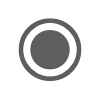
**Teams Meeting Azure Network Choosing the Right Connectivity Architecture for Your Cloud-20251030\_120536-Meeting Recording**

October 30, 2025, 10:05AM

58m 28s

 **Nicolas Blank** started transcription

 **Nicolas Blank** 0:04  
Recording has started and with that welcome everyone to the last of the October Lunch and Learn sessions for the South African Azure User Group. This week alone we have grown from 2209 members because I built the slide on Monday and every day I had to go and update it and today.  
Today, as of this morning, we were sitting at 2223 members and I think most of that happened because they knew the Warren was going to come. So kudos to the Warren.

 **Warren du Toit** 0:37  
No, they didn't.

 **Nicolas Blank** 0:40  
If you are here, it's because you've probably joined through meetup.com and you are part of the Azure User Group South Africa this week. We've had a rather full week and we are ending today, Thursday, with Azure Network choosing the right connectivity architecture for your cloud with Warren Dutoy and there is a.  
Lot to go through today. If you miss a session and you are part of the user group, don't fear because you can also navigate to the GitHub that we have built for you and you can get an idea of what has been committed this week already. Warren's session will be up by the end of today as soon as the recording has processed.

 **Warren du Toit** 1:05  
OK.

 **Nicolas Blank** 1:20  
And as an example, you can see that we give you whatever the speaker gives us if there is a PDF. If not, I still provide the transcripts in two formats as well as the video recording, which is a Teams recording.  
I have to emphasize our code of conduct because we are part of the global Azure user groups, and with that we do have a very strict inclusion policy in that we respect everyone, irrespective of their gender, sexual orientation, physical appearance, disability, age, race, or religion.

 **Warren du Toit** 1:46  
Sure.

 **Nicolas Blank** 1:56  
And we will not tolerate any behavior that is harassing or degrading in any form. If any of that is reported to us, we will evict you from the group. And with that, I'd like to introduce.  
The amazing Warren du Toit. And this description does not do him justice. It really doesn't. It was what I scraped off his LinkedIn profile and I chided him that it wasn't reflection of of how amazing he is at minimum, besides the stuff he does in the community during.

 **Warren du Toit** 2:23  
Oh.  
Yeah.  
Oh.

 **Nicolas Blank** 2:30  
Day job. He is the Cross Solutions Lead Architect for Middle East and Africa and is a Cross Solutions Lead Architect. He is multidiscipline, which means he has to be amazing at everything in multiple disciplines and craft solutions across all of us.

 **Warren du Toit** 2:33  
A.

 **Nicolas Blank** 2:47  
And as Warren starts, I'm going to hand off to him for this Azure Lunch and Learn, which is today Azure Network choosing the right connectivity architecture.  
Let me start that again. Choosing the right. I was doing so well up until that point. Connectivity architecture for your cloud. I'm going to stop sharing and fumbling of my words and hand over to you, Warren.

 **Warren du Toit** 3:06  
You are.  
Yeah.  
Thank you, Nick. That was really cool. I really like that first animation. That's super funny. It actually really looks like me laughing.

