZURE


PUBLIC IP
VPN GATEWAY
Create a connection using vnet to vnet option
South-India → 10.0.0.0/16
SUBNET 1 – 10.0.1.0/24
VM
Subnet GATEWAY 2 – 10.0.2.0/24
PUBLIC IP
VPN GATEWAY
Create a connection using vnet to vnet option
Central – US → 20.0.0.0/16
SUBNET 1 – 20.0.1.0/24
VM
Subnet GATEWAY 2 – 20.0.2.0/24

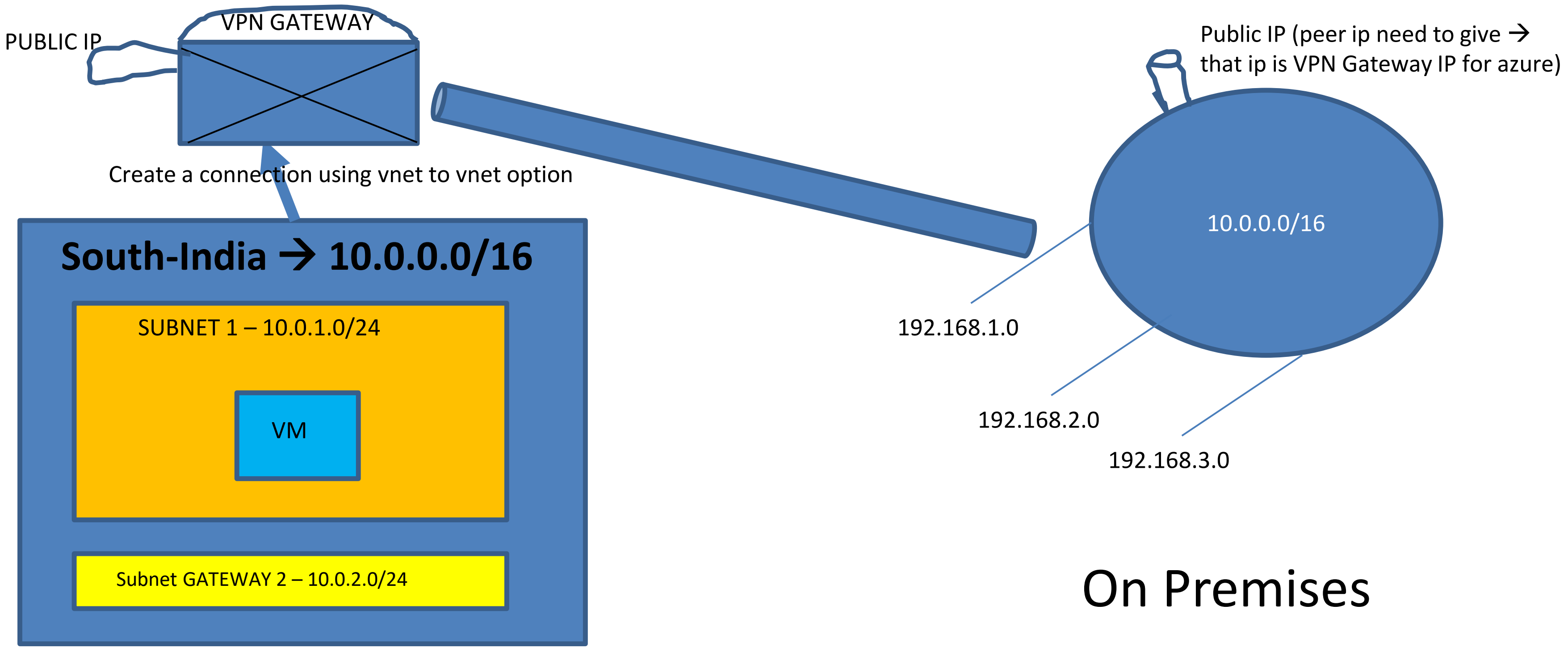
SITE TO SITE VPN

Site to SITe VPN → Azure to Onpremises



A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it. For more information about VPN gateways,

