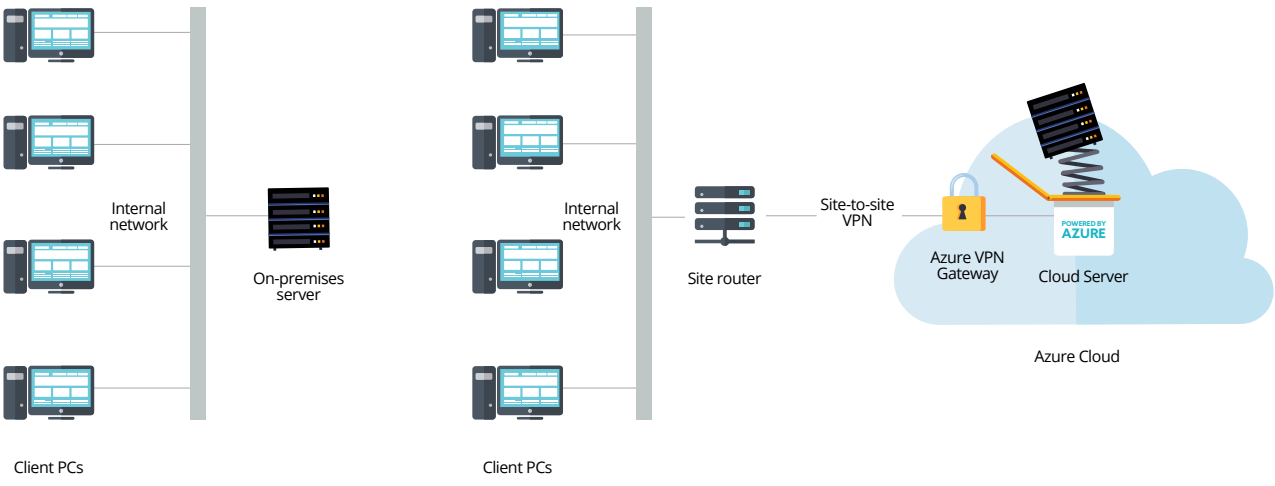
CLOUD SERVER USE CASES

INTRODUCTION

You can use Cloud Server for anything you would use an on-premises server for – any applications you can run on a physical server can also be run on a Cloud Server. You install the software, or configure the roles, exactly as you would on-premises. In this document we show a few example use cases, but there will be many more.

CONNECTING TO CLOUD SERVER FROM THE OFFICE

The only operational difference between a Cloud Server from Giacom and a physical server in your customer's office is the way you and your users connect to it. With an on-premises server, typically it is on the same network as the client PCs, as in the diagram below:



