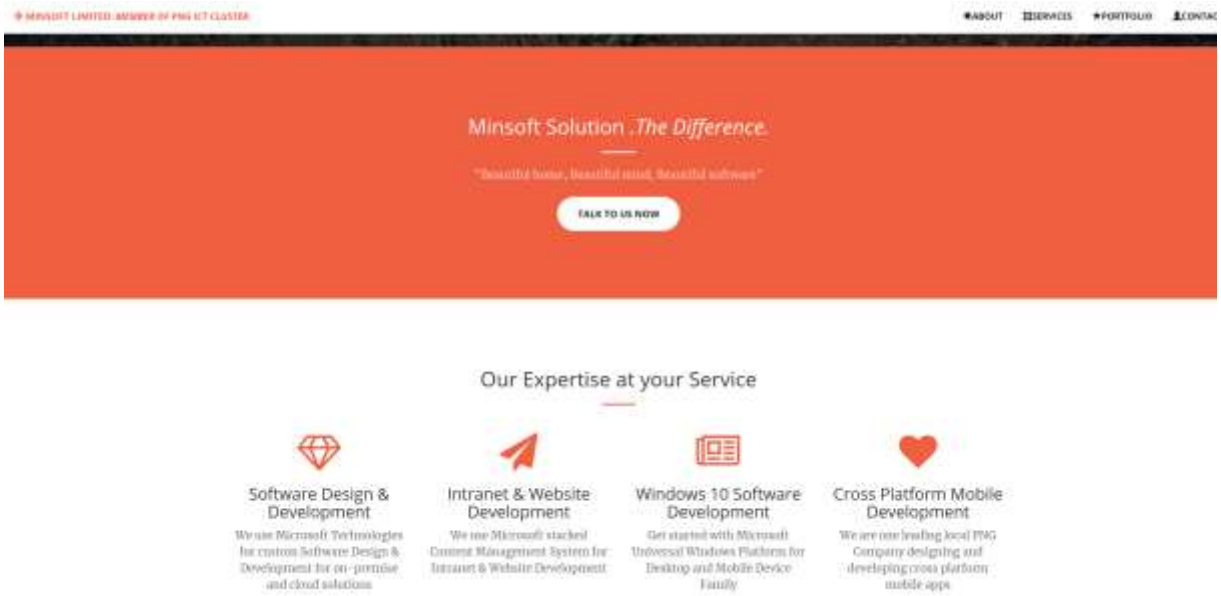
PNG COMPUTER SOCIETY 2017

Data Silos & Adoption of Cloud Web API Technology in Papua New Guinea



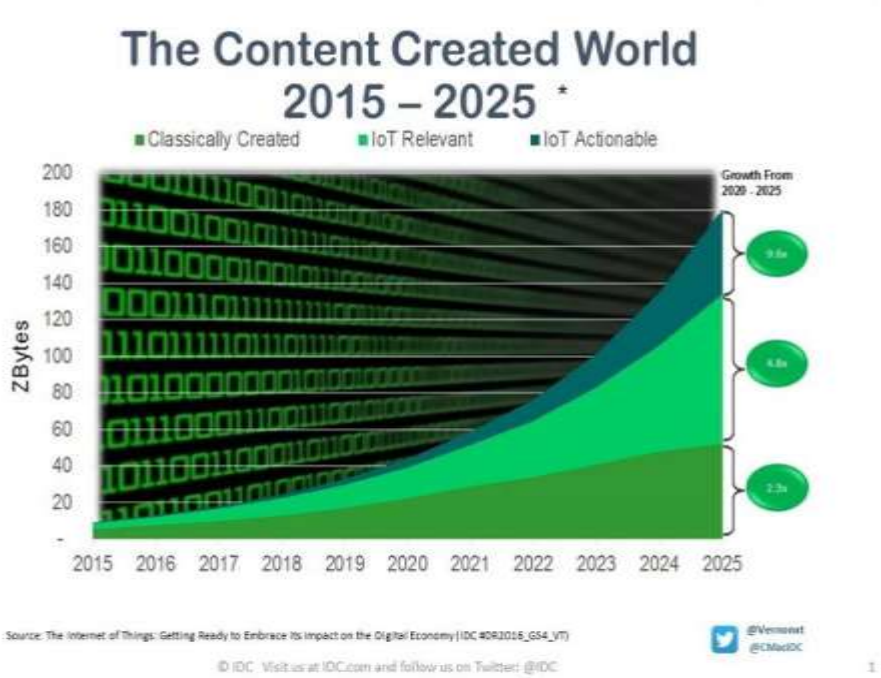
Leonard Wanusim

Minsoft Limited

November 15, 2017

Abstract

Cloud and mobile computing are driving demand for a never-ending supply of new applications as enterprises move toward digital transformation. $203 billion. That's what International Data Corporation (IDC) projects global revenue from big data will reach in 2020. By 2025, we'll produce 180 Zettabytes of data annually, much of it from IoT.



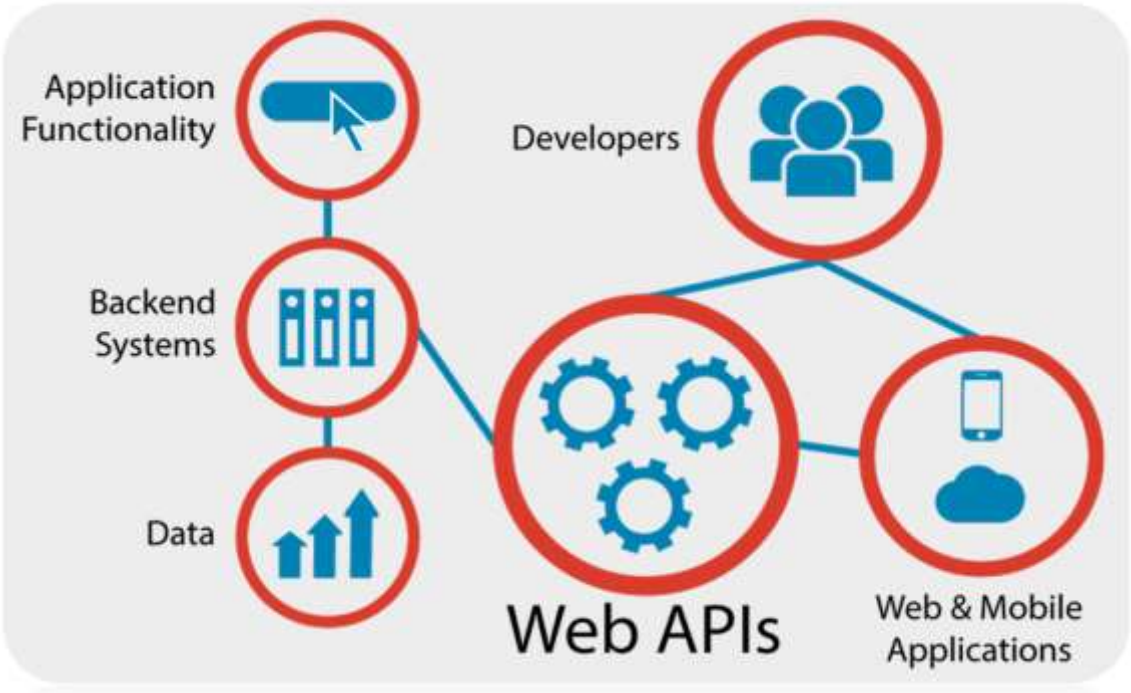
The evidence is clear: We're amid a data boom, driven by the increased ability to gather, store and analyze data with a seemingly endless reduction in the cost to do so. Amid this cosmic growth on the global stage, PNG based technology leaders need to know: What are the trends to pay attention to now and in the coming years. Department Heads especially the ICT Managers ready to take advantage of these trends and harness the power of data will be the ones who create the future in 2018 and beyond.

Now adopting and adapting this technological phenomenal change in Papua New Guinea is what this paper will try to discuss and provide a practical solution approach in the area of data silos which has had a negative impact in the ICT and overall economy.

Introduction

One thing common in Papua New Guinea is that "Most PNG Government Department/Entities operate Data Silos". Silo mentality is caused by divergent goals of different organizational units. Silo mentality preferably occurs in larger organizations and can lead to a decreased performance and has a negative adverse impact on the corporate culture. Silo mentality can be countered by the introduction of shared goals, the increase of internal networking activities and the flatting of hierarchies.

