CLOUD INFRASTRUCTURE DESIGN GUIDE

IT'S HOW
WE CONNECT

WELCOME TO THE CLOUD INFRASTRUCTURE DESIGN GUIDE

This guide illustrates various network configurations that can be designed using our cloud infrastructure. Typical scenarios are shown, although many more configurations are possible.

This guide may be read in conjunction with other ***Cloud Services guides***, for more details about specific features.

AUSTRALIAN ACCOUNT HOLDERS

For sales, account set-up enquiries and technical support, contact your Telstra representative or visit the ***Cloud Services website*** (www.cloud.telstra.com), where you'll find all our contact details plus a glossary, FAQs and Our Customer Terms.

TELSTRA GLOBAL ACCOUNT HOLDERS

For sales, account set-up enquiries and technical support, contact your Telstra Global representative or visit the ***Telstra Global website*** (www.telstraglobal.com/cloud) for the customer service team in your region.

> Note: we don't provide assistance with issues specific to a customer's local network, servers, operating systems and software (post-installation). Specialist technical support may be charged as an additional service.

CONVENTIONS USED IN THIS GUIDE

The following typographical conventions are used in this guide for simplicity and readability:

Web addresses, email addresses and hyperlinks are shown in ***bold italics***, for example ***www.telstraenterprise.com.au***.

Button names and titles/features on your computer screen are shown in *italics.*

User input is shown in `typewriter` font.

Cloud Infrastructure Design Guide, Version 3.0

WHAT'S INSIDE

CHAPTER 1
CLOUD INFRASTRUCTURE OVERVIEW

This section contains short introductions to the network components used in cloud infrastructure. Most of these descriptions provide links to further information.

VIRTUAL SERVER SERVICES

In cloud infrastructure, there are four types of virtual server services that can be used in various combinations. When creating your cloud environment, you select a virtual server service as part of a compute service.

Our virtual server services are:

- Virtual Server (Shared)
- Virtual server (Dedicated)
- Virtual server (Dedicated) Gen2
- Managed Virtual Server (Dedicated)

Virtual Server (Shared) uses a flexible pool of shared resources based in our cloud. Resources including CPU, RAM and storage are virtualised for your use, and scaled up or down to meet your needs.

Virtual server (Dedicated), Virtual Server (Dedicated) Gen2 and *Managed Virtual Server (Dedicated)* virtualise server CPU and RAM from a specific allocation of physical resources. Storage is drawn from a shared pool of resources.

As part of our *Managed Virtual Server (Dedicated)* service, we perform and take responsibility for a number of operational requirements for your cloud solution. *Managed Virtual Server (Dedicated)* is available from data centres in Australia, London, Hong Kong and Singapore, but is not available to Telstra Global customers.

Each of the server types listed above have different ways of using and configuring resources such as storage, CPU, RAM, operating systems and software. For more information, see the user guide for each server type:

- ***Virtual Server (Shared) User Guide***
- ***Virtual Server (Dedicated) User Guide***
- ***Virtual Server (Dedicated) Gen2 User Guide***
- ***Managed Virtual Server (Dedicated) User Guide***

Network configuration and features are common between all server types. Our backup service is available across all server types.

OUR DATA CENTRES

Our data centres securely house the physical resources and infrastructure used to provide our cloud solutions. We own, operate and maintain all our physical data centres. Data centres are currently located in:

Australian locations

- Melbourne
- Perth

- Sydney

International locations

- Singapore
- Hong Kong
- London

Data centres provide you with connectivity to:

- The internet
- Your private networks via a Telstra Next IP® network, Global IP VPN connection or IPsec VPN tunnel
- Your data in the cloud
- Both dedicated and shared virtual servers and resources

You can select which data centre location(s) you wish to contain specific cloud infrastructure services. We describe your chosen data centre location(s) as your *virtual data centre(s)*. You can use virtual data centres in different countries, and have multiple virtual data centres in the same location.

If you're drawing your cloud resources from Australia, your Virtual Server (Shared) can only be provisioned from our Melbourne data centre. Virtual server (Dedicated) Gen2 is available from select Australian data centres. All other virtual server types and resources are available from any of our data centres in Australia and globally.

VIRTUAL SERVER NETWORKS

You can choose to contain a virtual server within a public or private network, or use ***dual homing*** to connect a virtual server to both networks.

Each of your networks (excepting Gen2) can contain virtual servers, firewalls, load balancers and up to 10 subnets per ***virtual server service***. Virtual Server (Dedicated) Gen2 offers up to 100 subnets, All virtual servers within a network can be allowed to communicate with each other, or separated using firewall rules.

Your *public network* is accessible through an internet connection, via your public interconnect.

Your *private network* is only accessible through a private network connection, via your private interconnect.

Learn more about virtual server networks in our ***Network and Security User Guide.***

CONNECTING TO YOUR PRIVATE NETWORK

There are a few different ways to connect to your private network through your private interconnect:

- A Telstra Next IP® network (or Global IP VPN for virtual data centres outside Australia)
- An IPsec VPN tunnel
- Both a Telstra Next IP® network and an IPsec VPN tunnel

A *Telstra Next IP® network* allows connection to all, or selected private subnets within your private network. A Telstra Next IP® network can only access Australian data centres. International data centre users have an equivalent Global IP VPN network connection available.

IPsec VPN provides a permanent, site-to-site network tunnel between an office LAN and a private network within a single virtual data centre via the internet.

You can create up to ten IPsec VPN tunnels per virtual data centre. Each IPsec VPN allows connection to one virtual data centre.

For more details on how you can connect to your virtual server networks, see our ***Network and Security User Guide.***

IP ADDRESSING

We allocate *public IP addresses* to virtual servers in your public network, from a shared subnet on a one-by-one basis. Public IP address allocation may happen automatically, or after you request it, depending on the type of virtual server.

You can choose up to 10 *private subnets* per ***virtual server service*** (non-internet addressable) for virtual server groups in your private network. You can have more than 10 private subnets on the Virtual Server (Dedicated) Gen2 network.

For more information about managing IP addresses and subnets, see the ***Network and Security User Guide.***

VIRTUAL SERVER CONNECTION TO A SECOND NETWORK – DUAL HOMING

A dual homed virtual server has both a public and private IP address, allowing it to be accessed through both your public and private network connections. Dual homing can also be used to allow communication between virtual servers contained in different networks (public and private).