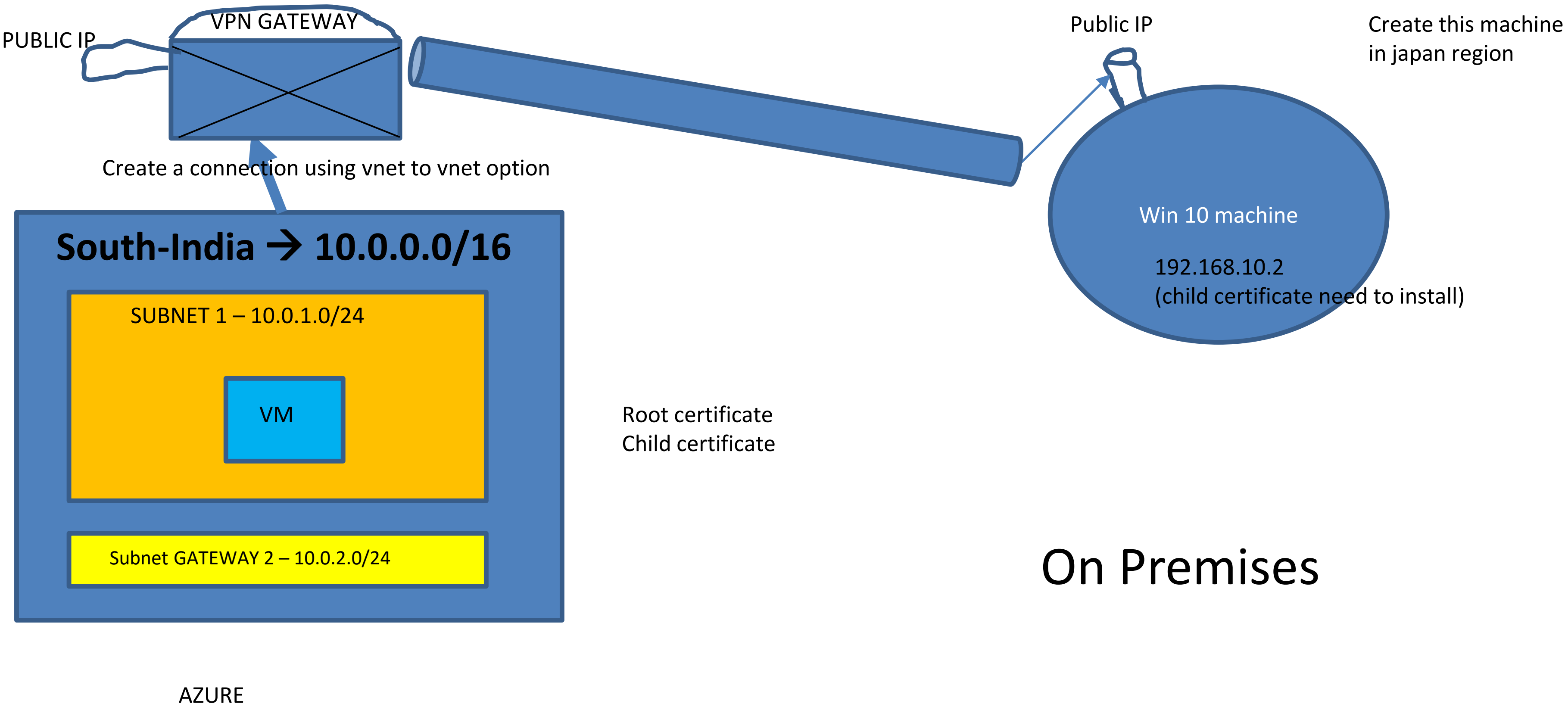
Site to SITe VPN → Azure to Onpremises


PUBLIC IP
VPN GATEWAY
Public IP (peer ip need to give →
that ip is VPN Gateway IP for azure)
Create a connection using vnet to vnet option
South-India → 10.0.0.0/16
SUBNET 1 – 10.0.1.0/24
VM
Subnet GATEWAY 2 – 10.0.2.0/24
10.0.0.0/16
192.168.1.0
192.168.2.0
192.168.3.0