This paper introduces one common approach using Web API Technology together with Cloud Services such as IaaS, PaaS, and SaaS to counter information silos and aid in moving PNG with the changing technology.



The benefits of using Web API Technology is not new however the time is right for a practical adoption in Papua New Guinea to realize the following: -

- Greater Data Sharing
- Improved Data Security and Data Integrity
- Reduction in Cost
- Revenue Generation
- Embracing trending technologies like IoT and Block Chain

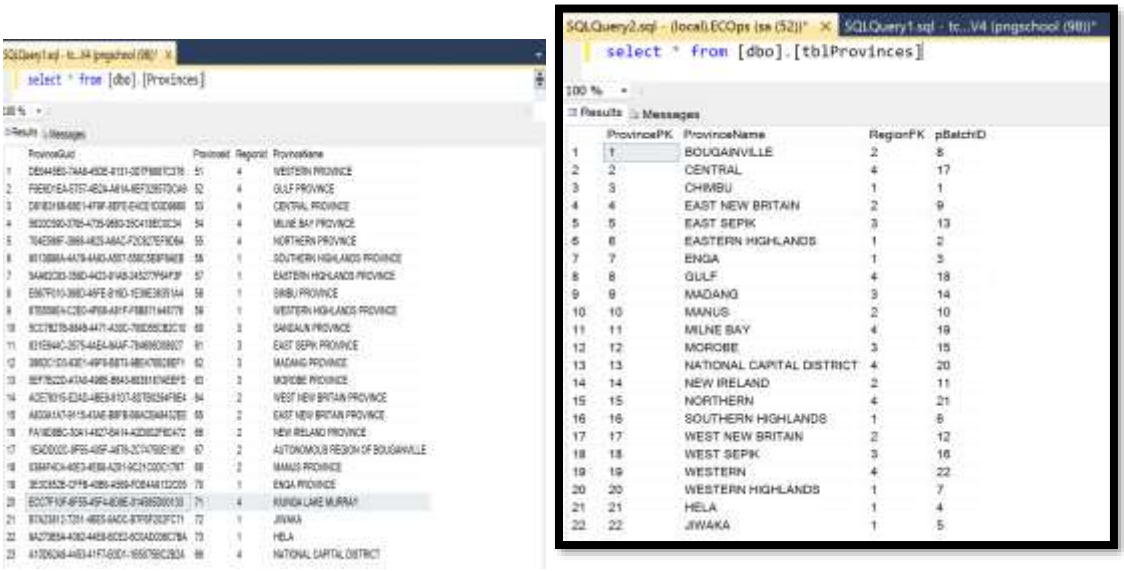
Data Silo in Papua New Guinea

Data silos tend to arise naturally in large organizations because each organizational unit has different goals, priorities and responsibilities. Data silos can also occur when departments compete with each other instead of working with each other towards common business goals. Information silos are generally viewed as a hindrance to effective business operations and organizations are increasingly trying to break down silos that are a barrier to collaboration, accessibility and efficiency.

In recent years, data silos have faced increasing criticism not only because they impede productivity but also because solos negatively impact data integrity. When two or more in-house silos exist for the same data, their contents are likely to differ, creating confusion as to which repository represents the most up-to-date version. As a result, current (or more recent) data may accidentally get overwritten with outdated (or less recent) data.

Although it can be challenging to integrate data from systems that were not originally intended to work together, cloud storage is helping organizations to create a more unified view of data, provide better access to data and help ensure data consistency.

