Office 365 – How NOT to do it

UKNOF43

Andrew Ingram

- Owner of High Tide Consulting
- Corporate mergers, acquisitions and divestments expertise
  - Infrastructure
  - Applications
  - User migrations etc
- Design and Build Data Centres, Citrix, AD
- Always looking for the next challenge!

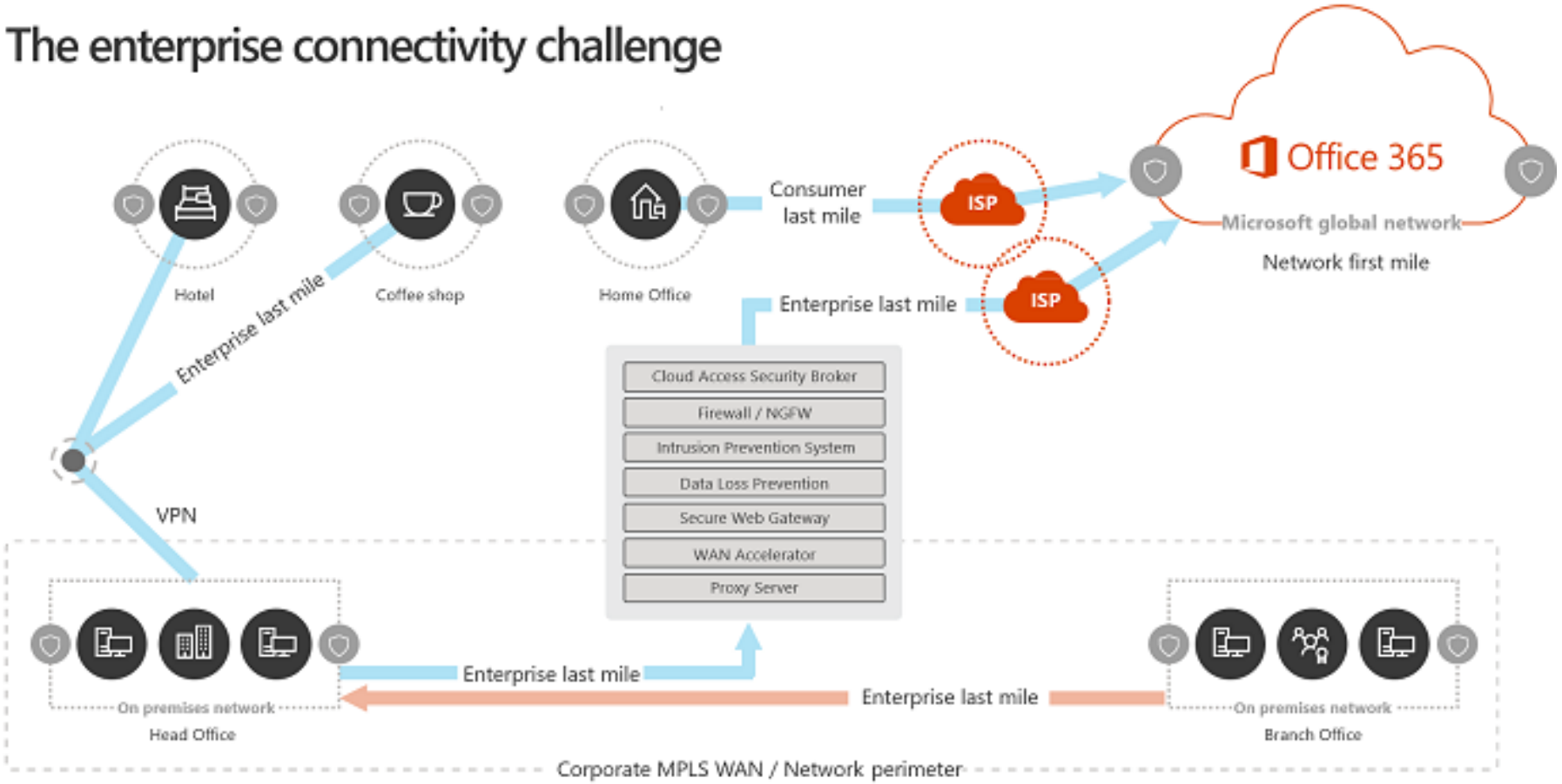
Before the cloud

- Proxy servers where king
- Routing all internet traffic over WAN or VPN back to the DC
- All external DNS requests send back to the DC
- Firewall at the DC handling NAT for the whole company out of a single IPv4 address

Then came the cloud

- More traffic to the Internet, links not big enough
- WAN links are expensive
- Global DNS load Balancing broke with Central DNS
- DC Firewall started to struggle
- Proxy servers struggle
- QOS implemented as a temporary solution