On Premises

Point to Site VPN → Azure to client machine

Point to Site VPN → Azure to client machine



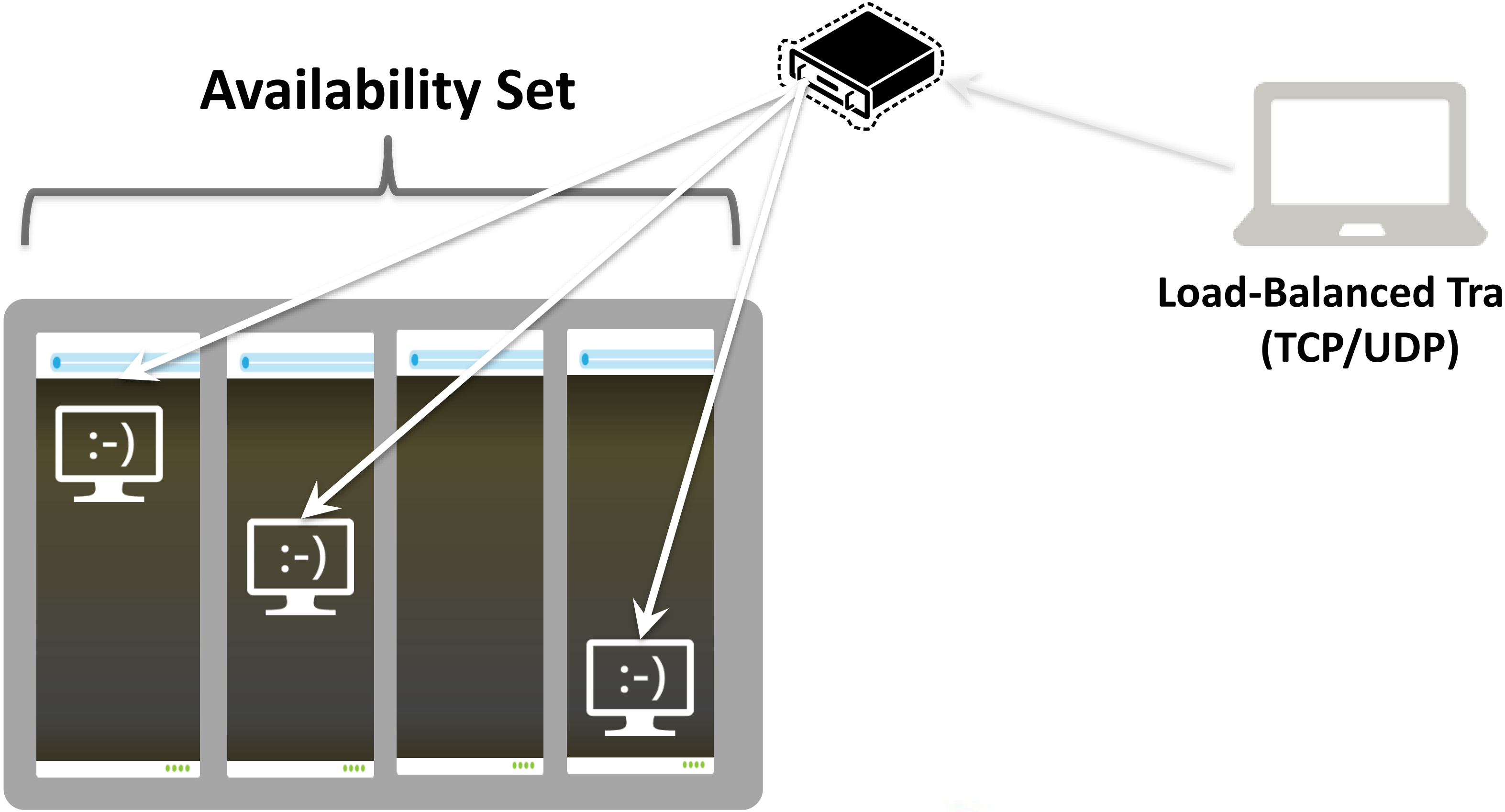
Vnet to vnet peering

Which is best for you?

While we offer two ways to connect VNets, based on your specific scenario and needs, you might want to pick one over the other.

VNet Peering provides a low latency, high bandwidth connection useful in scenarios such as cross-region data replication and database failover scenarios. Since traffic is completely private and remains on the Microsoft backbone, customers with strict data policies prefer to use VNet Peering as public internet is not involved. Since there is no gateway in the path, there are no extra hops, ensuring low latency connections.
VPN Gateways provide a limited bandwidth connection and is useful in scenarios where encryption is needed, but bandwidth restrictions are tolerable. In these scenarios, customers are also not as latency-sensitive.