Example of Data Silo: Department of Education and PNG Electoral Commission Province List in Dec 2017



```
select * from [dbo].[tblProvinces]
```

	ProvincePK	ProvinceName	RegionFK	pBatchID
1	1	BOUGAINVILLE	2	8
2	2	CENTRAL	4	17
3	3	CHIMBU	1	1
4	4	EAST NEW BRITAIN	2	9
5	5	EAST SEPIK	3	13
6	6	EASTERN HIGHLANDS	1	2
7	7	ENGA	1	3
8	8	GULF	4	18
9	9	MADANG	3	14
10	10	MANUS	2	10
11	11	MILNE BAY	4	19
12	12	MOROBE	3	15
13	13	NATIONAL CAPITAL DISTRICT	4	20
14	14	NEW IRELAND	2	11
15	15	NORTHERN	4	21
16	16	SOUTHERN HIGHLANDS	1	6
17	17	WEST NEW BRITAIN	2	12
18	18	WEST SEPIK	3	16
19	19	WESTERN	4	22
20	20	WESTERN HIGHLANDS	1	7
21	21	HELA	1	4
22	22	JIWAKA	1	5

The above relational tables show major inconsistencies and un-uniformity of Province listing between two major PNG Service Departments. Data in PNG Electoral Commission is more updated then PNG Department of Education however the true custodian of this data is the Department of Province and Local Level Government.

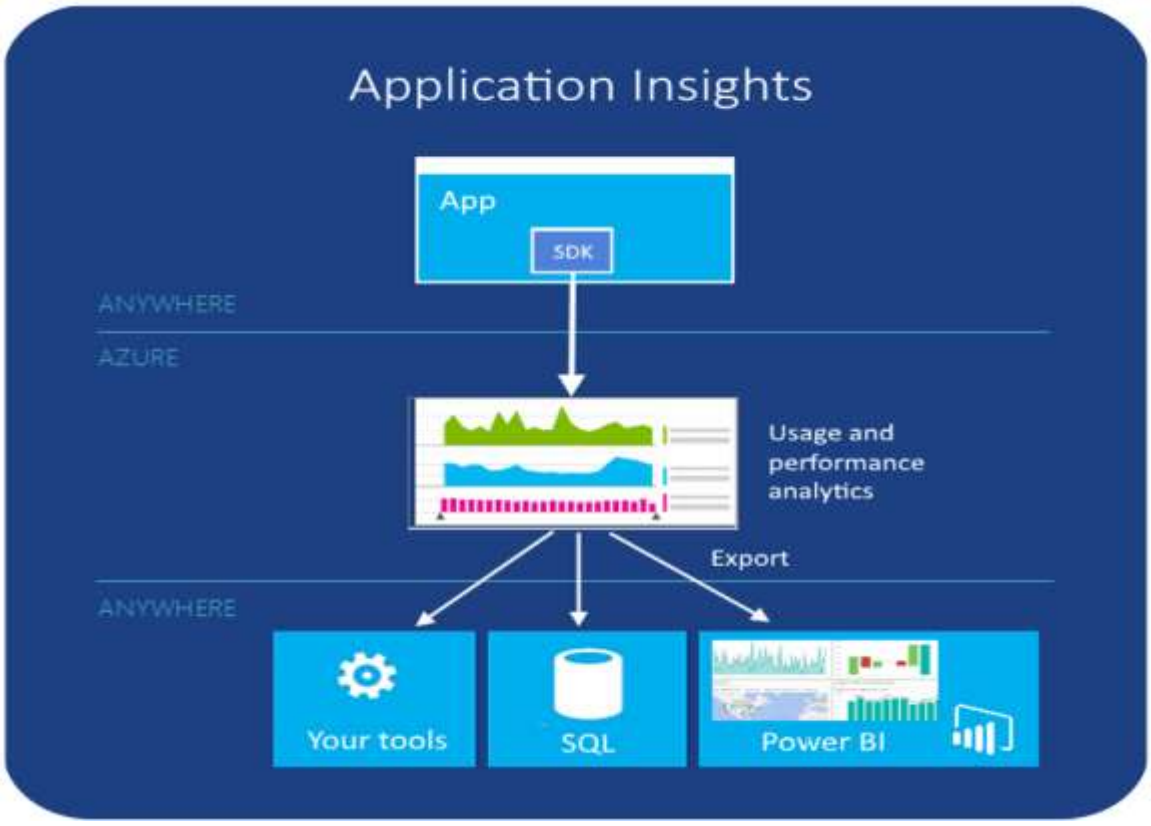
In Papua New Guinea we have Civil Registry, NSO, PNG Electoral Commission, Police, CIS, PDM and Hospitals all managing their own citizens data and some of these organizations are selling data. NID project is a functional data store and falls short in exposing public interface for accessibility by third party data consumers.