For more detailed information about public and private networks, refer to our ***Network and Security User Guide.***

SSL VPN MANAGEMENT CONNECTION TO VIRTUAL SERVERS

Using secure remote access (SSL VPN), you can remotely and securely manage any virtual server. SSL VPN is made possible through a management connection point (vNIC) available on all virtual servers. This management connection is separate to any public and private network connections, and can’t be used as a secure access method for end users.

For Gen2 a separate management connection point is not required.

Our ***Network and Security User Guide*** contains more information about SSL VPN.

NETWORK FEATURES

You can manage traffic flow, privacy and security of your data using firewalls and load balancers.

Firewalls are used to create most of the network configurations shown in this guide. You can customise firewall rules to allow or deny traffic through groups or individual virtual servers. A separate firewall is required for each network, and each compute service within your cloud solution.

Load balancers can be used to distribute traffic across multiple virtual servers within the same network, which could include different virtual server types.

To learn more about firewalls and load balancers, see the ***Network and Security User Guide.***

CHAPTER 2
INTRODUCTION TO MULTI-TIERED NETWORKS

In network architecture, servers can be separated into tiers according to their functionality within the network and/or security requirements. Tiers allow the presentation, processing and storage of data to be separated within a network.

TIERS AND ZONES IN CLOUD INFRASTRUCTURE

Using our cloud resources, virtual servers can be grouped into tiers using several methods. Separate tiers can be formed by creating both a public and private network. Each of these network tiers can be split further into multiple tiers using firewall rules.

Virtual servers can be allowed to communicate with each other if they are within the same tier, or located in adjacent tiers.

Zoning is a way of separating groups of virtual servers within the same tier. Each zone can include one or more virtual servers that can communicate with each other. Zoning is achieved through firewall rules.

BENEFITS OF MULTI-TIER CONFIGURATIONS

Tiered network configurations can provide greater security, privacy and control of your data in the cloud.

By separating your databases from the presentation tier where data is accessed and viewed, you can securely control access to the database itself. In its most basic form, this scenario creates a *two-tier* network configuration.

To further increase the security and scalability of your cloud solution, you could separate your database virtual servers from your application tier - the virtual servers used to process your data. This will also reduce the workload on individual virtual servers. This scenario results in *three-tier* network configuration.

In the following pages, this guide illustrates common network scenarios you can produce in our cloud environment.

For each scenario, we'll describe the cloud resources, networks and connections you'll need to use.

CHAPTER 3
TWO-TIERED NETWORKS

TWO-TIERED SCENARIO

You may want to run an application from the cloud using a typical two-tiered network configuration.

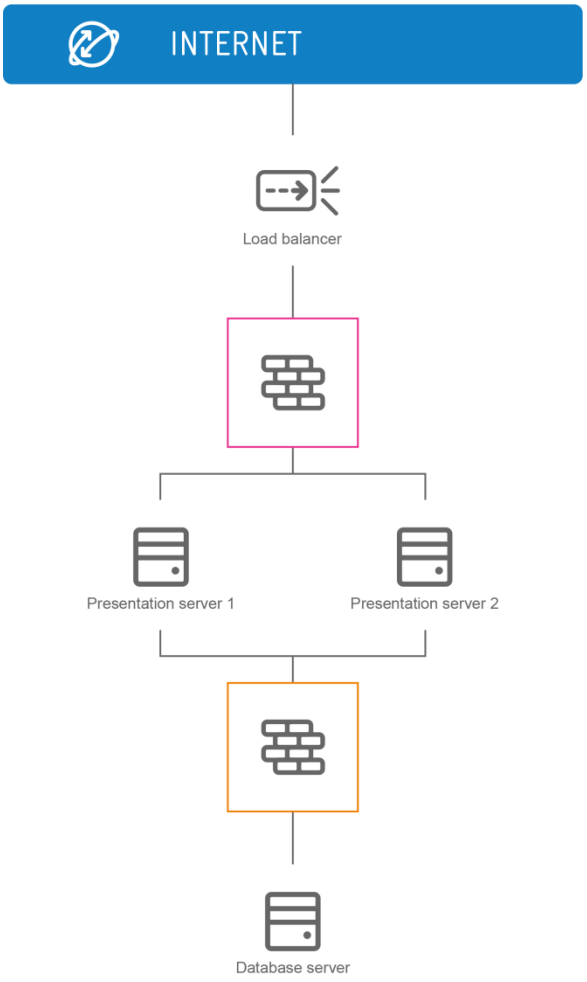
In this example the presentation tier is accessible to users via the internet. An alternative two-tiered scenario would be to make your presentation tier accessible only from a private network connection (an intranet for example). Read about running ***applications in a private network*** later in this guide.

The presentation tier will need to manage high volumes of traffic, so a load balancer is used to distribute traffic across the virtual servers in the presentation tier.

To send and receive information to and from the database, the virtual servers in the presentation tier will need to communicate with the virtual server in the database tier.

For data security you may want to restrict access to the database tier.

For simplicity in this particular scenario, we're only using a total of three virtual servers. We'll assume you may want to add more virtual servers later on.