Load Balancing and High Availability



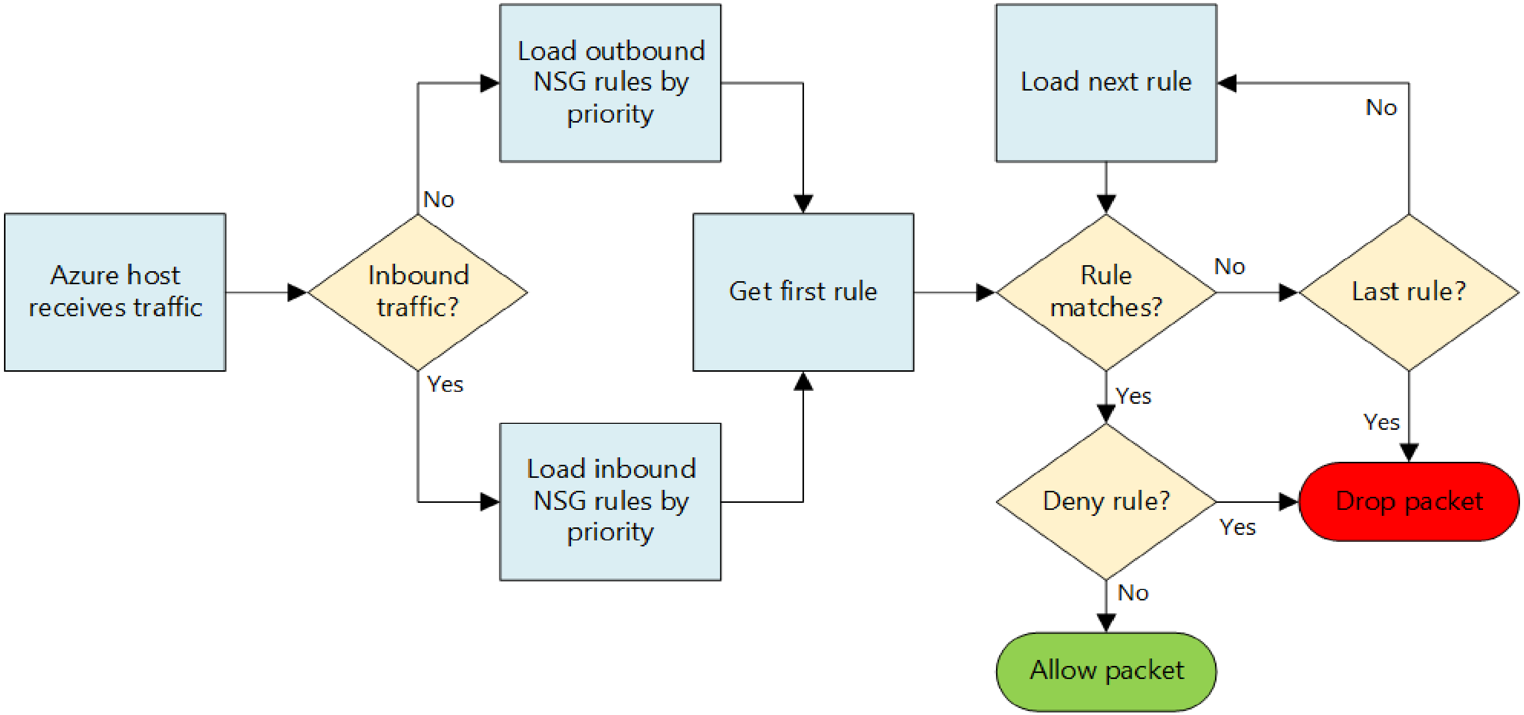
Load-Balanced Traffic (TCP/UDP)

Focus on apps,
Not Infrastructure

Application High Availability

- An application should be built keeping High Availability as one of the important architectural concerns. Some of the important application related High Availability practices are mentioned next:
- An application should implement appropriate exception handling to gracefully recover and inform stakeholders about the issue.
- An application should try to perform the same operation again in the fixed interval for a certain number of times before exiting in an event of an error or Exception.
- An application should have inbuilt timeout capability to decide that an exception cannot be recovered from.
- Maintaining logs and writing logs for all errors, exceptions, and execution should be adopted within the application.
- Applications should be profiled to find their actual resource requirements interms of compute, memory and network bandwidth for a different number of Users.

