

Digital Tools by

BRINEL



BACKGROUND

- *INTEGRATOR with complex communication solutions to customers of all sizes and different IT maturity. Technicians (or partners) remotely connect to the customer's network to provide remote support. The customer often dictates what connection method is to be used; Client VPN, Site-to-site VPN, TeamViewer (or similar).*
- *The purpose of this service is to provide a flexible and effective means of remotely supporting and monitoring "INTEGRATOR" product solutions in external customer environments. Replace used remote access solutions with a cloud-based service.*



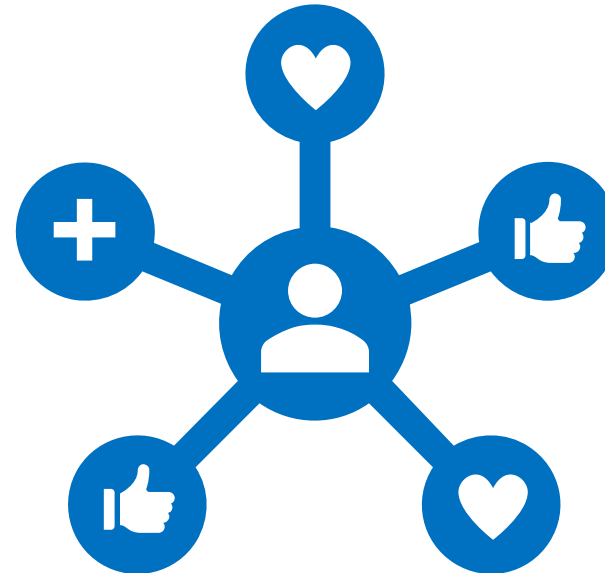
GOALS AND OBJECTIVES

- *Azure Remote Access Management (ARAM) to be used to support customers remotely in a secure and reliable way. The solution presented intend to:*
- *Reduce overhead expenses*
- *Thought leadership through innovation*
- *Help clients focus on their core business.*
- *Reduce time dedicated to infrastructure management*
- *Free up investment capacity*
- *Shift from Capex to Opex*



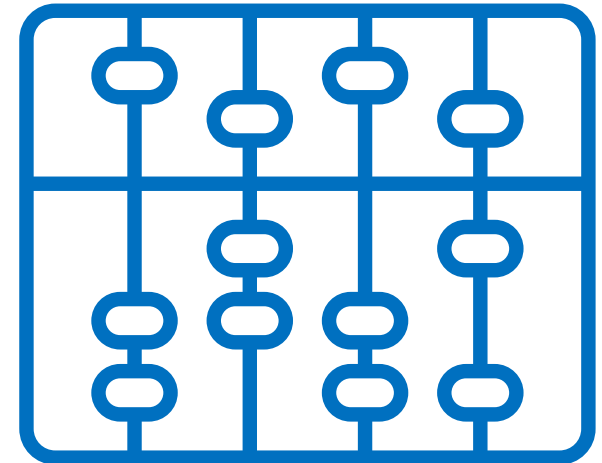
CHALLENGES & APPROACH

- *Connecting to multiple customers exposes both Provider and customers to IT threats. Provider must protect the customer's data / networks from intrusion and malware infections as well as protecting its own data / networks. Provider is not staffed to maintain and run a service to provide thousands of customer connections with an uptime of 99.9% monthly.*
- *Complete managed service for secure and reliable remote access to Provider technicians and provider partners*
- *Azure based solution – with no hardware and software in Provider datacenter.*
- *Provider consumes the solution through secure access to his own customers.*