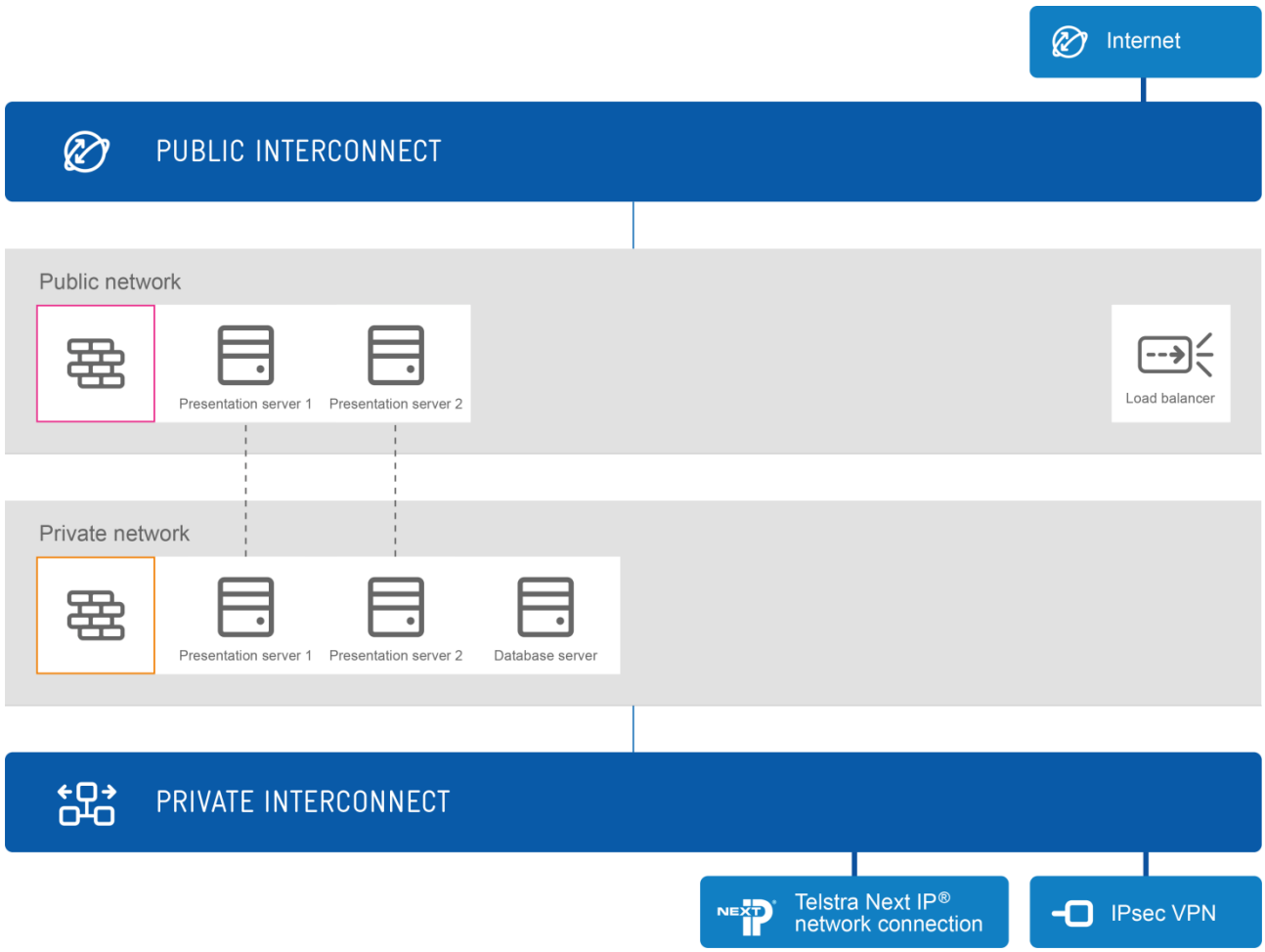
HOW TO CONFIGURE TWO TIERS USING CLOUD INFRASTRUCTURE

There are two alternative ways to create this configuration in cloud infrastructure:

- ***Separation of networks***
- ***Virtual tiering***

TWO-TIERED CONFIGURATION 1: SEPARATION OF NETWORKS

This is the first of two methods that can be used to achieve a ***two-tiered network scenario***. In this method, tiering is achieved using two networks, with the database server accessible from a private network connection.



VIRTUAL SERVERS AND CONNECTIONS

To build the presentation tier, create two virtual servers – each connected to both a public and private network (dual-homed). These virtual servers will be contained in your public network and always connected to the internet, with traffic potentially restricted by firewall rules.

Create a virtual server for your database in your private network. Your database virtual server will be directly accessible through a private network connection (IPsec VPN, Telstra Next IP® network or Global IP VPN).

In addition to their network connection(s), all virtual servers in both tiers can be managed directly through an SSL VPN connection. With Virtual Server Dedicated Gen2 servers you can only directly manage virtual servers on private networks via an SSL VPN connection.

There are no limits to the number of virtual servers you can add to any tier, at any time.

FIREWALLS

Configure a firewall in your public network to control traffic between:

- The internet and the virtual servers in your presentation tier

Add and configure a firewall in your private network to control traffic between:

- Virtual servers in the presentation tier and the database server
- The database server and your private interconnect

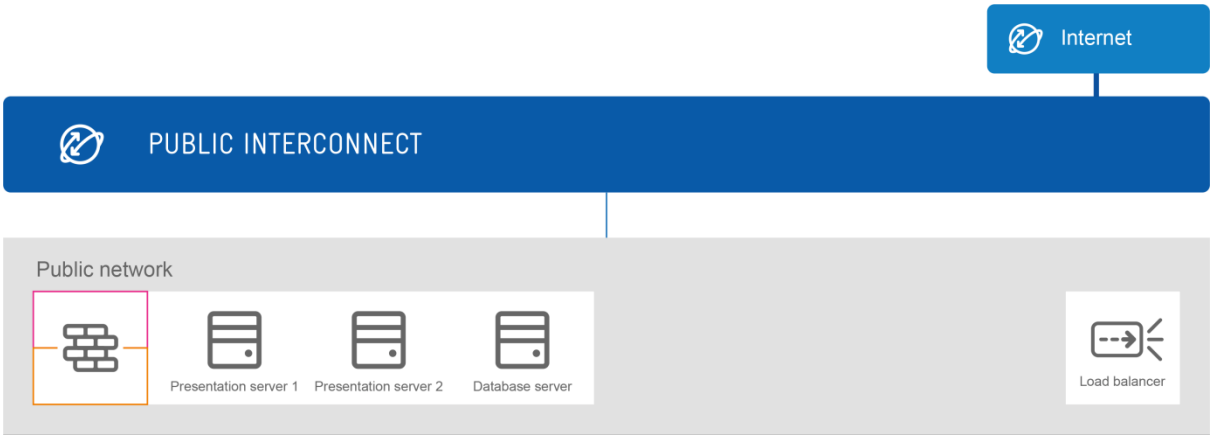
LOAD BALANCER

Add and configure a load balancer in your public network to distribute traffic across virtual servers in your presentation tier.