Cloud Web API Technology

A true counter solution for data silos in Papua New Guinea is applying cloud web api technology. Many governments collect a lot of data, and some developed governments are now opening access to this data. The interfaces through which this data is typically made accessible are web APIs. Web APIs allow for data, such as "budget, public works, crime, legal, NID, Boundaries, Electoral Roll" to be accessed and consumed by any third party in a convenient manner.

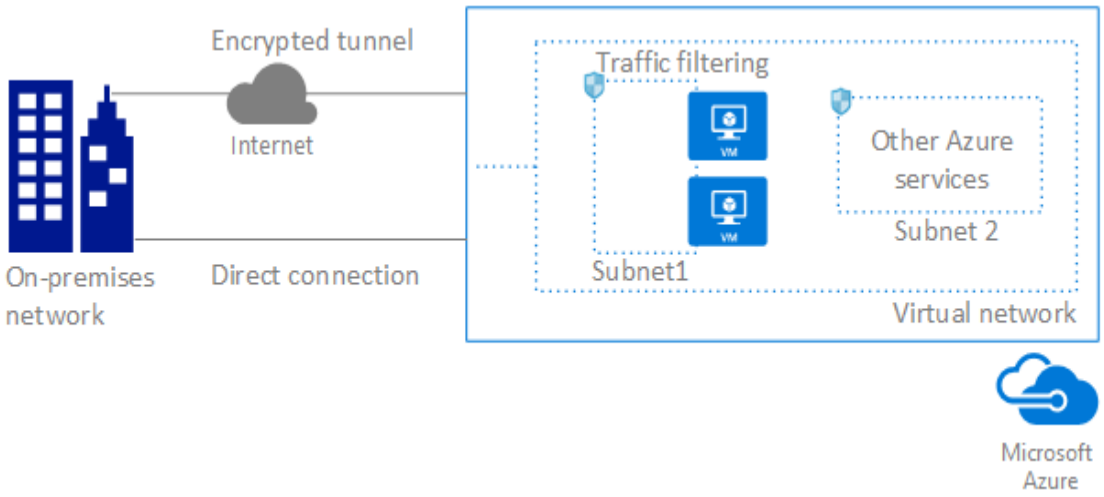
A web API is an application programming interface (API) for either a web server or a web browser. A server-side web API is a programmatic interface consisting of one or more publicly exposed endpoints to a defined request–response message system, typically expressed in JSON or XML, which is exposed via the web—most commonly by means of an HTTP-based web server.

With popular trending technologies like IoT, AI and Block Chain the application of Cloud Web API is the way forward for addressing data silos in Papua New Guinea.



The API allows app connectivity of corporate or local network using on-premise connections with enterprise-grade security. The application insights allow usage and performance analytics anywhere everywhere which can be billed to generate revenue for departments and organizations selling data.

With big name Cloud service providers like Google and Microsoft, PNG Government Departments and Entities can establish Virtual Network and use one or more of the services like Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). ***Microsoft Azure which is a cloud service provided by Microsoft is a choice implementation.***



Capabilities of the Azure Virtual Network service

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with other in a virtual network. A virtual network is a representation of your own network in the cloud. A virtual network is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or to your on-premises network.

- **Isolation:** Virtual networks are isolated from one another. You can create separate virtual networks for development, testing, and production that use the same CIDR (10.0.0.0/0, for example) address blocks. Conversely, you can create multiple virtual networks that use different CIDR address blocks and connect the networks together. You can segment a virtual network into multiple subnets. Azure provides internal name resolution for virtual machines and Azure Cloud Services role instances deployed in a virtual network. You can optionally configure a virtual network to use your own DNS servers, instead of using Azure internal name resolution.

- **Internet communication:** All Azure Virtual Machines and Cloud Services role instances in a virtual network have access to the Internet, by default. You can also enable inbound access to specific resources, as needed.

- **Azure resource communication:** Azure resources such as Cloud Services and virtual machines can be deployed in the same virtual network. The resources can communicate with each other using private IP addresses, even if they are in different

subnets. Azure provides default routing between subnets, VNets, and on-premises networks, so you don't have to configure and manage routes. You can customize Azure's routing though, if desired.