Design Network Security Group

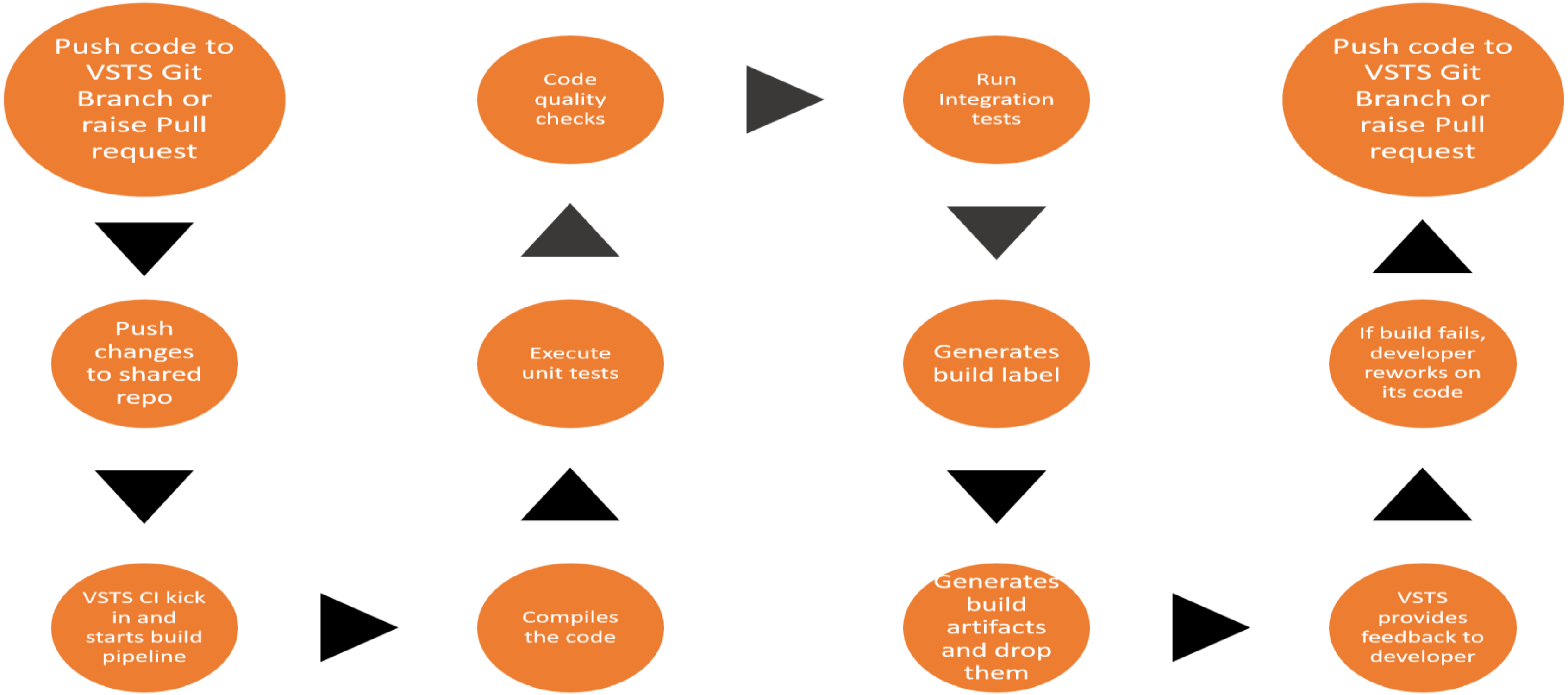


Design Network Security Group

The first step in designing is to ascertain the security requirements of the resource. The following should be answered:

1. Is the resource accessible from the internet only?
2. Is the resource accessible from both the internal resources and the internet?
3. Is the resource accessible from the internal resource only?
4. Determine the resources load balancer, gateways, and virtual machines used
5. Configuration of a virtual network and its subnet
6. Based on answers from these questions, adequate NSG design should be created.