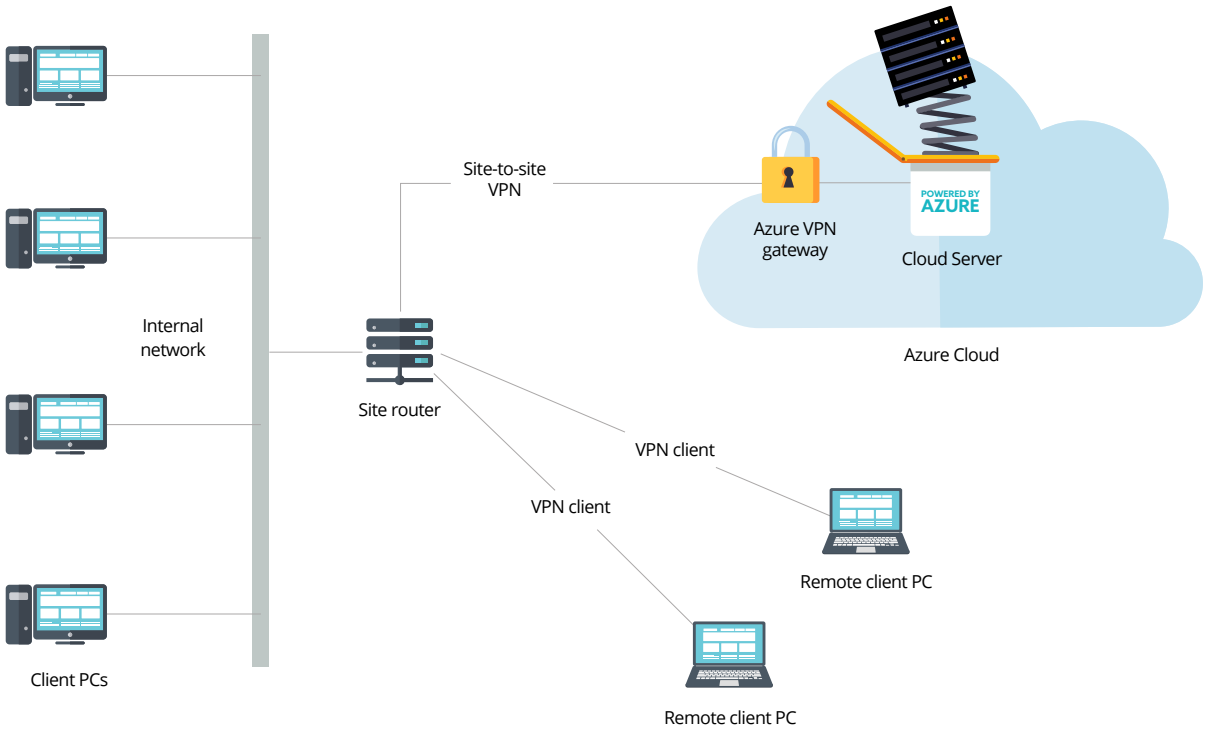
GIACOM™

When we deploy a Cloud Server it will exist on its own virtual network in the Azure cloud. We can connect it to the office network using a site-to-site VPN, as shown in the diagram on the right. Although the server is no longer in the building, the clients access it just as they did when it was on-premises. In effect we have just extended the office network beyond the boundaries of the physical building. Some of the benefits of Cloud Server vs. on-premises server are:

- Predictable monthly costs with no upfront capital investment
- No need to provide a separate controlled environment for the server
- No worries about hardware failure or replacement
- Optional fully automated backup
- Other services (e.g. web sites) can be served publicly from the Cloud Server without opening up access to the customer network

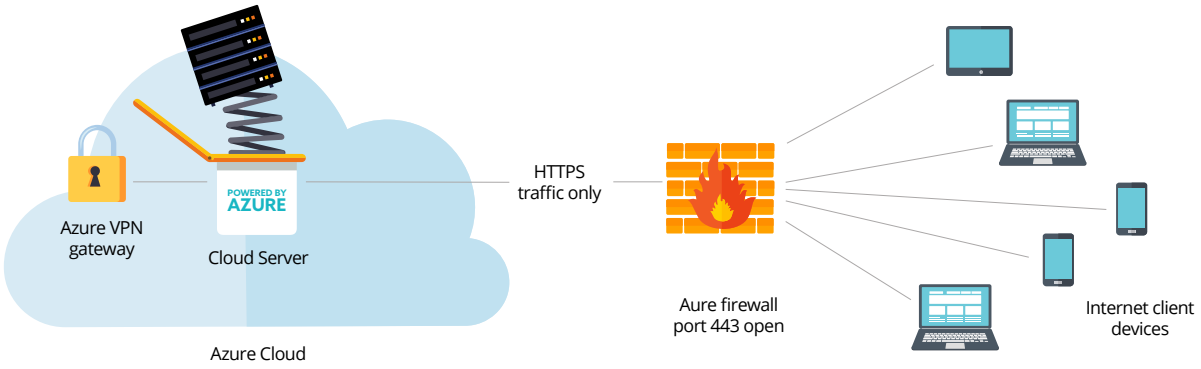
CONNECTING TO CLOUD SERVER – REMOTE USERS

Remote users can first connect to the office network using a VPN client – most business-grade firewalls will have a proprietary VPN client enabling users to connect securely from outside of the office network, e.g. from home or a customer site. Windows also has a built-in VPN client which can perform the same function if the office firewall supports it. Again, this is exactly how they would access an on-premises server from a remote location.



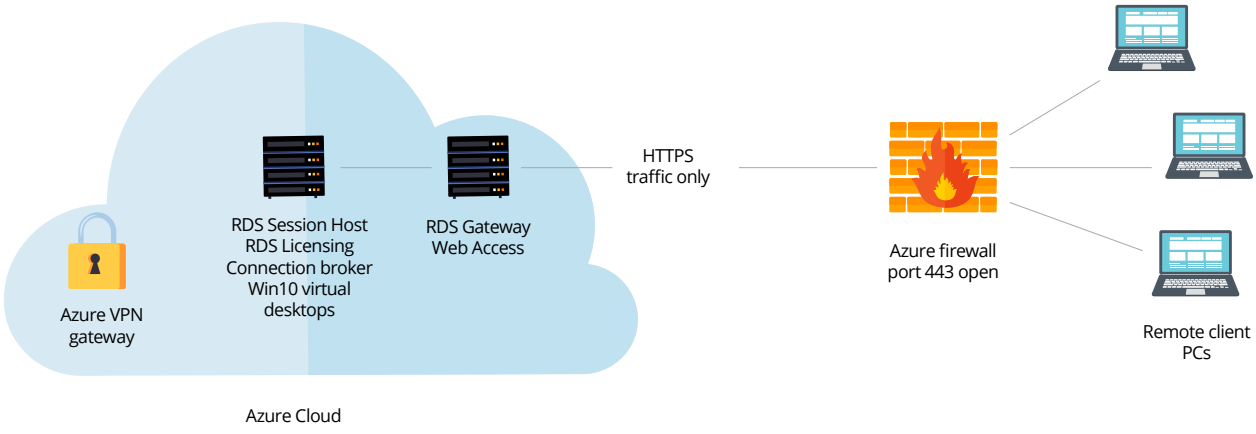
PUBLIC CONNECTIONS TO CLOUD SERVER – (E.G. WEB SERVER)

Connections to public-facing services can be facilitated by using the Cloud Server firewall, which is included with Cloud Server. These users will connect directly over the internet without any interaction with the customer's local network.