TWO-TIERED CONFIGURATION 2: VIRTUAL TIERING

This is a second method for creating a ***two-tiered network scenario*** using cloud infrastructure.

In this configuration using a single public network, virtual tiering is created using a firewall. None of the virtual servers are accessible from a private network connection.



VIRTUAL SERVERS AND CONNECTIONS

Create three virtual servers, all connected to the public network. One of these virtual servers will contain your database.

All these virtual servers will be contained in your public network and connected to the internet, with traffic restricted by firewall rules.

All virtual servers can be managed directly through an SSL VPN connection. Gen2 virtual servers will need to be connected to a private network for management via SSL VPN.

There are no limits to the number of virtual servers you can add to any virtual tier, at any time.

FIREWALLS

To create separate virtual tiers for your presentation servers and database servers, you'll need to configure multiple rules on the firewall in the public network to control traffic between:

- The internet and all your virtual servers in the public network, including restricting access from the internet to the database server
- Virtual servers in the presentation tier and the database server

LOAD BALANCER

Add and configure a load balancer to distribute traffic across only your virtual servers in the presentation tier.

CHAPTER 4
THREE-TIERED NETWORKS

THREE-TIERED SCENARIO

You may want to run an application from the cloud using a typical three-tiered network configuration.

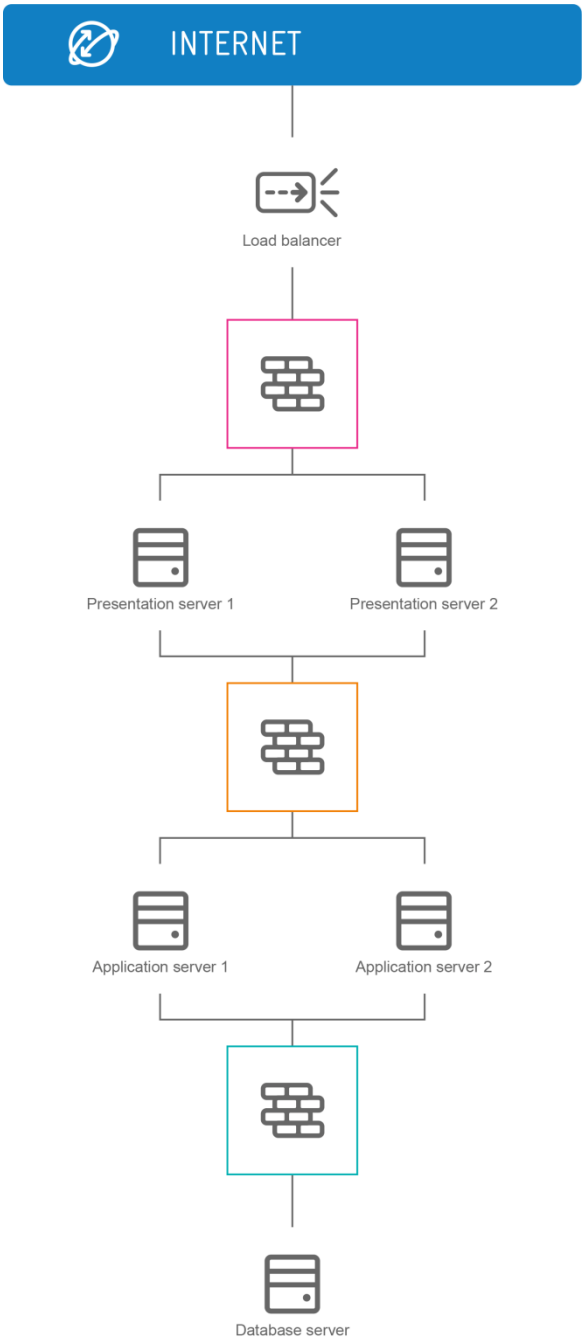
In this scenario, the presentation tier is accessible to users via the internet. An alternative three-tiered scenario (not illustrated on this page) would be to make your presentation tier accessible only from a private network connection. Read about ***applications in a private network*** later in this guide.

In the configuration shown, the presentation tier will need to support high volumes of traffic - so a load balancer is used to distribute traffic across both virtual servers in the presentation tier.

The application tier contains the virtual servers that will process data, and communicate with both the presentation tier and the database tier. If connecting to your application tier through a private network connection, an optional firewall can restrict traffic from directly accessing virtual servers in the application tier.

A third tier is needed to contain the database, and separate it from the data processing that happens in the application tier. If you want to connect to your database tier through a private network connection, an optional firewall can restrict access to the database server.

In this specific scenario, we're using a basic configuration of just five virtual servers. We'll make allowance for you to add more virtual servers in the future.