DevOps On Azure



Push code to VSTS Git Branch or raise Pull request

Push changes to shared repo

VSTS CI kick in and starts build pipeline

Compiles the code

Execute unit tests

Code quality checks

Run Integration tests

Generates build label

Generates build artifacts and drop them

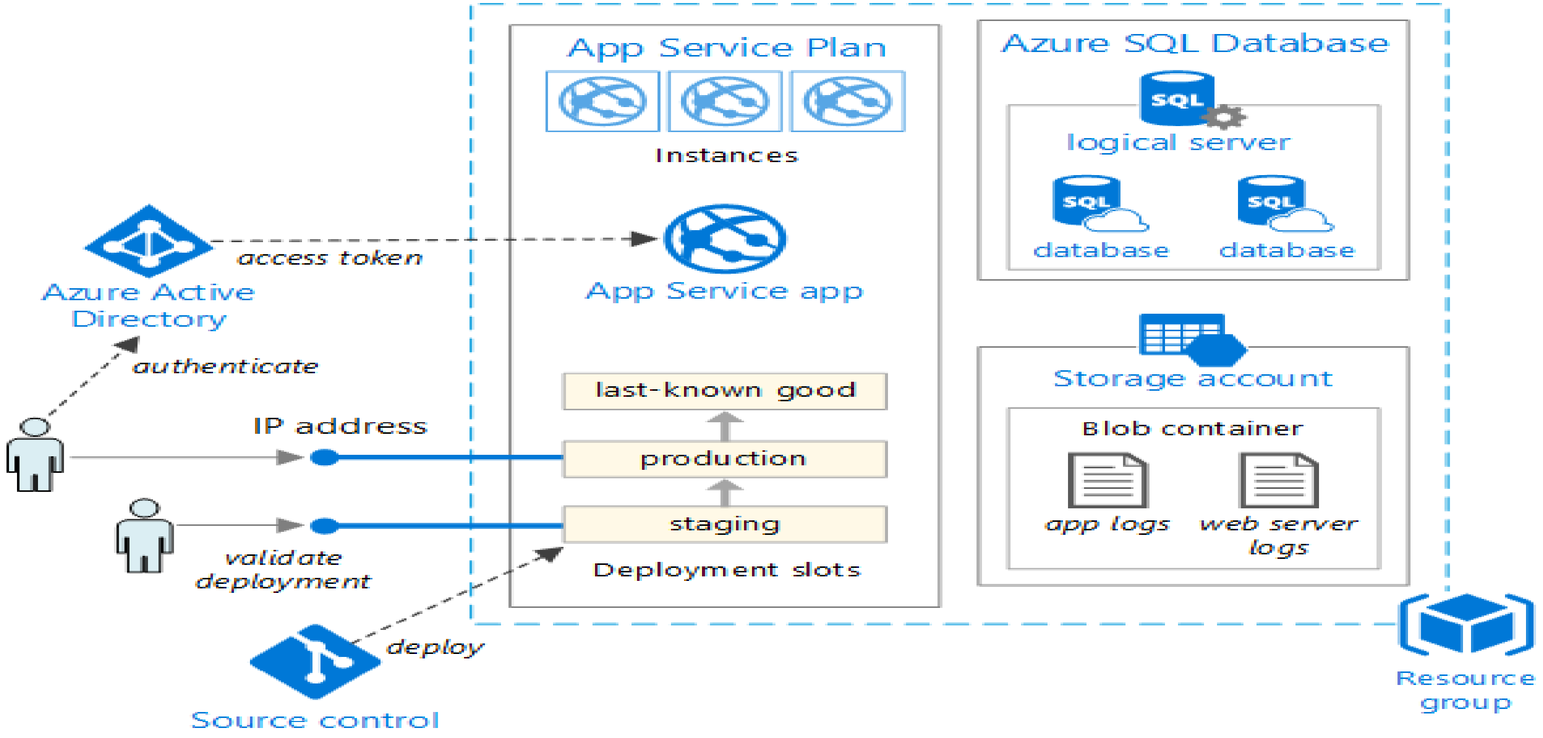
VSTS provides feedback to developer

If build fails, developer reworks on its code