- **Virtual network connectivity:** Virtual networks can be connected to each other, enabling resources in any virtual network to communicate with resources in any other virtual network.

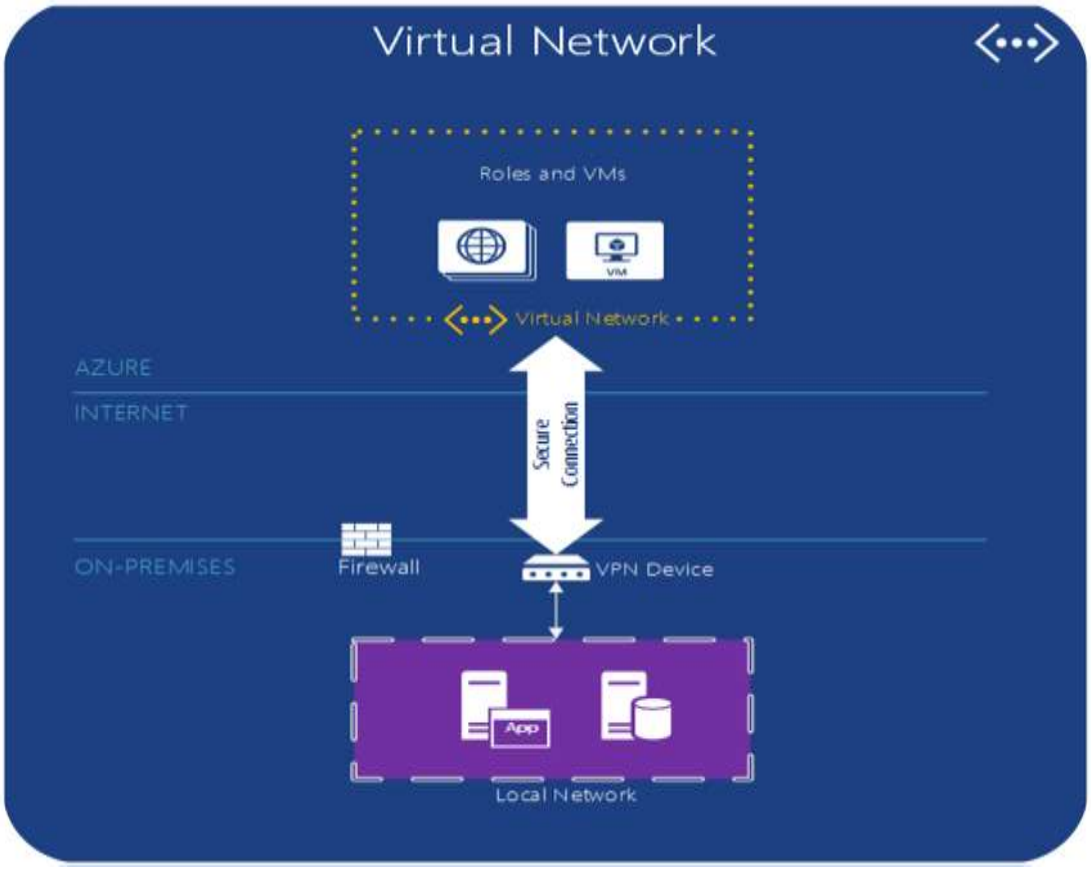
- **On-premises connectivity:** A virtual network can be privately connected to an on-premises network or by using a site-to-site VPN connection over the Internet.

- **Traffic filtering:** Virtual machines and Cloud Services role instance network traffic can be filtered inbound and outbound by source IP address and port, destination IP address and port, and protocol.

- **Routing:** You can optionally override Azure's default routing by configuring your own routes, or by propagating BGP routes through a network gateway

Microsoft Azure Network

Web API implementation will require a virtual network and Microsoft Azure is a serious contender for cloud service.



Network isolation and segmentation

You can implement multiple virtual networks within each Azure subscription and Azure region. Each virtual network is isolated from other virtual networks. For each virtual network you can:

- Specify a custom private IP address space using public and private (RFC 1918) addresses. Azure assigns resources in a virtual network a private IP address from the address space you assign.
- Segment the virtual network into one or more subnets and allocate a portion of the virtual network's address space to each subnet.
- Use Azure-provided name resolution or specify your own DNS server for use by resources in a virtual network. To learn more about name resolution in virtual networks, see Name resolution for VMs and Cloud Services article.