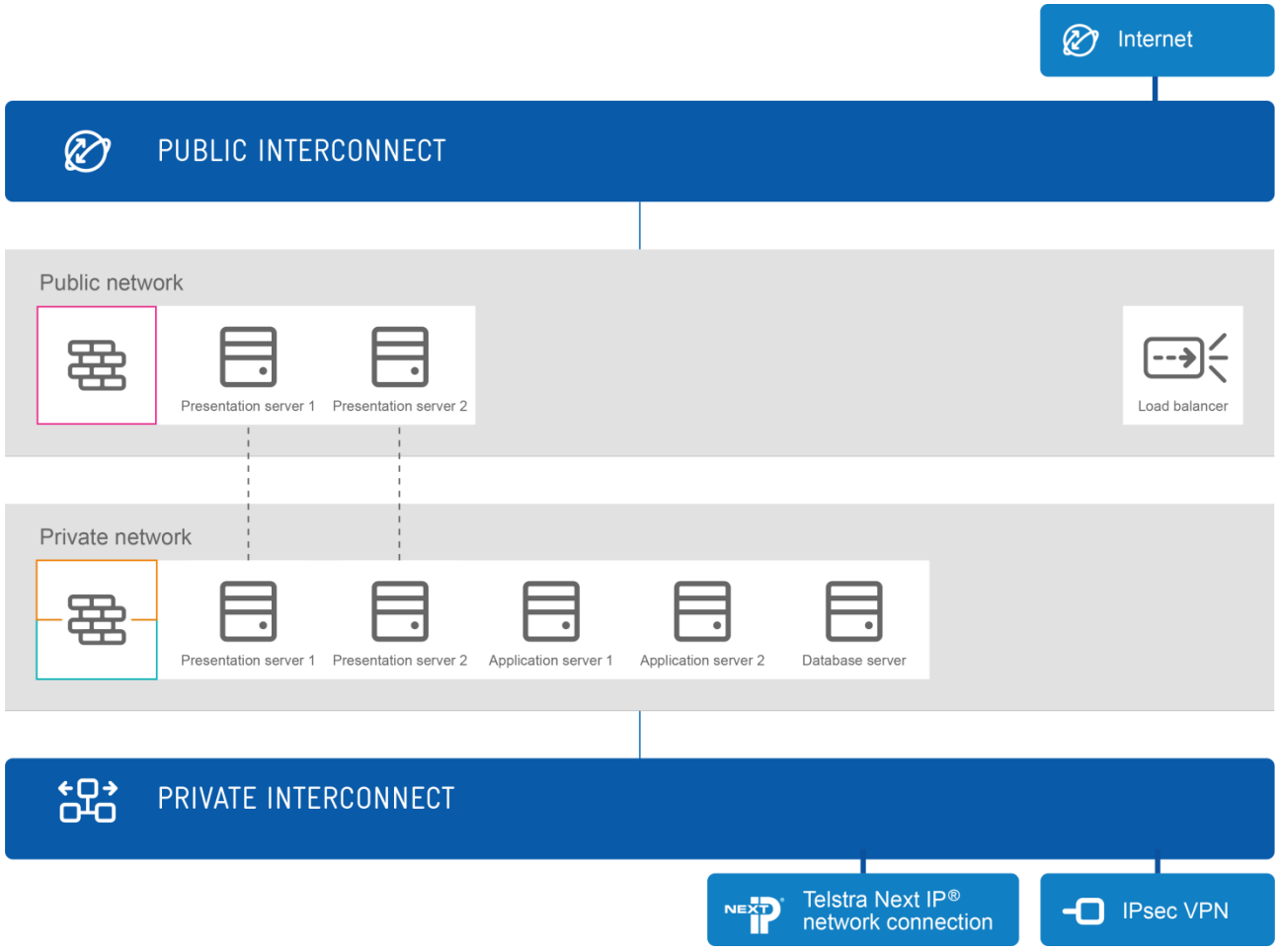
HOW TO CONFIGURE THREE TIERS USING CLOUD INFRASTRUCTURE

There are two different ways to create this three-tiered configuration in cloud infrastructure:

- ***Separation of networks***
- ***Virtual tiering***

THREE-TIERED CONFIGURATION 1: SEPARATION OF NETWORKS

This is one of two methods you could use to achieve a ***three-tiered network scenario***. Using this method, tiering is achieved using two networks, with both the application servers and database server accessed from a private network connection.



VIRTUAL SERVERS AND CONNECTIONS

To construct the presentation tier as shown in the scenario, create two virtual servers – each connected to both the public and private network (dual-homed). These virtual servers will be contained in your public network and always connected to the internet, but potentially restricted by firewall rules.

Create three more virtual servers in your private network. These servers will all exist in your private network, but will be separated into application and database tiers using firewall rules.

Both your application and database virtual servers will only be directly accessible through a private network connection (IPsec VPN, Telstra Next IP® network or Global IP VPN).

In addition to their network connection(s), all virtual servers in all tiers can be managed directly through an SSL VPN connection.

There are no limits to the number of virtual servers you can add to any tier, at any time.

FIREWALLS

Configure a firewall in your public network to control traffic between:

- The internet and the virtual servers in your public network (presentation tier)

Add and configure a firewall in your private network to control traffic between:

- Virtual servers in the presentation tier and the application tier
- Virtual servers in the application tier and the database server
- All virtual servers in your private network (application and database), and the private interconnect

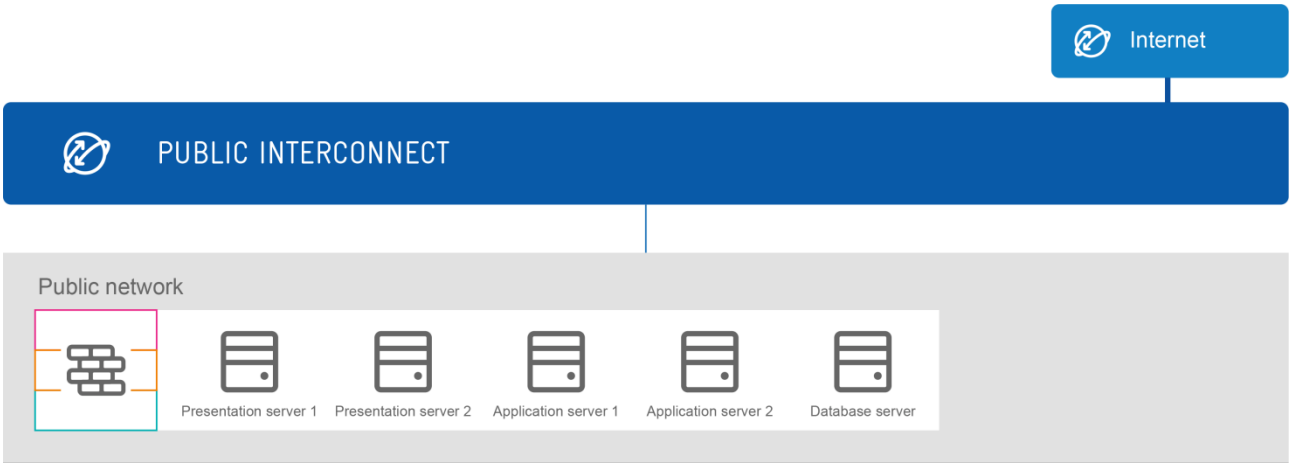
LOAD BALANCER

Add and configure a load balancer in your public network to distribute traffic across virtual servers in your presentation tier.

THREE-TIERED CONFIGURATION 2: VIRTUAL TIERING

This is an alternative method for creating a ***three-tiered network configuration*** using cloud infrastructure.

This configuration uses a single public network, and creates virtual tiering within the network using a firewall. None of the virtual servers are accessible from a private network connection.