WEB ACCESS TO REMOTE DESKTOP SERVICES

By deploying 2 Cloud Servers, you can provide web-based access to Windows 10 virtual machines hosted in RDS. The Azure firewall is configured to only pass port 443 traffic to the RDS Gateway/Web Access server, which in turn communicates with the Connection Broker, Licencing and Session Host server.



GIACOM™

EXAMPLE USE CASES

Here are a few typical use cases for Cloud Server. Remember, they are no different to ways in which you might use an on-premises server, except for the way we connect to the Cloud Server.

APPLICATION SERVER E.G. ACCOUNTING, CRM	
What server would I need?	It is always worth checking the vendor's system requirements to establish which Cloud Server to provision. If there is an on-premises server already hosting the application, refer to that to estimate the disk capacity required.
How would the users connect?	Ideally, use a site-to-site VPN to a central office location then allow users to connect to the office through a client VPN. If this isn't possible, you could access directly over the internet, but you should make the firewall rules tight and ensure the users have strong passwords for the Sage and SQL servers
Any additional costs?	• You may need to purchase a SQL Server license if the application requires one, unless: you transfer one you have already, or you use SQL Server Express Edition, which is free (and is often included with server apps) • We recommend Cloud Server backup or Acronis Cloud Backup
Other considerations?	Check for any potential performance issues running your application remotely. The vendors knowledgebase may have tips to mitigate any known issues, such as pre-processing reports on the server, for example

FILE SERVER INCLUDING ACTIVE DIRECTORY DOMAIN SERVICES	
What server would I need?	An entry server will generally suffice as a combined AD/file server as this is not usually a heavy workload. Again careful estimation of required storage capacity is key
How would the users connect?	A site-to-site VPN with users connecting via client VPN is recommended. If you wish to use a Cloud Server as an additional domain controller for an existing domain, site-to-site VPN is essential
Any additional costs?	We recommend Cloud Server backup or Acronis Cloud Backup
Other considerations?	If you choose you can synchronise user account information with Azure AD (for existing Office 365 users) by adding the Azure AD Connect agent. This will give users Single Sign-On capability between Office 365 and the domain login and will also allow you more flexibility in setting password policies

WEB SERVER	
What server would I need?	An entry server will generally suffice as a web server for up to 20 concurrent users. If usage will be higher, apply the standard RAM calculations for IIS to ensure the correct server is specified
How would the users connect?	A site-to-site VPN with administrative users connecting via client VPN is recommended, although admin users could connect directly as long as the firewall rule tied access to specific IP addresses.Public users would connect over port 443 (HTTPS) as normal
Any additional costs?	We recommend Cloud Server backup or Acronis Cloud Backup to ensure that web server code and data is backed up
Other considerations?	For low volume use, an Entry server could accommodate a Microsoft SQL Server Express or MySQL instance. As the Cloud Server offering is currently Windows only, IIS would be the recommended web service platform

REMOTE DESKTOP SERVICES	
What server would I need?	Supporting multiple remote desktops or applications is very resource-heavy, so using a Premium Plus server to host the RDS Session Host and Connection Broker would be the best option
How would the users connect?	A site-to-site VPN with users connecting via client VPN is possible, which would not require the RDS Gateway. If client VPN can't be used, then the Remote Desktop Gateway service would be required – for a production environment it is strongly recommended that this be a separate server. This could be a Standard server for a light to medium load – heavier loads would require Premium
Any additional costs?	• Each user would require an RDS CAL • We recommend Cloud Server backup or Acronis Cloud Backup to ensure that user data is protected • An SSL certificate from a trusted authority (e.g. GoDaddy, Verisign, etc.) would be required to secure the connection
Other considerations?	If you choose you can synchronise user account information with Azure AD (for existing Office 365 users) by adding the Azure AD Connect agent. This will give users Single Sign-On capability between Office 365 and the domain login and will also allow you more flexibility in setting password policies

GIACOM™

ROLE	ENTRY	STANDARD	PREMIUM	PREMIUM +	NOTES
Domain Controller	✓	✓	✓	✓	
IIS	✓	✓	✓	✓	
Microsoft SQL Server	x	✓	✓	✓	SQL licences available to purchase separately via Giacom or use existing SQL licences
WSUS	✓	✓	✓	✓	
File Sharing	✓	✓	✓	✓	Migrate using Robocopy
Remote Desktop Services	x	x	✓	✓	RDS CAL licences available to purchase separately via Giacom or use existing RDS CAL licences

TOP TIP: We'd recommend using an Entry Level server for single service or role usage only. If your customer is looking to host several applications, multi role servers would be best practice so as not to add to system and configuration complexity. We've investigated several key services and specified what server size is best for multi role purposes.

ROLE	ENTRY	STANDARD	PREMIUM	PREMIUM +	NOTES
Domain Controller + WSUS + File Share	x	✓	✓	✓	
IIS + Microsoft SQL Server	x	✓	✓	✓	SQL licences available to purchase separately via Giacom or use existing SQL licences
IIS + MySQL	x	✓	✓	✓	