 **Nicolas Blank** 3:22  
Oh.

 **Warren du Toit** 3:24  
I'd love to know how it does that. Really, really cool. Thank you. I think Nick's pretty much said exactly what he needs to say about me, so I'm not going to say anymore, except I guess I love what I do and.  
I like to live in Azure. Every now and then we cross over to AWS because we have to, but I don't love it as much. I'm kidding. Yes, I enjoy playing around in Azure and taking people to Azure, so.  
With that, I'm going to share some stuff, and please do stop me if there's anything that you wanna ask. There's a lot of content to get through. We don't have to get through all of it today. Nick has graciously invited me back for another one, so if.  
If we don't finish, or if things are taking too long or whatever the case may be, we'll make plans to do something else. And I'm also going to leave you with some goodies. There's a wonderful human being, and his name is Vince Resente.  
That works along with me at Microsoft, and he was gracious enough to provide pretty much most of the PowerPoint presentation today because it's just it's so expansive, it's just beautiful. And also he provided me with a GitHub link. It's his repo, but.  
He built it with helping people how to troubleshoot and learn how Azure networking actually works. So things from VPN connections, how to.  
Monitor information flowing in and out of Vnets through gateways, doing PCAP dumps, those sorts of things so that you can understand how to troubleshoot networking inside of Azure. Are your UDRS your user defined routes working? Have they been applied to the Vnets? Have they been?  
Allocated correctly? Are the routes actually working the way they're supposed to? IP addressing correct? Have you done your subnetting correctly? All those lovely things and it's just it's beautiful. It's got some diagrams in it and I'll send that to you a little bit later. And with that, let's hit the PowerPoint presentation.  
And I'll do that and let's start O.  
We're gonna go through.  
What our backbone looks like as Microsoft and Azure, what it looks like around the world. We're going to do some networking resources, how our routing works, some of the network topologies that you can have inside of Azure Expressroute.  
I have learned over the years, instead of saying express route, to say express route. It's not because I want to be American, it's just because that's how everybody else around the world says it. So express route is actually a thing. Route means many different things to many different cultures, especially in Australia.  
We express route, VWAN, some resiliency stuff and then what Azure Maps is. So let's hope we get through all of it. Oops.  
OK, what does our global network look like? Like that? It's a bit of spaghetti, but what's cool about it is if you go to submarincablemap.com, you'll be able to see all of the Internet connectivity.  
And all of the connectivity that Microsoft has access to when we deliver our services to you. So it's a very, very busy slide and you'll see that when it comes to some of these things.  
That's pretty much what ours looks like out of that previous picture. We have more than 65 regions and at any given moment in time, I mean currently right now.  
We probably have around 500 data center projects around the world active and it generally takes anywhere between three and five years for one of those to complete. So it's actually it's, it's a big business.  
And in each one of those regions, as you can imagine, we have to deal with everything. So from workers, unions, strikes, delivery of concrete, making sure that whatever we build is green, all that lovely stuff, but we get through it.  
There's over 320 data centers. We have over 225 edge pops and we'll discuss what that means a little bit later. Over 500,000 network devices. Can you imagine managing over 500,000 network devices? It's it's pretty insane.  
And over 2 petabytes per second of WAN capacity around the planet. We have 360,000 kilometres of WAN fibre and we we pretty much own that fibre, which is pretty cool.  
Um, if you look at how our data center design works.  
You've got Earth, you've got regions, and inside of those regions you'll have zones, and generally inside of a Geo, which you could call a country inside of a Geo, we'll try to have two regions, so you'll.  
You'll see, like in South Africa, we've got South Africa North, we have South Africa West, and as part of our new data center design, we generally don't want to launch a data center unless that data center has three zones. South Africa W was launched before this happened, so South Africa N is still considered as a single zone.  
Even though there's actually more than one data center and it's still considered a single zone.  
You've got Azure zones, and those zones will always be more than 10 physical kilometers apart. We don't specify how far apart they are, but we generally do provide an SLA of around two to three milliseconds between those zones, right?  
You how far apart they are, security reasons, but you'll have AZ one, AZ two, AZ three and how we do load balancing of resources between that. So you'll see we've got subscriptions, the concept of a subscription inside of Azure where you deploy your resources.  
You'll find that when you're using a subscription, you'll have AZ1AZ2AZ3 physical locations, and then another subscription might be AZ3AZ2AZ1 physical locations. We'll actually mix and match those. They won't actually be the same, so subscription A.  
AAZ one will not be the same as subscription B's AZ one. They could be different as far as physical locations are concerned because we'll load balance the capacity as we go along. Then each inside those Azure zones we can have more than one physical data center per zone.  
So in places like West Europe, North Europe, I mean some of those zones have like 6 or 7 data centers. Inside the data centers we have stamps, we have many stamps and each one of those stamps will be custom built before we deliver them to the data center and those stamps.  
Will either be storage stamps or memory optimized stamps, compute optimized stamps, AI stamps, and these change based on generation and they get more and more efficient every time we deploy these and then inside those stamps we have racks.  
And then those racks will then consist of fault domains. And if you know your Azure, you'll know that fault domains, so that fault domains, update domains will give you a certain level of redundancy so that for instance if you've got update domains.  
And we decide to patch hosts if you've got your update domains configured correctly. When we update those hosts, your virtual machines won't be affected based on how you've configured that. And this is one of the availability set concepts concepts, but you can dig into that when we do a session on resiliency. Hint hint 99, Nick.  
Um.  
When we connect them. So you've got a, we've got what we call RNGS, which are regional network gateways and those regional network gateways, we generally have one per availability zone and those regional network gateways, nobody knows where they are.  
It was just a week internally, they don't even know where they are and they actually are separate to the actual availability zones. So you'll find that they're out of those availability zones and we've got extreme amount of scaling in there. So they can go from 100 gig to 200 gig to 1.6 terabit.  
Through any one of those RNGS at any given time, the low latency, anything sub one millisecond, super high bandwidth and we have we use an we use a protocol called Sonic which I'll dig into a little bit later.  
And then we have our edge devices where Internet peers will connect to. So this would be maps or any other of the sort of like Afrinic or Map Africa. Those will connect through our edge and then you'll have the private side which is Expressroute which connects directly in the Via service provider.  