VIRTUAL SERVERS AND CONNECTIONS

To achieve the configuration shown in the ***scenario***, create five virtual servers, all connected to the public network. One of these virtual servers will contain your database, two of the servers will be used for the application tier and two virtual servers will form the presentation tier. Firewall rules will be used to create the separation.

All these virtual servers will be contained in your public network and connected to the internet, with option of restricting internet traffic using firewall rules.

All virtual servers can be managed directly through an SSL VPN connection. Virtual server (Dedicated) Gen2 will require virtual servers to be connected to a private network for management via SSL VPN.

There are no limits to the number of virtual servers you can add to any virtual tier, at any time.

FIREWALLS

To create three separate virtual tiers, you'll need to configure multiple rules on the firewall in your public network to control traffic between:

- The internet and all your virtual servers in the public network, including restricting access from the internet to the application tier and database server
- Virtual servers in the presentation tier and the application tier
- Virtual servers in the application tier and the database server

LOAD BALANCER

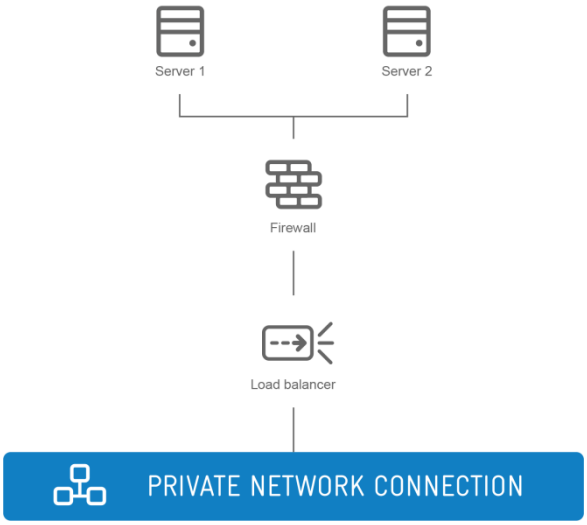
Add and configure a load balancer to distribute traffic across virtual servers in your presentation tier.

CHAPTER 5
APPLICATIONS IN A PRIVATE NETWORK

PRIVATE APPLICATION SCENARIO

In the previous pages of this guide we've described typical two-tier and three-tier network scenarios, where the presentation tier virtual servers are accessed via the internet.

Alternatively, you could choose to make your application accessible only via a private network connection. Creating an intranet is a typical example.



HOW TO CONFIGURE A PRIVATE APPLICATION USING CLOUD INFRASTRUCTURE

To replicate a typical intranet network scenario, follow any of the previous virtual tiering examples in this guide, with these exceptions:

- Instead of creating virtual servers with public network connections, create *all* virtual servers with *only* a private network connection (do not dual home)
- Create your firewall(s) in your *private network*, not a public network
- Create your load balancer(s) in your *private network*, not a public network

Following these instructions will mean none of your virtual servers will be publically accessible via the internet.

You'll need an IPsec VPN, Telstra Next IP® network or Global IP VPN to access your virtual servers.

USING MULTIPLE INTRANETS IN A SINGLE PRIVATE NETWORK

You can choose to create multiple intranets within the same private network, separated by firewalls.

Firewall rules can be configured to separate zones of virtual servers within a private network.

CHAPTER 6
USING MULTIPLE VIRTUAL DATA CENTRES

MULTIPLE VIRTUAL DATA CENTRES SCENARIO

You may want to run an application in the cloud, and draw your virtualised resources from separate locations. In this case, access to two separate virtual data centres is required.

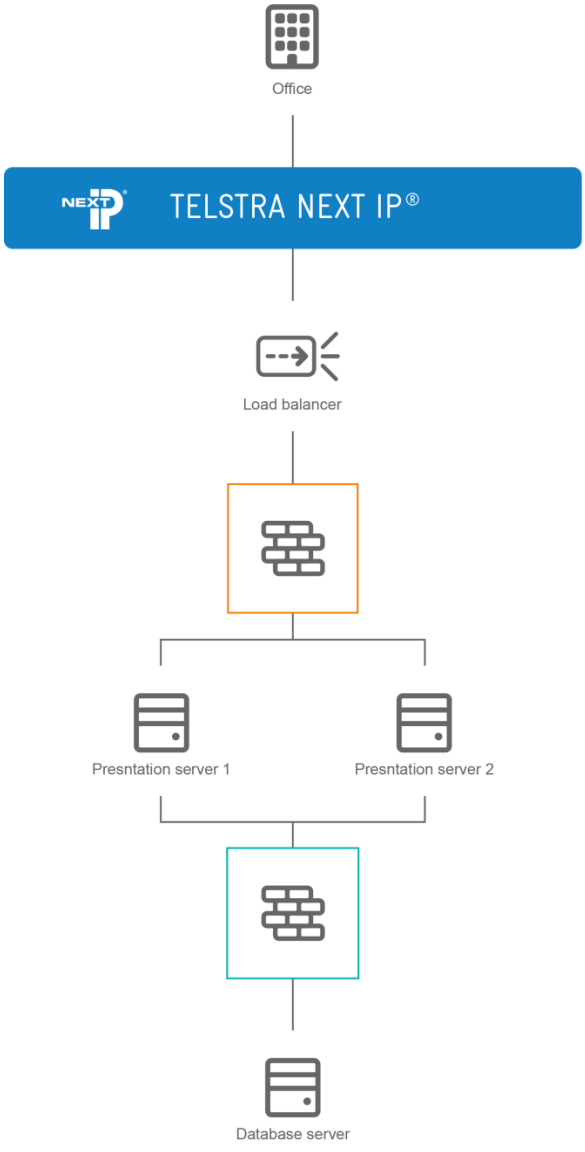
In this scenario, the virtual servers will need to support high volumes of traffic, so a load balancer is used to distribute traffic within each virtual data centre.

Communication between the two virtual data centres is allowed in this scenario.

An alternative scenario (not shown) may be that communication between different virtual data centres is intentionally blocked.

Multiple virtual data centres might be used to locate specific cloud resources closer to where the end users are based.

