Official documentation on ports: <https://msdn.microsoft.com/en-us/library/cc646023.aspx#BKMK_ssde>

The following should be followed:

Port 1433 TCP – Block (do not allow) – Default Instance port (i.e. not a “Named Instance”, Precise only use named instances)

Port 1434 TCP – Block (do not allow) – Dedicated Admin Account (should be available internally only)

Port 1434 UDP – Allow – This is the SQL Server Browser Port, it is required for Named Instances & therefore must be allowed

SQL Server Browser

Listens for Named Instance connection requests on UDP 1434. It will scan the registry for the Named Instance’s TCP Port & return it to the requester.

**NB: The firewall has a service definition for this called “MS-SQL\_Browser\_Port”, do not create any others for 1434 UDP**

SQL Ports for Named Instances

By default Named Instances use dynamic ports & the SQL Server Browser will be used to determine the port of the Named Instance. We change these to fixed Ports using SQL Server Configuration Manager, this is so that we can allow traffic only on that TCP port. Using dynamic ports would mean we would have to open a wide range of ports.

Firewall Rules for SQL Server

1. As we exclusively use named Instances, each instance will need its own “Service Definition” for the TCP Port (do not use TCP/UDP).
2. The naming convention must start MS-SQL\_Port\_
3. Both this service definition & MS-SQL\_Browser\_Port must be included in the services section of the firewall rule