Into our Azure routers and then that will then route into those RNGS and that will then go into the Azure region. We use software defined networking and they're controlled by an SWAN stack which is based on Sonic, which is open networking in the cloud.  
And we've developed Sonic and we have a whole bunch of partners that help us as well. And you'll see it supports things like IPV 6. We're actually supporting more and more IPV 6 as we go along and hopefully soon it'll start becoming more of the standard.  
So we've got a lot of active contributors when it comes to Sonic, and this is the stuff that we use for our software defined networking. So it's basically the Linux switch of network operating systems. How does LGO work specifically?  
As I mentioned before, you'll see that we've got SA W, we've got SA N. Inside the Africa Geo, you'll see that we've got the RNGs there sitting in the middle. Round trips between those RNGs and those DCs are sitting between one and two milliseconds with an average of 1.  
1.6 petabyte per second of traffic available. You'll see that 10 kilometer run between those and then you'll see that we've got redundant DC's in each zone and then those are connected up together and then they're connected to a ring and then those are then fired up to those RNG's and then those RNG's then connect to Global Azure.  
You'll see that, for instance, the round trip between South Africa West and South Africa N is generally around 36 milliseconds, 18 milliseconds one way, reason being physics.  
It's just very far away. I mean, you know, speed of light over 1000 kilometers physics.  
Azure networking some of the stuff that's available to you.  
As part of the Azure networking stack, there's a lot. There really, really is a lot. We've got four different pillars. So the deliver side, bottom right, load balancers. We've done a lot of work with load balancers.  
Our Azure load balancers as it stands right now are zone redundant. So when you deploy a load balancer, you can deploy a load balancer and it'll automatically be spanned across three zones in a zone supported region. So like in South African N deploy a load balancer.  
That load balancer will be spanned across all three of those zones, very similar with an application gateway will do the same if you deploy it in the correct way. We've also got Front Door, Traffic Manager, those sorts of things. So Front Door are globally available WAF unfortunately.  
Had a bit of, as you say, bad publicity in the past couple of weeks. It's unfortunate, but sometimes it happens. And then Front Door also consists of a CDN, a content delivery network, which is part of the Front Door service which is there and then Traffic Manager, which is just a globally distributed load balancer, can work on DNS as well.  
And then we've got the protect side of things with DDOS protection on Vnets. We've got our own version of Firewall, which integrates a lot with our services. So what's cool about the Azure Firewall, it's things like VWAN, which I'll get to a little bit later.  
Azure Firewall can connect directly into VWAN hub and it can protect the hub. We've got network security groups which allow you to protect your Vnet, restrict incoming and outgoing traffic port based as well and then we've got.  
WAFs which are also part of the Application Gateway and then Vnet endpoints which allow you to keep everything private which connect up to platform as a service services. And then we've got your stock standard stuff on the left, virtual networks which are same as VPCs in AWS.  
We've got VPN gateways, VPN tunnels, we've got DNS, we've got private DNS, we've got public DNS. Our DNS infrastructure is actually pretty incredible if you have to dig into the architecture around DNS. So something that happened to a WS couple weeks ago would probably never happen to us because we learned our lesson the last time.  
So you'll see that we've actually got two sets of redundant DNS resolvers that we use globally. They're replicated globally. We've actually got a Linux set and a window set that are completely redundant and is completely replicated with one another. So the chances of our DNS going down are very, very, very small.  
Our Express Routes, we've got a lot of different options there, which I'll get to a little bit later. We've got our VWAN hubs and again, what would all of this be if we didn't monitor it? So we've got Azure Monitor, Network Monitor, KX Monitors, which I can take you through a little bit later and again that GitHub repo.  
Advances deployed will help you use that to the best of your ability so that you can troubleshoot all of the stuff that I've just mentioned. We've made some really cool new updates that are in preview which allow you to have the single pane of glass view.  
Or your networking. So we've got the hybrid connectivity pane now, which allows you to check your Expressroute circuits, any of your route filters for BGP, some of your VPN gateways, what your VWAN hubs look like, and if you've got any route servers.  
Active inside of your inside of your subscription tenant. We've also got the network foundation pane, which gives you access to all of your virtual networks, your DNS zones, traffic managers, any of your private endpoints, any of your network interfaces attached to any of your VMS, your network security groups, public IP business.  
All that cool stuff as well. We've also got the Network Security Pane, which you can help admin your Azure firewalls, any of the policies that are in your Firewall Manager, the DDoS protection on your Vnets, your virtual hubs and your virtual networks. So we're creating this single pane of glass view so that you can look at.  
This from a bird's eye so that we've also got something really cool. It's a little bit later. I'll show it to you. We've got Azure Virtual Network Manager, which is really cool. It allows you to deploy different policies down to all of your Vnets. So if you're making a routing change, it's actually quite cool.  
Um.  
We've got Storage Center now, also single pane of glass view. You'll see that we've also released this new, this new update called Storage Discovery, which is also really cool, which allows you to scan all of your storage accounts and understand what your storage ecosystem looks like.  
We can also manage your private connectivity here for all of your storage accounts. I am. I know I'm going a little bit fast, but I've got a lot to get to. Then we've got our cloud adoption framework and.  
I know everybody's heard us beat this drum, but the Cloud Adoption Framework is very important. You can see that we've actually updated it recently. There's a couple of new extra blocks. You'll see there's this AI Services subscription.  
Down there at the bottom that we've also got this next piece here and you'll see sort of in the top. I know it's it's it's grayed out, but you'll see the top left. We've got a security subscription now which has been made standard and then landing zones themselves have been split into a platform side and an application side.  
So that you can delineate between those, but they can still become part of those landing zone designs that you do up front. So we've singled out the connectivity subscription here specifically because as part of the cloud adoption framework.  
In your regions, you can excuse me. In your regions, depending on the design that you've chosen, you can choose to automate this entire process using infrastructure as code, Terraform, Bicep, whatever you choose. You can have your expression circuits, your firewall policies, your NVAS.  
Let's say you choose to use Palo Alto, Fortinet, whatever the case may be. You can deploy those inside of this using infrastructure as code, and again you can deploy them redundantly. You can make them. You can do the role based access control for all of your network admins.  