Internet communication

All resources in a virtual network can communicate outbound to the Internet, by default. The private IP address of the resource is source network address translated (SNAT) to a public IP address selected by the Azure infrastructure. To learn more about outbound Internet connectivity, read the Understanding outbound connections in Azure article. To prevent outbound Internet connectivity, you can implement custom routes or traffic filtering.

To communicate inbound to Azure resources from the Internet, or to communicate outbound to the Internet without SNAT, a resource must be assigned a public IP address. To learn more about public IP addresses, read the Public IP addresses article.

Secure communication between Azure resources

You can deploy virtual machines within a virtual network. Virtual machines communicate with other resources in a virtual network through a network interface. To learn more about network interfaces, see Network interfaces.

You can also deploy several other types of Azure resources to a virtual network, such as Azure Virtual Machines, Azure Cloud Services, Azure App Service Environments, and Azure Virtual Machine Scale Sets. For a complete list of Azure resources, you can deploy into a virtual network, see Virtual network service integration for Azure services.

Some resources can't be deployed into a virtual network, but enable you to restrict communication from resources within a virtual network only. To learn more about how to restrict access to resources, see Virtual network service endpoints.

Connect virtual networks

You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other using virtual network peering. The bandwidth and latency

of communication between resources in different virtual networks is the same as if the resources were in the same virtual network. To learn more about peering, read the Virtual network peering article.

Connect to an on-premises network

You can connect your on-premises network to a virtual network using any combination of the following options:

- **Point-to-site virtual private network (VPN):** Established between a virtual network and a single PC in your network. Each PC that wants to establish connectivity with a virtual network must configure their connections independently. This connection type is great if you're just getting started with Azure, or for developers, because it requires little or no changes to your existing network. The connection uses the SSTP protocol to provide encrypted communication over the Internet between the PC and a virtual network. The latency for a point-to-site VPN is unpredictable, since the traffic traverses the Internet.
- **Site-to-site VPN:** Established between your VPN device and an Azure VPN Gateway deployed in a virtual network. This connection type enables any on-premises resource you authorize to access a virtual network. The connection is an IPSec/IKE VPN that provides encrypted communication over the Internet between your on-premises device and the Azure VPN gateway. The latency for a site-to-site connection is unpredictable, since the traffic traverses the Internet.
- **Azure ExpressRoute:** Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not traverse the Internet. The latency for an ExpressRoute connection is predictable, since traffic doesn't traverse the Internet.

Filter network traffic

You can filter network traffic between subnets using either or both of the following options:

- **Network security groups:** A network security group can contain multiple inbound and outbound security rules that enable you to filter traffic by source and destination IP address, port, and protocol. You can apply a network security group to each network interface in a virtual machine. You can also apply a network security group to the subnet a network interface, or other Azure resource, is in. To learn more about network security groups, see Network security groups.
- **Network virtual appliances:** A network virtual appliance is a virtual machine running software that performs a network function, such as a firewall. View a list of available network virtual appliances in the Azure Marketplace. Network virtual appliances are also available that provide WAN optimization and other network traffic functions. Network virtual appliances are typically used with user-defined or BGP routes. You can also use a network virtual appliance to filter traffic between virtual networks.