In this scenario we don't specify the tiering configuration of the network in each virtual data centre. The network configuration at each virtual data centre needn't be identical, unless redundancy is your purpose.



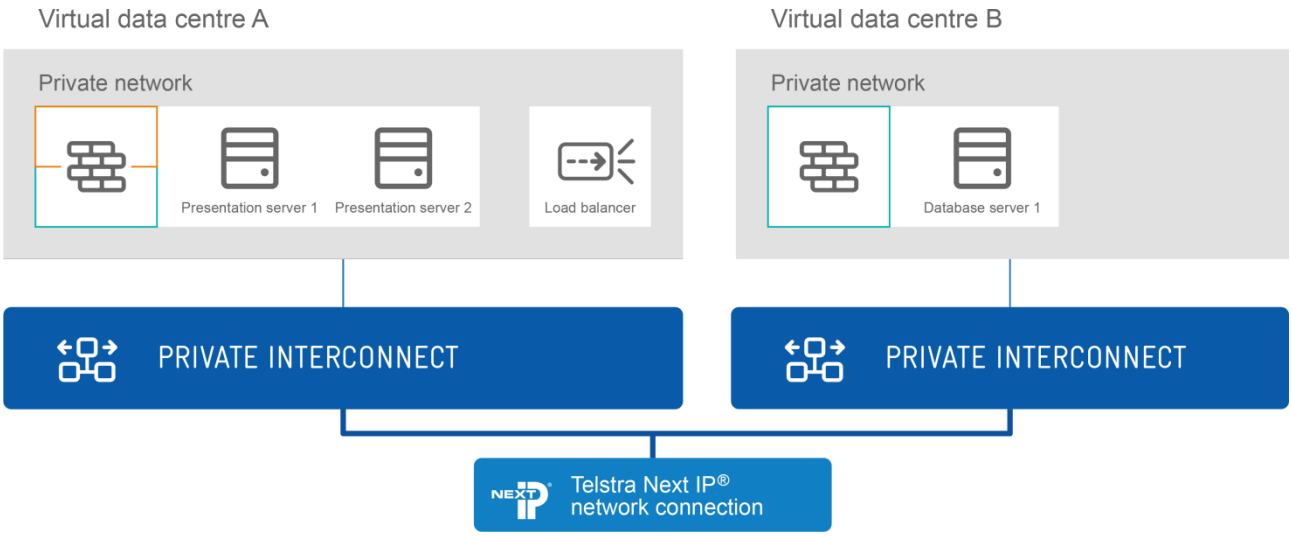
HOW TO CONFIGURE MULTIPLE VIRTUAL DATA CENTRES USING CLOUD INFRASTRUCTURE

The following configuration shows how you can connect to, and allow communication between two virtual data centres in different locations. You could connect any number of virtual data centres using these methods.

Connection is via a private network connection in this scenario, although this isn't a requirement in cloud infrastructure. You can create public networks in addition to, or instead of private networks in two virtual data centres. To allow two public networks in different virtual data centres to communicate with each other, you'll need to either:

- Establish connectivity between the virtual data centres via the internet
- Dual home all the individual virtual servers in both virtual data centres, you want to be in communication. Then ensure you have a separate private network connection to each virtual data centre.

You can choose a virtual data centre service in any of our Australian and global locations, in any combination.



VIRTUAL SERVERS AND CONNECTIONS

Any of the two or three-tier network configurations shown in this guide could be created in each virtual data centre.

If you require private networks in separate data centres to communicate with each other, then you'll need a Cloud Direct Connect™connection (or Global IP VPN) to each private network.

You'll need to make sure the private IP addresses in the two data centres you are connecting, don't overlap.

This will mean your virtual servers will only be accessible through a private network connection.

FIREWALLS

Configure a firewall in each of your data centre networks to control traffic between:

- Your public and private interconnects and individual virtual servers

You may require additional firewalls to control traffic flow between your virtual tiers (not illustrated).

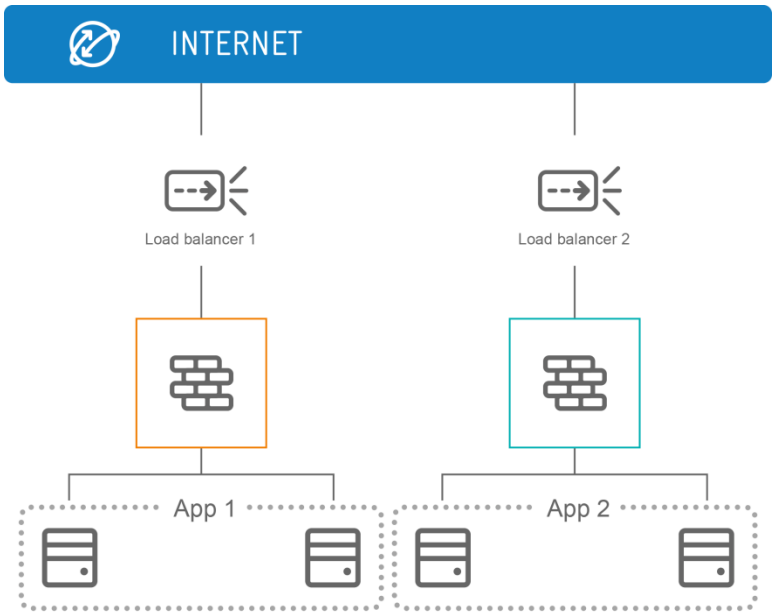
LOAD BALANCERS

You can configure a load balancer in each data centre to distribute traffic across virtual servers in your presentation tiers.

CHAPTER 7
USING MULTIPLE APPLICATIONS

MULTIPLE APPLICATIONS SCENARIO

You may want to run more than one application within a network, but restrict communication between different applications.