You can make sure that the monitoring is done and everything all via infrastructure as code based on the Cloud Adoption Framework. And we give you a lot of these templates so that you can deploy these connectivity subscriptions relatively easy and the policies that lie on top of them which would go into your management groups.  
And in those management groups, you then add your connectivity description into that so that all of these policies will apply to the subscription. What does secure networking look like? I added this in because this is quite important with today because.  
Everything's AI. And what would life be without an AI landing zone? What would life be without a secure AI landing zone? So in this particular picture, you'll see we've got our connectivity subscription on the right hand side.  
We've got our management groups that are managing it and let's say we've connected up to on-prem. We could even connect to a WS, doesn't matter. You'll see that we've then got a peer, a virtual network and peered to another network and inside that network we've got a landing zone which has been designed for an AI application.  
You'll see that there's a whole bunch of private endpoints in the middle. Reason being you'll see that we've got whoops.  
You'll see that we've got the dump box over here. We've got a storage account which has got private endpoint over there. We've got AI Search with a private endpoint, Cosmos DB private endpoint, Key Vault private endpoint.  
AI services. So this could be something like Face API or whatever the case may be with private endoints. We've got our models.  
So anything like you could use Grok, you could use 534, you could use GPT, doesn't matter. Any of the larger language models that we support, you could then use on a private endpoint.  
It's.  
My mouse keeps doing that. OK, then you'll see that we they can go into different subnets. You can manage the routing between those subnets via NSGS. Then you'll see that we've got a container app environment which is actually managing the application. So we'd be running microservices. In this case it could be a Kubernetes cluster, it could be.  
App services choice is yours. We've got container registries, we've got app configurations. But the idea behind this is that every single one of these services is communicating internally to the network. So you've got this entire AI application which is sitting behind an application gateway, behind a web application.  
Firewall, but all of the networking and all of the private endoints has allowed you to keep that entire application inside and safe.  
So you can use as much AI as you want, but it's never going to leave the network. Cool thing is as well is you can make this entire architecture redundant. We can even have these foundry models sitting behind an API manager, so APIM API Gateway and those large language models.  
You could have one in Sweden if you wanted to. You could have your primary large language model here in South Africa, and then you could have a secondary one in Sweden. And if, let's say, the one in South Africa N had to die, we could fail over.  
Automatically to the ones in three so that you wouldn't lose access to the large language model and your application wouldn't break and you could still do that privately. It would just traverse our backbone via the private endpoint. So there's a lot of options to make sure that this is redundant. OK.  
When it comes to routing preference inside of Azure, so you'll see we've got hot potato routing, cold potato routing. So routing via our global network you'll see from you it's the local ISP. So if you route via.  
The Microsoft Global Network, let's say cold potato routing. It's going to enter Microsoft network closest to the user, so it's going to stay on our backbone until it exits closest to the router. OK, so you can think of this as.  
Um.  
Office 365, Office 365, it's going to hit us as quickly as it possibly can, and then it's going to route inside of us, inside of our network, it's going to access the services it needs to, and then it's going to exit.  
So you'll see it's the default network for all of our networking services, right? Then we've got hot potato routing, which is cost optimized. It's going to route via the Internet, which means it's up to you. It's going to enter the Microsoft region closest to the hosted service region.  
And then it's going to exit Microsoft in the same region the service is hosted. So even though it's cost optimized, it's not exactly the greatest. So you'll see that there's some descriptions around how that works.  
Then connecting to Azure, we've got the Internet, so Internet facing stuff, public IP addresses.  
Stuff that's sitting on the edge of Azure. So we would have a public IP address. You could attach that to a firewall, you could attach that to an application gateway, and then everybody would just use the Internet wherever they are to hit the cloud. Then you've got remote access, which is point to site where you've got a VPN.  
So Mac, Linux, Windows Phone, you could use AD authentication, you could use Radius. They essentially use a VPN client, they remote into Azure and they can be on the network inside of Azure. Then you go site to site. Site to site is when you've got, let's say a firewall or a VPN device.  
On premises and it establishes an IPsec tunnel into Azure. You could use BGP, you could add active, active, you could do transit routing here. This is high throughput again. You could also use something like ECMP where it load balances across multiple tunnels because you've got limitations on the IP.  
the protocol, so IKE. Then you could load balance across multiple VPN tunnels if you wanted to, and increase the throughput. Then finally we've got ExpressRoute. In ExpressRoute, you could...  
By default, not encrypted, which I'll get to a little bit later. You could run an IP6 tunnel over that to make it encrypted, but ideally that's private connectivity. So you would want to run this. You've got anything from I think 50 Meg all the way up to I think if we take.  
Express direct in this country, I think goes up to 40 gig per second now. I think it was just. Oh no, wait, it's 100. It's 100 now. I think it's 100 now. Um, Express, Express route will get to 100. Um.  
As far as speeds are concerned, providing the switching and the service provider supports it. Then inside of Azure we've got Vnet peering, you've got Vnet to Vnet gateways and then private link. Private link is cool because it can also work cross region.  
Like I said about the AI thing, but it can also work cross tenant. So for instance if you let's say you've got a hosted service from someone like Mongo DB. So Mongo DB has a service called Atlas where they spin up.  
A database service inside of their tenant which they manage, but then they will give you a private link and that private link will be inside your subscription inside your tenant and you'll have an IP address locally in your Vnet.  
But then using our software defined networking, you're then connected to their tenant privately to the service that they provide. We've got Azure VWAN, which is our software defined networking for WANS, which is branch to Vnet, Vnet to branch, Vnet to Vnet.  
We can do VPN, we can do Expressroute, and then we've got Expressroute Global Reach. Global Reach is great because what that allows us to do is it allows you to have DC to DC connectivity via our backbone. So for instance, if you've got an Expressroute circuit here in South Africa, you.  
Connect to our data centers, but then you've got an express route in the UK and you connect to our data centers. We can allow you connectivity from South Africa, your South Africa branch or DC to your UK branch or DC over our backbone.  
So it'll take the Expressroute from this side and connect it to the Expressroute on that side and you can route over our backbone as opposed to paying a service provider for a link or for an MPLS link that traverses the entire world.  
Then it's apologies.  
