NYUTILITY Whiteboard session topic

Utilize Azure Cloud Services for UTILNET's Internet related needs in lieu of building a traditional on-premises Internet infrastructure.

The use case for this whiteboard session is to review the potential gains, technical and economic, for UTILNET to eliminate upcoming and ongoing CAPEX/OPEX challenges and time constructing a rigid, purpose built, UTILWAN-INT internet infrastructure.

Pending Project issue:
Currently planned UTILWAN-INT infrastructure will comprise of expensive monthly circuits, routers, switches, firewalls, load balancers, DMZ appliances, different carrier peering policies and security services while increasing overall build, maintenance and troubleshooting scope of such an infrastructure.

Considering this build effort has started only 5% of its activities to date it is prudent and not unreasonable to conduct a re-visit of direction prior moving forward.

Consideration for direction change and pivot to cloud:

The currently planned infrastructure is ridged – UTILNET must provision multiple physical routers, switches, load balancers, firewalls, security appliances and ISP circuits – possibly building another equivalent sized NYUTILITY internet platform for just an initial limited use case Internet level service.

Current planned UTILWAN-INT related concerns:

1. Increases attack footprint on UTILNET: Site A, SITE C and Azure Internet touch points.
2. Increase OPEX/CAPEX on physical devices, OS/NMS license and support plans, ISP MRC
3. Increases complexity of build x 2 sites with different ISP vendors for the following:
    - Routers
    - Switches
    - Firewalls
    - Load Balancers
    - Security FireEye type appliance
4. Brittle DMZ design
5. ISP BGP peering, routing policy and prefix list/acl management.
6. ISP DDoS
7. Maintenance, troubleshooting and management, NOC, NMS of all UTILWAN-INT components.
8. Ridged internal Routing, fail over mechanics between Site A/SITE C and troubleshooting.
9. Rigid dual ISP AS announcement policy
10. ISP /30 vs /29 for Arin anonymity, limited address constraint, unique addressing from ISP and fail over mechanics constraints.
11. Load balancing design and planning - additional complexity
12. Firewall and DMZ planning and design - additional complexity
13. Internet ripples or attack leaks are seen first in UTILWAN felt first in UTILWAN.
14. Service costs are the same regardless of use.

The initial UTILWAN-INT equipment was ordered prior to finalizing build plans during the pandemic supply chain period to ensure the project had equipment regardless.

UTILNET Currently has two active but unused ISP circuits, billed monthly. The completed design isn't final as well as initial equipment receive hasn't been touched. This current situation is costing NYUTILITY monthly to catch up based on other project priorities.

Solution - Pivot to Azure

Suggesting the order or use services already in Azure and logically provision internet northbound via Azure instead of conducting the traditional on-premises build. The same Azure infrastructure will need to be built for VDI regardless thus we are utilizing that same services and paths that may as well accommodate Internet Access traffic. Utilizing NYUTILITY's Azure team to assist with UTILNET's team also provides consistent and efficient use of knowledge and reduced provisioning delays.

Moving from a fixed always on MRC to a pay as you use for Internet service is appealing to review before committing to another rigid on-premise build. The ISP savings would help reduce projects CAPEX and OPEX(pay for only what you use).

Benefits:

1. UTILNET gains consistent failover and access radius automatically via Azure availability zones and service redundancy options.
   UTILNET gains the use of NYUTILITY Azure internet gateways or orders its own separate IG service.
2. UTILNET gains virtual CDN, load balancing, routing and DNS services all available with protection options.
3. Use Azure for UTILNET "backdoor" or general Internet egress services (PSC reporting, RDX etc).
4. Use for Ingress/Egress Internet services when islanded initially and expand when needed.
5. Can be set by Azure as "data diode" type simplex traffic flow leaving UTILWAN using WAF, CDN/EDGE, Front Door type services.
6. All services consistently provisioned in Azure vs. separate FW, ISP, peering rules, prefix-list points etc. to provision, duplicate and or keep unique and manage.
7. Build Once and set in Azure vs. build in Azure for VDI, Site A for Internet, SITE C for Internet
8. UTILNET gains a secure and flexible(how much/how little to implement) location for RDX type SFTP services. (UTILNET can host future public facing services on prem. or in Azure. However, the egress connections are still through Azure's service)
9. Utilize existing SITE B and SITE D circuits from UTILWAN for the Cloud exchange and UTILNET AZURE only express route type service. Utilize the OPEX services sitting in SITE B and SITE D.
10. Provides simple single deterministic traffic path and pattern for VDI and egress Internet flows.
11. UTILNET gains Azure's management and support services for accounting, visibility and accountability.
12. UTILNET consolidates three public attack vectors to one.
13. Reduce management/NMS footprint required to manage UTILNET assets(Azure's dashboard will cover all the Azure virtual components. No need to manage additional physical equipment.
14. Reduced troubleshooting zones. An issue encountered is zoned based. Azure virtual related vs. UTILWAN, FW, ISP, NYUTILITY etc.
15. Simple kill switch point at Virtual Network Gateway vs. dual UTILWAN-INT FW points.
16. UTILNET gains consolidation of builds – VDI infrastructure, which will use most of the same virtual component needed for UTILWAN-INT, securely share virtual service or add to same VNETS for specific UTILWAN-INT use.
17. Can be provisioned in simple small incremental steps, without carrier and site dependencies.

18. Provisioning and operation will be familiar as the VDI build so share/combine experiences.
19. Reduced OPEX initially and in future via AZURE use discount – increased services used, OPEX are lower.
20. Reduced troubleshooting via zones. An issue encountered is zoned based. An UTILNET problem will either be in the Azure Zone(virtual services) vs. in the UTILNET/UTILWAN zone of ISPs, Routers, Switches, Nutanix-HCI, FW, ISP, NYUTILITY services etc.
21. Simpler addressing and privacy - Azure provides the internet service and addressing – al cart for UTILNET on block sizes and it is registered to Azure - https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses

    Source Network Address Translation (SNAT) for outbound connections - Azure Load Balancer | Microsoft Docs

22. Security by obscurity using Azure public addresses registered to Azure
23. Many virtual security protection services, compliance and reporting services (including base DDoS and Enhanced DDoS) to complement or provide parity with InfoSec requirements. https://docs.microsoft.com/en-us/azure/security/fundamentals/network-overview

24. Northbound Azure services are isolated to UTILWAN issues and changes. UTILWAN can grow or reduce(future consolidate) in size without impacting services in Azure.
25. Always on service services to be used for UTILNET users only.
    - Auto-scale as necessary
    - Azure is responsible for the security of their cloud.
    - NYUTILITY is responsible for security in the cloud – their VNET.
    - Reduces large WAN/ISP footprint and expense.
    - AZRUE SLA/RECOURSE AND COMMITMENT
    -
26. Internet ripples or attack leaks seen first in Azure and are felt last in UTILWAN via Azure kill switch connection point.