HOW TO CONFIGURE MULTIPLE APPLICATIONS USING CLOUD INFRASTRUCTURE

The scenario objectives can be achieved within a single virtual data centre using:

- Zoning with firewall rules
- Public and private network separation

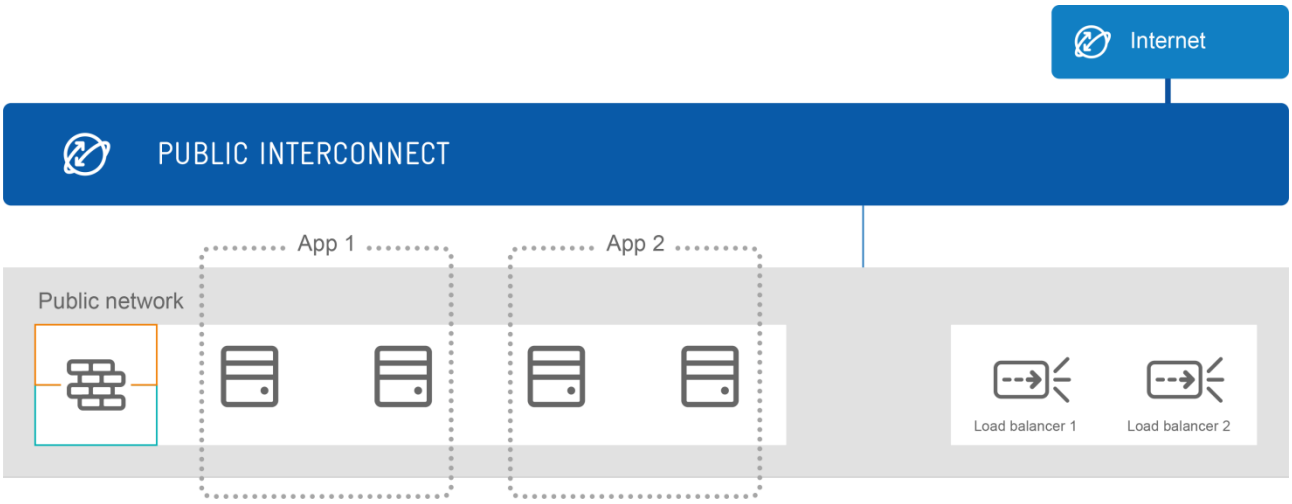
It's also possible to use a combination of these methods to separate multiple applications within a single data centre.

You could also place applications in different virtual data centres.

ZONING WITH FIREWALL RULES

The virtual server(s) handling a single application can be separated (zoned) from all other applications using firewall rules. Zoning allows you to separate any number of applications.

Different firewall security policies can be applied to virtual servers on each tier. So for instance, for a particular application you could choose to create a zone for virtual servers in your application tier, but allow virtual servers in your database tier to communicate with other virtual servers.



PUBLIC AND PRIVATE NETWORK SEPARATION

Using this method, a maximum of two applications can be separated within the same virtual data centre, if one operates in your public network and the other one in the private network.

In this case, all virtual servers (in the presentation tier, application tier and database tier) handling one application must be contained in a single network (public or private).

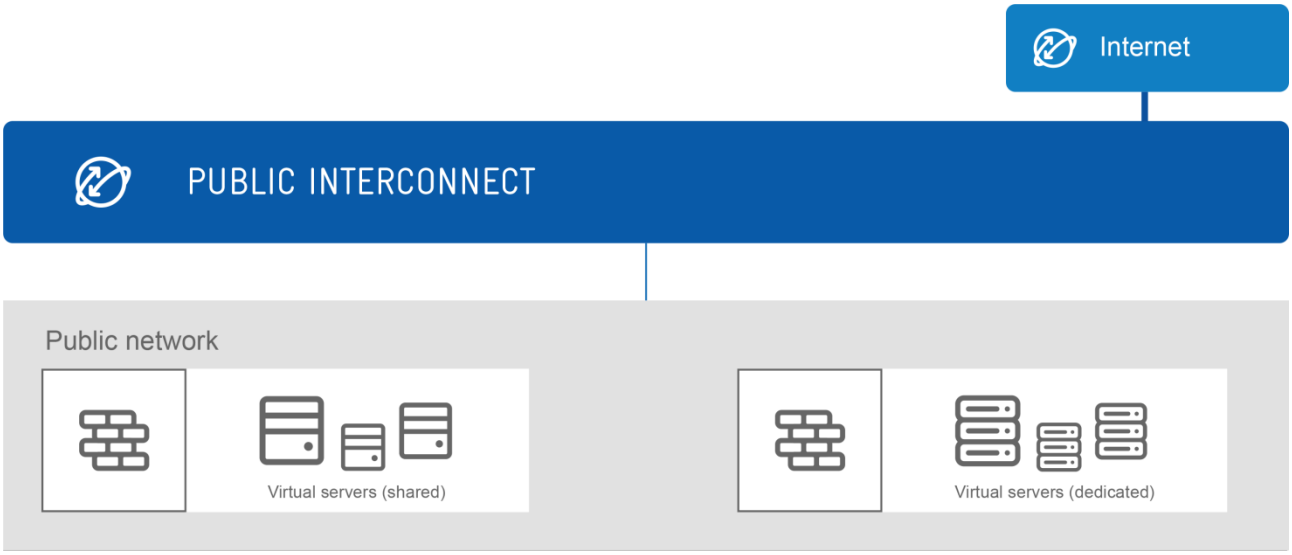
CHAPTER 8
USING MULTIPLE VIRTUAL SERVER TYPES

There are different ***types of virtual servers*** we offer in cloud infrastructure, with varying levels of configuration control.

You can use one type of virtual server alongside virtual servers of another type. Different virtual server types can be used within a single network (public or private), or in separate networks in the same virtual data centre.

Each compute service can have its own firewall. To allow communication between two virtual servers of different types, within a single network (public or private), separate firewall rules need to be configured for each compute service within the network.

If load balancers are required, a single load balancer can service all virtual servers within a network, regardless of their type.



WHY USE MULTIPLE VIRTUAL SERVER TYPES?

There are several situations where you may want to use a combination of virtual server types.

For example:

Testing environments

Virtual Server (Shared) could be used to create a testing environment with lower, more variable traffic volume in and out of testing phases.

Simultaneously, it may be more efficient to run a production application on Virtual Server (Dedicated), assuming your resource demand is relatively constant.

Additional short term capacity

You may want to use Virtual Server (Dedicated) Gen2 to handle your core traffic volumes, and use Virtual Server (Shared) to meet spikes in traffic.

Virtual Server (Shared) can be quickly provisioned, and allow you to efficiently use shared resources for short periods of time.