We've got AVM, so Azure Virtual Network Manager, which is like I said, it was just recently released where you can define certain topologies automatically where you can say I've got a hub spoke model, you can define which one is your hub, which are your spokes.  
Then it will go automatically and create those routing definitions for you and then make sure that it applies all of those policies and effective routes to all of those different Vnets inside the ones that you've chosen. Or you could have mesh or you could have hubspoke with direct connectivity between the spokes. So if there's.  
Ever a case where you need two spokes to talk to each other, let's say you're trying to minimize cost or you're trying to decrease latency or you don't want it to necessarily go through the hub or firewall. Let's say it's a high intensity data workload or whatever the case may be, you could do that as well.  
Connecting to some of the Azure services when it comes to the IaaS, PaaS, SaaS workloads. So we've got the Expressroute private peering where you can connect to IaaS, we've got site to site or alternatively you can then do Microsoft public peering where you can connect to platform.  
As a services as well. Then you'll see that we've got site to site VPN as well connecting to a branch. We can also connect via Expressroute to IaaS from a branch as well. You could do Paas. I'm gonna just do the rest there. So ideally you could connect any one of these.  
Ways to Azure services and you'll see that there's maps there at the end, which I'll explain towards the end. So there's a whole bunch of different ways that you can connect to each one of the different services, and ideally there's a more optimal way to connect to them.  
But at the same token, you've got to understand what the costs for each one of these are. Also performance versus security as well. So there'll always be trade-offs depending on which one it is that you choose.  
And between performance, cost and security. So just be careful, take that into account whenever you're designing network infrastructure.  
Expressroute. So like I said before, you're creating a private connection between our data centers and yours. How does it work? So it supports route filters. We've got resiliency because you'll always have a primary connection and a secondary connection.  
Whoops, it's layer 3 connectivity. OK, like I said before, it also allows you to connect not just to Microsoft Cloud services, but you can use Global Reach so that you can connect to your DCS. There's dynamic routing.  
Via BGP, it also supports quality of service and again we do have connection uptime SLS as well. So it'll do private connectivity as well as platform as a service connectivity as far as Microsoft online services are concerned.  
This has changed somewhat. You can't do things like Office 365 unless you get special clearance. The recommendation is to use maps instead when it comes to Express Route Direct. Express Route Direct is when.  
You in some ways become a provider. So for instance, if you're the IT department and you're supplying connectivity to different business units inside of the organization, what we'd be doing is.  
You could have these Express Route Direct dedicated ports, so let's say 10 gig or 100 gig. And then what you can do is then carve these 10 gig circuits or 100 gig circuits up as much as you wanted in specific speeds. So you could either, let's say, use a 5221.  
For the 10 or you could do 222222 or you could just do the single 10. The idea behind this is that you can attach each one of these circuits to different virtual networks for different BU's and then you won't get this noisy neighbor type vibe where one is going to overtake from the other or alternatively.  
We've had it in situations where customers have decided they'll take an Express Route direct because they want to do a large scale migration of virtual machines. They'll go, they'll get the the 210 gig circuits, the primary, secondary, they'll bond them together. They'll have 20 gigs of throughput and they'll just smash as much as they can.  
Um.  
Then you've got local, Express Route Local, you've got Express Route Standard, Express Route Premium. There are differences. Express Route Local is obviously unlimited when it comes to egress, but again, you'll only be able to contact SA N if you're within the SA N Metro and SA W if you're in the.  
In the in sort of the Cape Town metro, then you've got standard, which is either unlimited or metered, and then you've got premium, which then allows you to do the global reach thing.  
The connectivity models, I'm going to skip that one to go through here. Express direct. I want to take the Max SEC thing into consideration quickly. So with Max SEC, you've got layer 2 encryption where you as the customer would own the key.  
You can oversubscribe slightly by creating additional circuits, and because of the Max Sick, it means that anything inside of that particular layer two would be encrypted from the start, and as a result you don't actually need to apply encryption on.  
The the link so.  
Certain financial services customers or compliant customers don't have to apply additional encryption. So you'll see that there's a letter that you have to sign. There's a whole bunch of cool stuff that has to happen there for you to get Express to Direct. We've got a couple of customers in South Africa that have it, mostly banks.  
Then you'll see that we've also got 802.1Q, so you can carry multiple Vlans over a single wire. So you can also do double tagging as well where Vlans in the trunk can overlap. So you can have an outer tag, inner tag.  
So private peering and Microsoft peering in the different Vlans, which is also quite cool. IPsec over Expressroute is.  
The way that certain customers, if they can't afford Express Route Direct, they will encrypt over Express Route so that they'll be compliant. And for links generally smaller than a gig, they can do that too site to site, which I explained before.  
Max bandwidth speed is 2.5 at the moment. If you use the correct settings for the IKE protocol, generally the limitation is around 1.4, but we've been able to push it with our new gateways so it connects over the Internet.  
Yeah, non-mission critical workloads. It uses RKE RP SEC. Then we have VWAN.  
Um.  
We've got a bunch of partners when it comes to the VWAN ecosystem. This is around security and integration into VWAN using NVA, so network virtual appliances. So we've got Fortinet for instance will integrate, they'll deploy network virtual appliances directly.  
Directly into the VWAN hub and it will be able to then secure all the traffic that goes in and out. Things like Palo Alto. Unfortunately it's not necessarily an NVA, it's more a cloud service.  
So it's like a software as a service firewall which sort of sits outside the view end, but we route the information out the view end into their cloud service and and back out it. I mean, look, the latency's not not anything to worry about, it's just it's not an actual virtual machine sitting within the tenant.  
So it can scale. It's great. It's actually a pretty rad service, but it's how they got around not having to custom design a network virtual appliance that goes into our into our hub. Checkpoint has something inside of the hub as well.  
So you've got you've got options when you're deploying a hub. The great thing about this is that it integrates directly into the hub, so you don't have to worry about all the complex routing and all that stuff as well when it comes to the Vnet.  
VWAN hub in a single region looks something like this. You'll have a VWAN hub in the region like South Africa North, and you'll have a bunch of Vnets connecting into the VWAN hub. You can then have the VPN gateways sitting inside that VWAN. You can then scale those VPN gateways using.  