The enterprise connectivity challenge

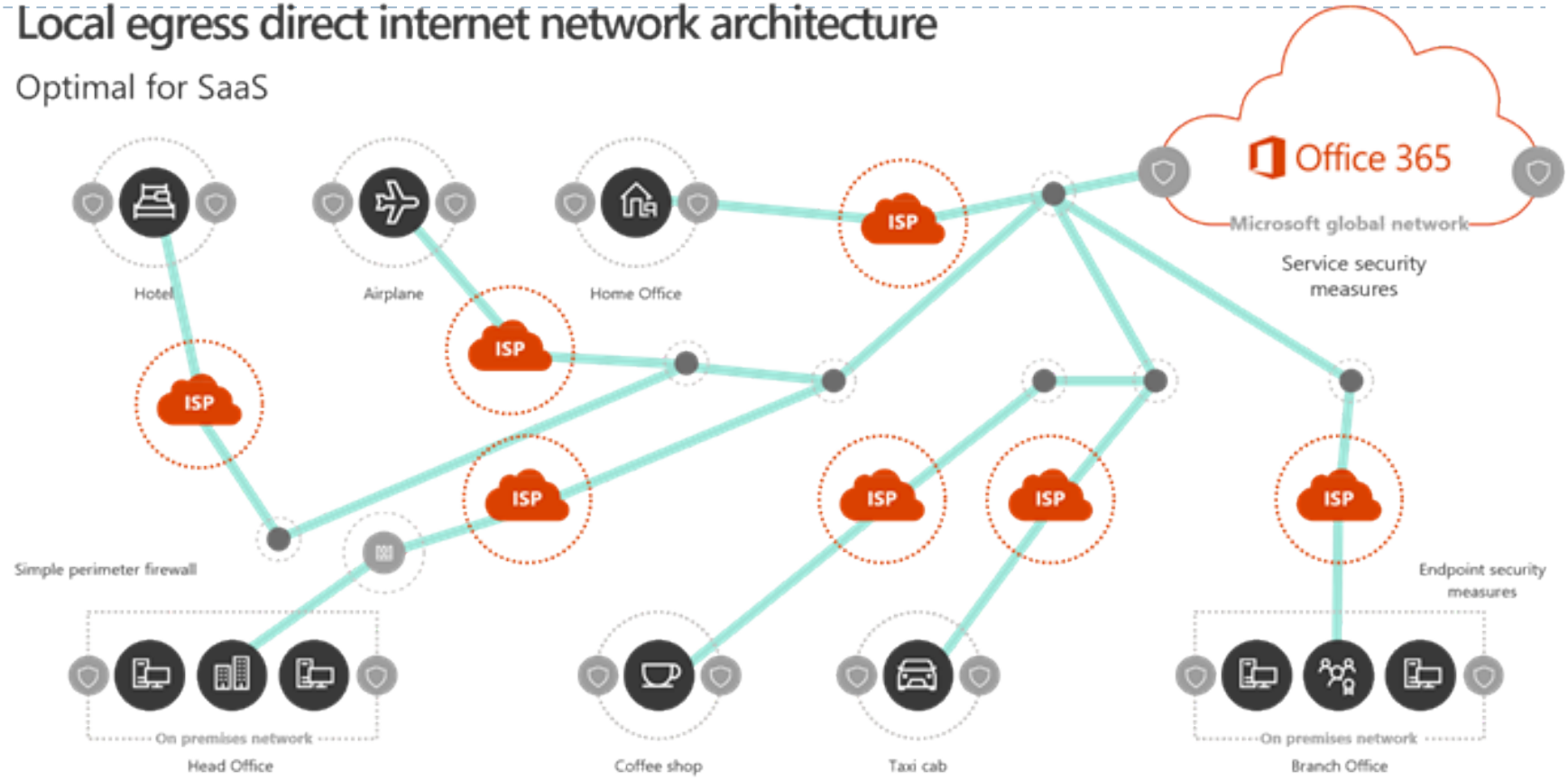


Then came O365

- O365 is not Proxy server friendly
- O365 merges applications and web browser apps together
- Global DNS Load balancing heavily used
- CDN networks heavily used with a large list of URL's
- O365 use TCP Windows Scales
- TCP Idle times default of 100 to 300 seconds (Previously recommended best practice)
- Updates of CRL (Certificate Revocation List)

Local egress direct internet network architecture

Optimal for SaaS



What to Plan for

- Local internet breakout
- Local DNS Breakout
- Enterprise grade internet links (Not a domestic ADSL line)
- Internet Routing, need for a default gateway
- High number of NAT connections
- Network devices work on IP ACL, O365 is primarily URL based

Challenges

- Security, sending all traffic via a proxy made people feel safe.
- NAT Connections, NAT pools may be needed
- Need to start thinking of security at the Endpoint and not just the Perimeter

NAT – How bad can it get

- Maximum supported devices behind a single public IP address = (64,000 - restricted ports)/(Peak port consumption + peak factor)

- **Restricted ports:** 4,000 for the operating system
- **Peak port consumption:** 6 per device
- **Peak factor:** 4

- Total of 6,000 devices accessing O365 on a single address

How should you NOT do Office 365

- Many companies don't do the correct assessment and expect it to just work!
- Some parts of Office 365 need to talk at Windows System Layer (Causes issues with Proxy and Firewall Authentication)
- Windows Network Awareness can cause issues
- If deploying Microsoft Team with Voice and Video ensure WAAS or SD-WAN ensure associated services are configured correctly

Creative Work Arounds

- Bypass Proxy for Office 365 Traffic (PAC Files)
- Cisco Umbrella Branch to direct DNS requests out of local link without a global update to DNS (Inspection rule on local WAN router)
- Inject a Default route into the local site out of the DIA link
- Permit 443 and 80 out of the Local link (Security not happy □)
- Creating Stub zone in local DNS to refer Microsoft URL to google DNS servers. This forces the local client to query google DNS servers direct. (Not nice)