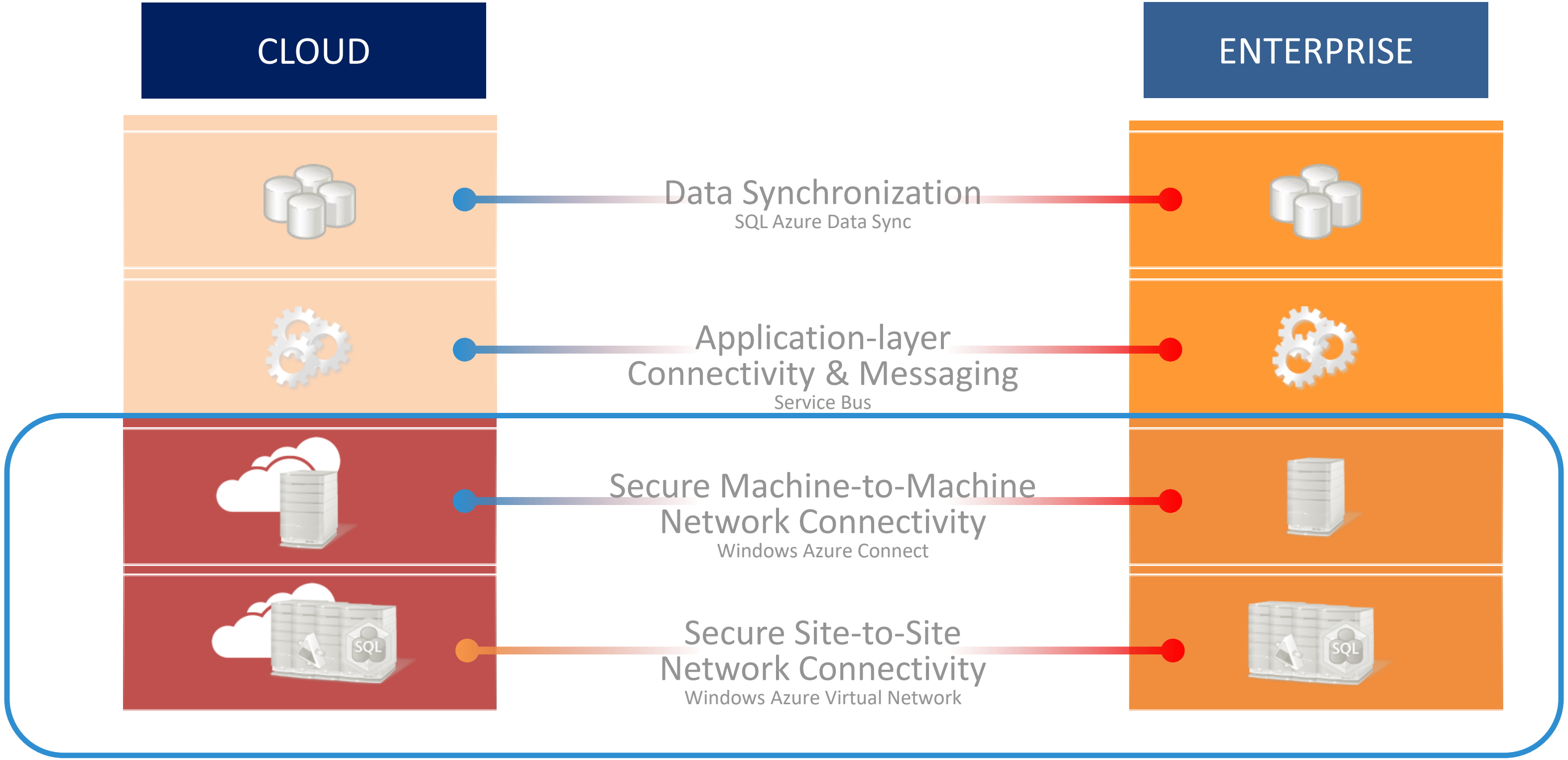
Push code to VSTS Git Branch or raise Pull request

VSTS - Visual Studio Team Services

Sample PAAS - DevOps On Azure



Hybrid Connectivity



Data Synchronization
SQL Azure Data Sync

Application-layer Connectivity & Messaging
Service Bus

Secure Machine-to-Machine Network Connectivity
Windows Azure Connect

Secure Site-to-Site Network Connectivity
Windows Azure Virtual Network

IP-level connectivity