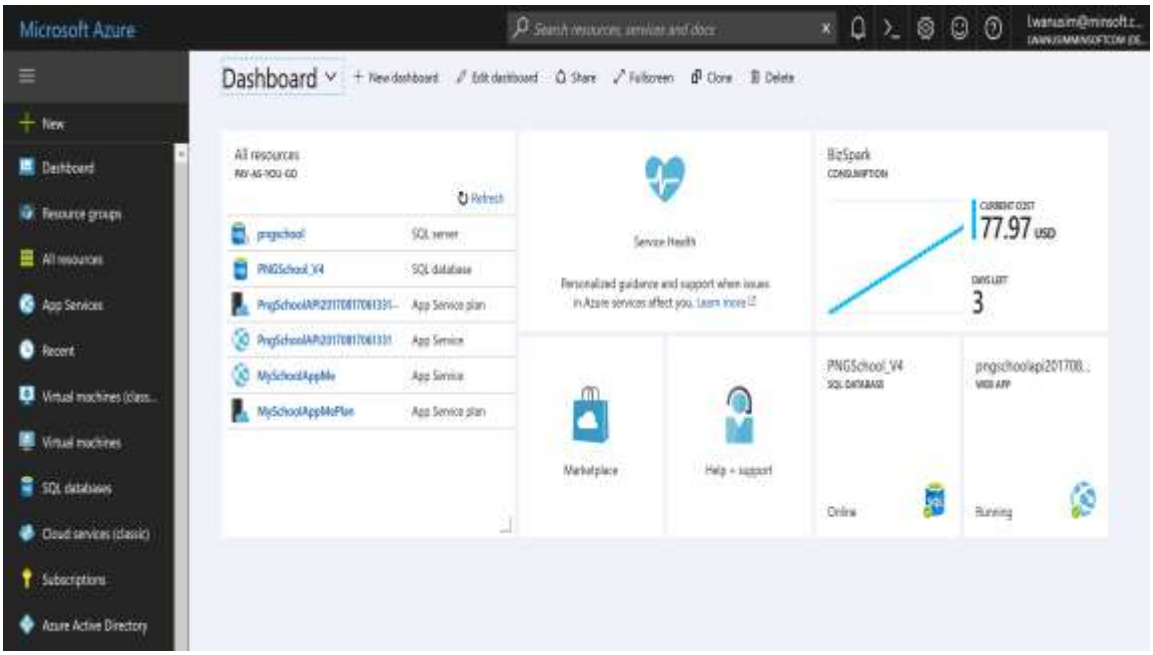
Route network traffic

Azure creates route tables that enable resources connected to any subnet in any virtual network to communicate with each other, by default. You can implement either or both of the following options to override the default routes Azure creates:

- **User-defined routes:** You can create custom route tables with routes that control where traffic is routed to for each subnet. To learn more about user-defined routes, see User-defined routes.
- **BGP routes:** If you connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute connection, you can propagate BGP routes to your virtual networks.

Pricing

There is no charge for virtual networks, subnets, route tables, or network security groups. Outbound Internet bandwidth usage, public IP addresses, virtual network peering, VPN Gateways, and ExpressRoute each have their own pricing structures. View the Virtual network, VPN Gateway, and ExpressRoute pricing pages for more information.



Minsoft Cloud Service with Microsoft Azure

Way Forward Discussion

In Papua New Guinea Data Silos will continue regardless of technological advancement because of the nature of business and its unique requirements; however, data silos as we all agree will continue to cost the National Government. Look at NID, Civil Registry, DPM, Police & CIS, Electoral Commission, Health & Education and the cost of capturing and maintain the same data.

Cloud Web API adoption in Papua New Guinea is the way forward using Virtual Network. The country has the human capacity to build these systems however it requires the policy and decision makers to properly understand the problem and solution recommended in this paper.

The excitement and benefits of technology such as block chain technology empowered by IoT and AI will become a reality when data is managed and made accessible in a secure and efficient way.

About the Author

Leonard Wanusim is the principal software architect and developer for Minsoft Limited; a software company based in Port Moresby. He has over 15 years of experience as software developer using Microsoft Technologies like .Net Framework.

Mr. Wanusim is the developer of numerous systems for clients like PNG Electoral Commission, PNG Department of Education, PNG Power, PNG Nambawan Super, PNG Office of Climate Change and NAQIA. He is also the software engineer for the PNG Roll Lookup App and the My PNG School App which was launched recently in September 2017 by the Prime Minister Hon. Peter O'Neil at the State Function Room in the National Parliament House. These two apps can be found in the Google Play Store.

Mr. Wanusim is passionate about designing and developing quality software for the PNG National Government. He has expressed interest to develop a Medical Drug Monitoring System for the PNG Health Department and a ERP including Acquittals for PNG Provincial and District Administration.

The author is available for consultancy should any client wishes to implement the Cloud Web API Technology presented in this paper. For more information visit www.minsoft.com.pg

Minsoft Limited is a proud member of PNG ICT Cluster and PNG Computer Society.