Insurance

ISSQUARED

REMOTE FILE ACCESS

Case study

ABOUT THE CLIENT

A leading government insurance pool service provider company.

OBJECTIVES

The client wanted to phase out the on-prem file service infrastructure and sought a cost-efficient solution that would enable its users to access file shares remotely from any location.

The client required Active Directory as the primary authentication and authorization source for all users.

The client sought a solution that would ensure secured authentication and prevent exposure of data hosted on file share to untrusted devices.

The client was also looking for remote connectivity to the on-premise VOIP system, VPN only access to file shares, auto-connect VPN and shares, and internet access for VPN users.

SOLUTION OVERVIEW

Based on the above objectives the ISSQUARED® team decided on a solution with the following features.

a) Cloud-based file share.

b) Network ACLs to restrict share access.

c) Data at rest and in-flight encryption.

d) Cloud-based secure VPN.

e) Portable and secured end-user devices.

f) Out-of-box integrability with Active Directory for access to shares.

g) Certificate-based authentication for VPN.

h) Domain controller VMs in the cloud environment.

ISSQUARED

APPROACH & METHODOLOGY

Based on the above directives, the following approach was taken by the ISSQUARED® team for privileged and regular user accounts.

- The team implemented and configured Azure file share.
- For remote VPN access, Azure VPN with certificate-based authentication was implemented.
- Domain-linked surface pro devices were provisioned for users.
- In the Azure VNET, a gateway subnet was set up for point-to-site VPN.
- Certificate-based authentication was configured for end-user devices that connect to Azure VNET.
- To cater to split tunneling for internet access and connecting back to on-prem, custom routes were decided to be pushed to clients. Scripts were scheduled to run every time a VPN connection was initiated on a user's device.
- All external access to file shares was blocked and was allowed only via Azure VNETs.
- Azure file share resources were linked to the Active Directory domain to allow Kerberos authenticated access.
- All files from the on-prem file server were migrated to Azure file share using the Azcopy utility.
- Permissions were restored as per the on-prem filer permissions.
- The windows scheduled task was configured on end-user devices to ensure custom routing to trigger when a VPN connection was initiated.
- The scheduled task was configured on end-user devices to ensure file share mappings have connectivity when a VPN connection was established.
- With the vpn gateway solution for both point-to-site and site-to-site connections, connectivity to on-premise VOIP system was also ensured.

RESULTS

- On-prem filer dependency was reduced to 0%, thus paving the way for offboarding the on-prem file service infrastructure.
- 100% of users were remote enabled for file share access from their managed devices.
- 0% access was allowed to to unmanaged devices and devices not connected to the internal Azure network.
- 0% end-user intervention was required for service enablement.
- 100% of users were connected to an on-prem VOIP system.
- 100% secure access to access file shares was allowed with Kerberos authentication only.