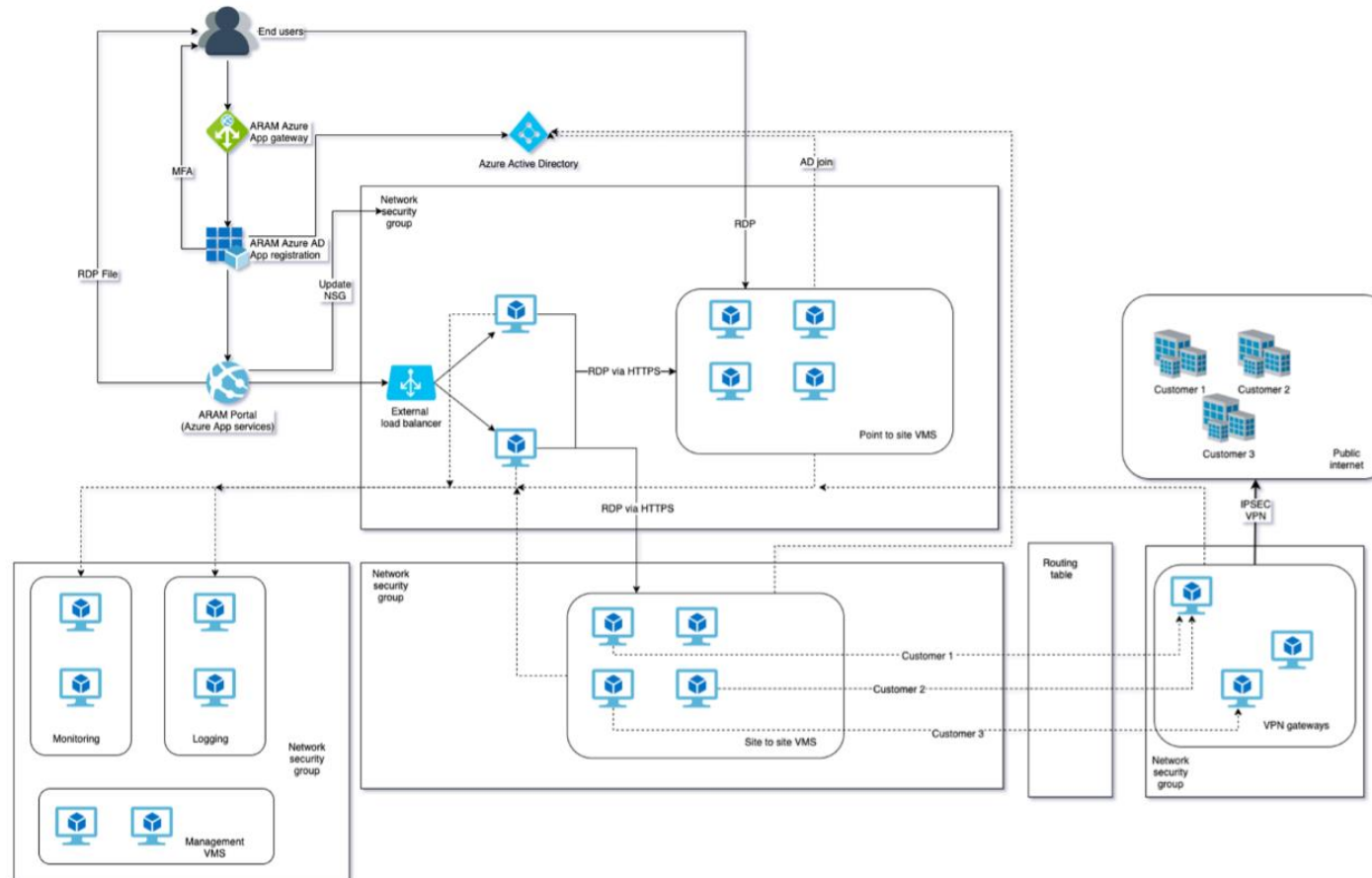


HIGH LEVEL SOLUTION FUNCTIONS

- Site to Site VPN :
 - Allow connectivity to all major IPSEC VPN providers, e.g. Cisco, Checkpoint, Juniper, etc.
 - Traffic isolated per customer still allowing overlapping customer target networks
- Client VPN :
 - Allowing connectivity to all major client VPN providers, e.g. Citrix, Cisco, Checkpoint, Juniper, etc. using HTTPS and IPSEC including support where required for 2 factor authentication
 - Traffic isolated per customer
- Remote Desktop type of support Requirements
 - Support for TeamViewer, GoToAssist, WebEx
- Access/User Access
 - Ability to use 2 factor authentication when outside of the WAN
 - Access list dependent on AD group membership
 - Multiple connections possible from the solution allowing multiple technicians to make out bound connections whilst keeping the traffic isolated from the different customer VPN's
 - GDPR compliant









HIGH LEVEL SOLUTION ARCHITECTURE











Status: Status **Running** ▼ Name: Client: Client

Site 2 Site VM's (0)

| | | |
|---|---|---|
| <p>Site_S2S</p> <p>VM Status ●</p> <p>Actions</p> <p> </p> <p>Active users: 1</p> | <p>Site_S2S</p> <p>VM Status ●</p> <p>Actions</p> <p> </p> <p>Active users: 1</p> | <p>Site_S2S</p> <p>VM Status ●</p> <p>Actions</p> <p> </p> <p>Active users: 0</p> |
|---|---|---|

Point 2 Site VM's (7)

| | | | |
|--|--|--|--|
| <p>Point_P2S_1</p> <p>VM Status ●</p> <p>Actions</p> <p> </p> <p>Active users: 0</p> | <p>Point_P2S_1</p> <p>VM Status ●</p> <p>Actions</p> <p> </p> <p>Active users: 0</p> | <p>Point_P2S_1</p> <p>VM Status ●</p> <p>Actions</p> <p> </p> <p>Active users: 1</p> | <p>Point_P2S_1</p> <p>VM Status ●</p> <p>Actions</p> <p> </p> <p>Active users: 0</p> |
|--|--|--|--|