Scale units depending on the amount of bandwidth you need, and then they can then do point to site to users, or they can do site to site to branches, or you can have an Expressroute gateway sitting inside of that vran as well, and it'll pretty much manage all of the routing between all of those different pieces.  
We've also got multi-region. If you're doing multi-region, you are going to want to deploy 2 VWAN hubs. So you'll have a VWAN hub in South Africa North and VWAN hub in let's say UAE central or whatever the case may be is and then those hub to hub connections.  
We'll manage the routing between those two regions, and then the Vnet attached to those regions will then be routed the same way, but we'd manage the connectivity between the regions that way. So how does it actually work?  
You'll see that we've got a Virtual Hub router. It controls the routes between all the gateways. As I said before, you'll have an MVA integrated into the Virtual Hub router. You'll see there there's a Fortinet. You have the option to have an indirect Vnet if you wanted to.  
So if let's say there's an NVA that isn't supported inside of the Vnet hub or the VWAN hub, you could create an indirect Vnet which could let's say handle your north-south traffic. So it could be like an egress firewall and then.  
You'd have, let's say, an Azure firewall on the inside which does your east West traffic. So you can have a combination of different firewalls which we do often see in financial services customers.  
You'll see down at the bottom there's the software as a service for Palo Alto. So there's a bunch of different ways you could do this. We generally do see two sets of firewalls, so you'll have one inside of the VWAN, and then you'll have one outside of the VWAN, which then manages the egress.  
So like let's say there's a bunch of IP addresses sitting on the outside of the network, they get inspected by the forty gates that then sends it into the VWAN hub, the VWAN hub will distribute it to the application service or whatever the case may be. So that's what that would look like there when it comes to the resiliency, excuse me.  
Resiliency for Express route.  
Currently in South Africa, for at least next couple months, we only have one edge location, soon to be two, but generally in most other locations you'll find that we have more than one edge location.  
And we would then have.  
Your Expressroute circuits peering to two different edge locations so that you would have redundancy. So you'd have link one, link two, primary, secondary, primary, secondary going to different edge locations so that if that one edge location went down.  
The other edge location would take over, so we don't currently have that now. We will soon. So we've also got the metro model coming out as well, and the metro model allows distinct edge locations with a single physical link, which is going to happen soon where you can have.  
The primary and secondary actually taking diverse paths as well, as opposed to just being like a like a pair.  
Hopefully that actually comes true and it doesn't slip. Jan twenty-six is in off. Let's hope. Yeah, I hope so. When it comes to the single circuit bow tie effect, we have a bunch of customers inside of South Africa that use it this way.  
So you would have Uh standard in South Africa North, Uh standard South Africa West and you'll see that there's let's say Vnet peering or using a VWAN hub and you'll see that customers create this bow tie effect.  
For now, in which case what happens is you'll have the.  
If one of the links goes down, let's say for South Africa N, you could then route via South Africa West. I mean the latency will increase, but at least you'll still have connectivity. So you'll see this would be the ideal way to create redundancy in South Africa. Plus you could also have local as well.  
In this scenario, a lot of customers do do that because local is also cheaper. The idea that you have unlimited traffic, you'd have that secondary link there as well. I explained global reach a little bit earlier. This is actually what it looks like. So for instance, if you had a DC in Joburg, DC in London.  
And you used our backbone to connect it, it would be like that. So that is what Global Reach is essentially achieving for you. So you can route traffic from one DC to another DC, but using us.  
OK.  
Then we've got disaster recovery designs, which I explained a little bit earlier, but this is just using VWAN instead. So you could have Virtual Hub A, Virtual Hub B in two regions and you could have two express short circuits.  
Both going to on premises and it'd be completely redundant. This would be with VPN as opposed to Expressroute.  
And this would be Express Route with VPN failover. So for instance, if you wanted Express Route, you have Express Route, but you don't have enough money for two, you could use VPN as a failover. So that's also possible.  
I'm gonna touch on this next subject very briefly. It can get super complicated.  
Um.  
VMware services is essentially an island. It's a private cloud. It has no connectivity to anything, so ideally you need to connect it. So excuse me, there's a bunch of different ways to do this.  
One is Expressroute, so you could deploy an Uh gateway and then you could then connect it up like you would deploy the ADS resource like so.  
And you can use Expressroute Global Reach and you'll see that it'll connect up the AVS network to your Azure Vnet and then to your DC if you wanted to connect any platform as a service services or software as a service services.  
It would then do that. So you would connect up to the Uh gateway inside of Azure on the Vnet. If you were going to be using a VWAN hub, you'd be doing it like that.  
So essentially what you're doing is you're just replacing the connectivity with the Vnet hub with a VWAN hub. So that's only real difference. Then there's IP SEC instead of an Expressroute gateway. You'd be doing that.  
So you'd have VPN on the one side, and then you'd have the Express Route gateway specifically just for the AVS network. So there's a bunch of different ways to do this, but you'd also have to have the root server for this particular way of doing things. So just remembering when you deploy an AVS network, this would be the way to do it. This is changing in.  
In ABS Gen. 2, in ABS Gen. 2, we're making it a little bit more simple. We're going to be using Vnets to attach the ABS clusters instead, so that it'll be a little bit less complicated for you to connect up your private cloud, so.  
Looking forward to that next year when it goes GA. Finally, we're looking at Maps, which is Microsoft's Microsoft Azure Peering service, which what we're trying to do here is we are essentially trying to give you.  
The closest.  
Way to get to Azure. So ideally what we're doing is we're allowing you to then peer over a service provider with us so that you could get the quickest entry point into our network. So let's say before maps you would have.  
3456 hops before you eventually hit our edge with us. What we're doing is with with maps, what you're doing is you're essentially shortcutting that. So you'll see straight down the middle there. What we're doing is we're saying you're going to go straight from you.  
With maps you can essentially one hop, 2 hops. So as opposed to it being 1234, you're going to be just going 1-2 and you're in the network. So ideally this is the best way for you to get the best performance for something like Office 365 with Teams and SharePoint.  
And those sorts of things, as opposed to using it the old way where we used to do it over Expressroutes, which was a disaster because you peer your Office 365 services and then sometimes your Windows Update would break because you get asynchronous routing or whatever the case may be.  
So this would be the best way to do it. So you'd have the shortest path to get straight through to us as opposed to going around. And with that, if you've got any questions, I know that was fast, but I think I did it in what, 45?

