

Mobile Phone VPN Enablement Deploying Microsoft Tunnel

Name : Geraint Jones (1908119)
Course : Networks
Email : 1908119@student.uwtsd.ac.uk

1. Introduction/aim

The project aim was to save service time within NHS Wales, when connecting to VPN, to access on premises monolithic systems.

Currently users are challenged for their username and password, plus multi factor authentication per connection, as well as phone unlock and application login. This is perceived as an unnecessary burden, which may compromise adoption.

2. Research

Showed that authentication can be replaced through addition of trusted mechanisms

- Configuring current VPN system to use certificates controlled though PKI
- Devolving identify management from VPN system to an Identify Provider, SAML token
- Deploying Microsoft Tunnel which shares O365 OAuth token, and EID conditional access

Focus was given to deploying Microsoft Tunnel (MT) looking at Microsoft Azure Public Cloud

- IaaS, costings, spend control
- Linux server and Podman containers
- FQDN, TLS Certificates
- Load balancing and Firewalls
- Certificate Pinning
- DTLS (TCP Meltdown)
- Fitting into the NHS Network
- VPN Profiles - On-Demand / Always-On / Per App

3. Design and implementation

The business opts for MT solution, figure 1, which is implement from a documented project plan, with the major challenges captured and explored such as

- Project planning choices
- Contingency
- Securing funding
- IaaS hardware selection third party tool
- Start and stop logic apps
- Governance and security
- Asymmetric routing

- Management agent connection failure (2fa) / proxy server bypass
- Unexpected consequences of start stop logic apps
- Cron start up fixes
- BGP routing
- Leveraging Intune VPN profile settings to troubleshoot split tunnelling
- Certificate creation

4. Evaluation

As the solution is yet to be enabled for service users, Smoke testing was used to evaluate the solution, as described by Memon and Xie and referenced by Whyte et al[1] smoke testing reduces cost, risk, and time to production, by testing critical functionality, against expected result, which are based on related oracles, which are knowledge on how the system should operate correctly. This built to showing the desired outcome of reducing VPN login.

5. Conclusion

Through literature review this paper explored options to resolve the aim, such as PKI, SAML and OAuth perceived compared figure 2, while defining their benefit to the aim. Through inferred feedback from other domain research[2][3], MT fulfilled the aim.

6. Methodology and references

- Qualitative
- Inductive
- Pragmatism

[1] <https://www.proquest.com/docview/900110610?pq-origsite=primo>
[2] <https://scholarspace.manoa.hawaii.edu/items/cd1bd19d-89b3-470c-8062-8332412d8bdd>
[3] <https://pubmed.ncbi.nlm.nih.gov/31423117/>
[4] <https://www.nei.nih.gov/learn-about-eye-health/eye-conditions-and-diseases/color-blindness>
[5] <https://guides.nyu.edu/posters>

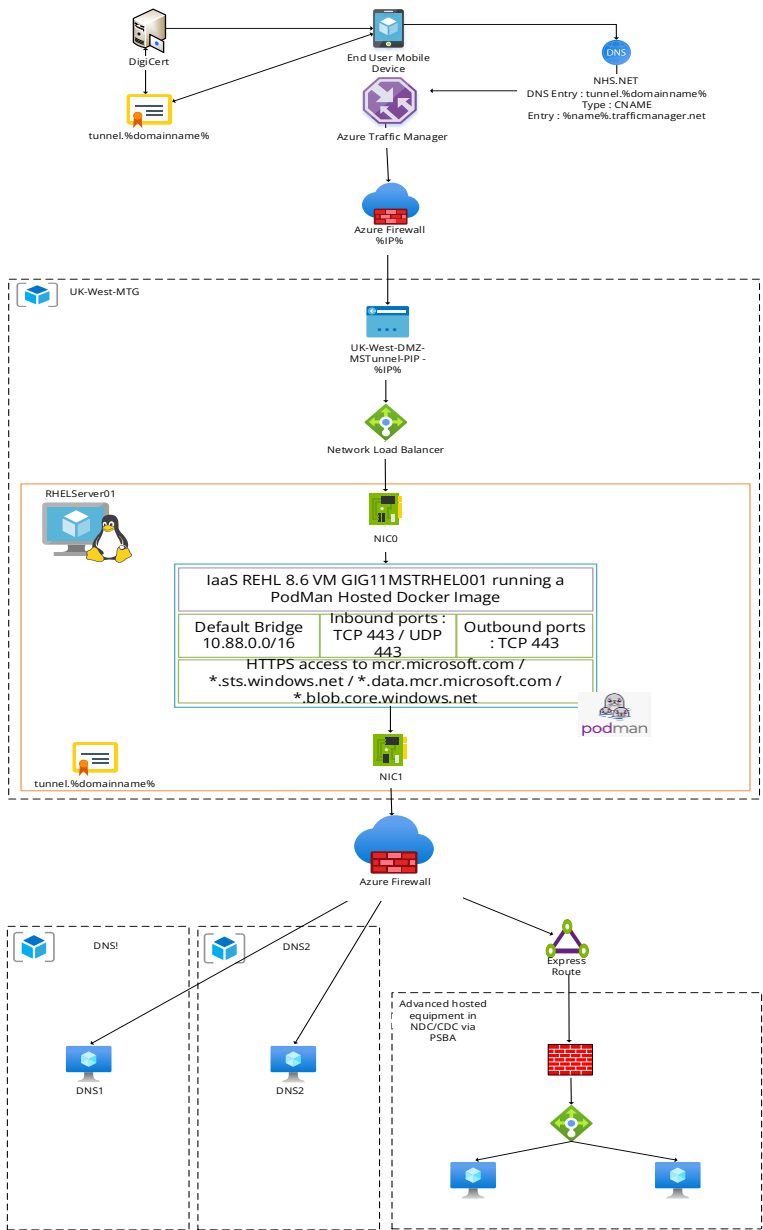


Figure 1

Comparing PKI, OAuth, SAML

Perceived administrative burden VS number of days without re authentication

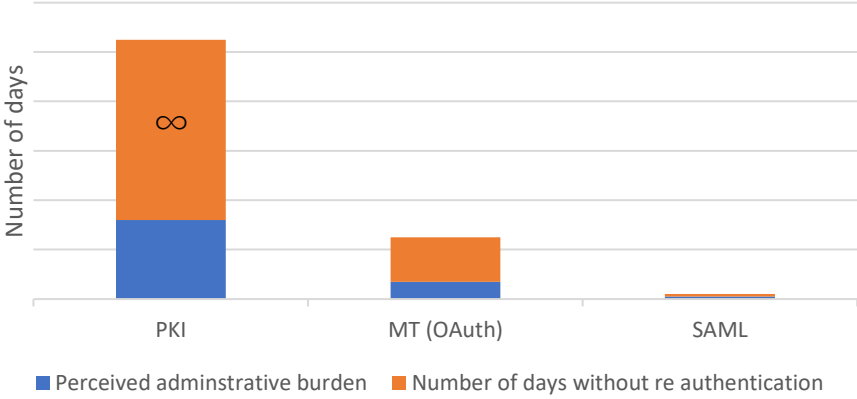


Figure 2