MEX Data Hosting Diagram

SiteName.mex.com.au

All Traffic

All Traffic

MS Azure Security

MEX Utilises Microsoft Azure Services

Some of the Azure Security components are:

- DDoS Protection
- Advanced Threat Protection
- Helps prevent Brute Force and other network attacks

It also offers suggestions on additional security measures etc… to ensure all components are secure.

MS Azure Network Security Group

Ports - 80/443/ 11433/1433/ 3389

The Network Security Group is utilised as a cloud based firewall where security rules and ports are configured. We have the 5 main ports open that we utilise for the Hosting Service, leaving all other ports blocked.

The 5 ports we utilise are split into 3 sections; Web, SQL, RDP.

- 80(HTTP), 443(HTTPS)
- 11433(Custom SQL), 1433(Standard SQL)
- 3389(RDP)

In addition to this, each VM has the standard Windows Firewall turned on and required ports are configured.

Each Hosting Group is only configured with 50 customers, this is to not only increase performance but to minimise the unexpected downtime impact and increase security measures. Backups are performed on all VM's that are being utilised. These backups occur daily and are kept for 30days.

Document Storage

Virtual Machine Firewall

Virtual Machine Firewall

Region - Australia East

Region - Australia South-East

Real-time Replication

MEX Hosting X

MEX Hosting X - Rep

Each Virtual Machine (VM) runs the Web Server and SQL Server components required for the MEX Application to operate.

The Document Storage utilises Microsoft Azure Storage, which is separated from the Virtual Machines. This ensures that all documents are accessible from both machines (if required). Utilising the replicated VM is only required if an unexpected outage is to occur.

All traffic is forwarded to this VM during this period. The connection between the two VM's is secured through the Azure Network.