 **Nicolas Blank** 49:11  
You did it right on the money. That was amazing.

 **Warren du Toit** 49:16  
Right. I know it was. I was speaking fast. I'm sorry.

 **Nicolas Blank** 49:19  
No, it was great. It was great. I did give a time constraint. You stuck exactly to it, so thank you.

 **Warren du Toit** 49:22  
Huh.

 **Nicolas Blank** 49:26  
So I'd like if whoever is not completely overwhelmed, actually, let's just do cameras on and no, not at all. Cameras on and and and microphones. And let's take the opportunity for the next 4 minutes to ask questions.

 **Warren du Toit** 49:32  
Sorry, sorry.

 **Neil Knapp | Cyberlogic** 49:43  
Yep. So first of all, just want to know if that presentation is going to be available because as you say, there's like I thought I had a fair understanding of Microsoft Azure networking, but that's just it's interesting to get a peek behind the curtain and to go and see exactly what it looks like to know that you're in your own fibre. There's things that I'd have a vague understanding of, but never really lost track of about.

 **Warren du Toit** 49:56  
Hmm.  
Mm.

 **Nicolas Blank** 50:03  
Mm.

 **Neil Knapp | Cyberlogic** 50:03  
Things like using Express Route, global peering and things like with the map stuff that you brought up at the end. Now I'm already curious about who the peering partners are in South Africa and how you know who we can use because we have an ISP that we work with who are using Express Route. So they would either like to consume the service or maybe even become a partner. So those kind of questions.

 **Warren du Toit** 50:07  
Hm.  
Hmm.  
Yeah.  
Mm-hmm.  
Yeah.

 **Neil Knapp | Cyberlogic** 50:22  
So there's a lot. And then you didn't. I was waiting for you to get into things on a deep dive onto Azure Firewall because that's probably the bit that I have in my Azure calculator list more often than not is that I tend to use virtual machines and go and put down infrastructure as a service. So would love to go and get in some detail on that and the pros and cons of that, but so.

 **Warren du Toit** 50:24  
Yeah.  
Hmm.  
Yeah.  
For sure.

 **Neil Knapp | Cyberlogic** 50:42  
There's a lot. So rather than just is there, obviously we've got the recording. Is that presentation that you've prepared going to be shared publicly?

 **Warren du Toit** 50:43  
There is.  
So what I can do is I can share it with you directly. So what I'll do is I'll get the details from Nick and I'll share it with you. And then when it comes to Maps itself, just search Microsoft Azure Peering Service on Google or Bing or whatever. And when you go to the link, you'll see in our documentation you'll see there's a very.

 **Nicolas Blank** 50:54  
Yeah.

 **Neil Knapp | Cyberlogic** 51:04  
Yeah.

 **Warren du Toit** 51:09  
Clear defined list of the partners that support maps and exactly how to activate it, because you'll activate it in a tenant, I think it costs.  
I think it's like 10 or $20 a month or something dumb. I mean, it's like it could even be $5 a month. It's something silly. You turn it on and then you just do the peering on your side and it's done. That's it. And then you just start learning the roots.

 **Neil Knapp | Cyberlogic** 51:36  
OK.

 **Warren du Toit** 51:38  
Then as far as Azure Firewall's concerned, maybe Nick, we do, I mean, maybe we do a session. Yeah, maybe we do a session on like network, on like network security and turning all of those features on and off. And maybe we do like a deep dive in the portal.

 **Nicolas Blank** 51:43  
A whole session.

 **Neil Knapp | Cyberlogic** 51:55  
Yeah.

 **Warren du Toit** 51:58  
You know how to deploy it, what to deploy, where to deploy, how firewall manager works, all that lovely stuff. I did say I'd share that repo with you as well, which is here. I'm gonna put it in the chat. This is.

 **Nicolas Blank** 52:02  
Mm.

 **Warren du Toit** 52:13  
Vince's repo. You can go have a look there. What that'll do is that'll run a a PowerShell script. It'll deploy a bunch of VPN gateways. It'll connect everything up. It'll basically sort of emulate an on-premises environment and a cloud environment to connect the two together with two Ubuntu machines on either side.  
And it's going to teach you about troubleshooting the routing, the routes, which tools to use, what to install, what to look for, how to ping this one to there and you know, not to use just ICMP all the time, rather use a TCP ping as well. So there's a lot of cool stuff that's in there as well and also.  
There is an Azure firewall that actually gets deployed in that environment, so it kind of trips you up a little bit. There's kind of some cool tricks that Vince has gone and done where he configures a firewall rule that hurts you. So it's actually quite cool, yeah.

 **Neil Knapp | Cyberlogic** 53:09  
OK, excellent. Thank you. I'll take a look because I've been because that's the one that we have most with our customer facing items is that obviously you want to go and have a firewall and have good security in place. And then at the moment I'm still putting down infrastructure as a service, putting a virtual appliance on top of it. But then you lose the benefits, the advantages of the automatic redundancy that comes with Azure Firewall.

 **Warren du Toit** 53:12  
Hmm. Yeah.  
Hmm.

 **Neil Knapp | Cyberlogic** 53:29  
They're really closely integrated networking and all those kind of things. So then it's and it's it always comes down to a costing discussion that a few things I have to fail over and then so that'd be good to go and dive into some of those and so thank you for sharing the link. I shall take a look.

 **Warren du Toit** 53:29  
Yep.  
100%.  
Yeah.  
Pleasure.  
Yeah. Any other questions, just hit me up. I mean, Nick's got all my details. Yeah, I'm more than happy to help.

 **Neil Knapp | Cyberlogic** 53:46  
OK, cool.

 **Blessing Bowora | Cyberlogic** 53:57  
Thanks, Warren. I'm I'm just, I'm just overwhelmed, but I'll definitely go through the information.

 **Nicolas Blank** 53:58  
It look oh.

 **Warren du Toit** 54:01  
Yeah, you can see, you can hear my voice is already. My voice is a little hoarse from talking so fast. Yeah, there's there's there's a lot. But the cool thing is, is there's so many different things to achieve.

 **Schalk van Wyk** 54:02  
Mind blowing.

 **Blessing Bowora | Cyberlogic** 54:09  
OK.

 **Warren du Toit** 54:18  
So many different ways to achieve the same thing. So depending on the organization and depending what it is that you're trying to achieve. So like I said, financial services and compliant customers, they use everything. Like everything that I spoke about, they turn on like doesn't matter what it is.

 **Blessing Bowora | Cyberlogic** 54:19  
Yeah.

 **Nicolas Blank** 54:33  
Mm.

 **Warren du Toit** 54:38  
It doesn't matter what it costs, they just turn it on and then the complexity triples. Then there's some customers that are a little bit more forward thinking where they say no, we don't want a single virtual network and we don't want a single private endpoint. We'll use.

 **Schalk van Wyk** 54:45  
Mm.

 **Blessing Bowora | Cyberlogic** 54:46  
Yeah.

 **Warren du Toit** 54:58  
Your platform as a service firewall, we'll use the public endpoints, we'll just turn everything off, we'll use identity as the barrier, and then they're cool. And then they'll just like, that's the way they'll do stuff. And it's actually, it works very, very well. So they'll use conditional access, as Nick knows.  
Additional access, multi factor authentication, all that stuff and that's how they'll do it. So there's no. So the more old school you are as a company, the more of the stuff you'll use. The more new school you are, the less you are because the more cloud native you go.  
You go, the less you actually have to worry about all the networking. But again, we have private endpoints for most of our services now. So like that AI thing that I discussed earlier, all of the cloud native applications, Kubernetes, Azure Container apps.  
App Services, Cognos VB, SQL DB, all that stuff is available privately, so you can route to all of it and the minute you can route to it, it just becomes so much easier.

 **Nicolas Blank** 56:09  
I'm quietly well, I've been rather vocal over the years. I'm a massive fan of Azure Global WAN because I like to call it poor man's WAN because it is.

 **Blessing Bowora | Cyberlogic** 56:10  
OK.

 **Warren du Toit** 56:20  
Hmm.

 **Nicolas Blank** 56:25  
So amazing and so cheap compared to what you can do for yourself. And the fact that you can do an endpoint in in Cape Town and pop up in Brazil and your routing is just done for you via a backbone that you just couldn't afford to assemble. It's just astounding.

 **Blessing Bowora | Cyberlogic** 56:26  
Yeah.  
OK.

 **Warren du Toit** 56:29  
E.  
Mhm.  
Mm.  
Yeah, I've actually got a lab at Liquid where I've got a 200 Meg Express routes that they've graciously given me for testing purposes. I've got a Microtek.  
Device that's terminating it. I mean it's like 2000 Rand switch and it's terminating the Expressroute connection and I've got.

 **Blessing Bowora | Cyberlogic** 57:06  
Yeah.

 **Warren du Toit** 57:13  
AI stuff running in the DC in that rack, connecting to the large language model in Sweden and East US, but connecting to a virtual network here. So all my large language models, because all the latest models happen that side in Sweden.

 **Nicolas Blank** 57:22  
Yeah.

 **Warren du Toit** 57:31  
But I usually hear in a DC over a private network and it's just it's the greatest demo ever.

 **Nicolas Blank** 57:39  
Why in Sweden? Why? Why does Sweden get things first?

 **Warren du Toit** 57:43  
Sweden gets all the latest models first, and to be honest with you, I think it's just the data center where we've got the most capacity at the moment. We're deploying GPUs there like nobody's business. It's efficient, cheap cooling.

 **Nicolas Blank** 57:58  
Mm.

 **Warren du Toit** 57:59  
Because of the environment, it's nice and cold there, so we've got a lot of capacity in in Sweden.

 **Nicolas Blank** 58:02  
Yeah, yeah.  
I can see that people are dropping like flies and we've hit that time boundary. Warren, thank you so much. This has been astounding. You've been amazing as usual and I am going to lean on you for another session.

 **Warren du Toit** 58:11  
Hmm. Yeah.  
Hey there.

 **Blessing Bowora | Cyberlogic** 58:19  
Yeah.

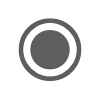
 **Warren du Toit** 58:20  
Sounds good. Have a good one. That's it. See you later. Ta ta. Bye.

 **Nicolas Blank** 58:22  
Thank you so much. Thanks everyone.

 **Blessing Bowora | Cyberlogic** 58:23  
Thanks. Thanks everybody. Yes.

 **Schalk van Wyk** 58:25  
Thank you.

 **Nicolas Blank** 58:26  
Bye, bye.

 **Nicolas Blank** stopped transcription