# Partitioning a Directory Server

Partitioning enhances your ability to use one Directory Server for your whole enterprise, rather than separate Directory Servers for different departments within your enterprise. The partitions each need to be managed separately, but only one Directory Server needs to be installed.

Here are some of the advantages of partitioning:

- You can use partitioning to direct specific clients to specific databases.

- If you have created Adabas databases with identical database IDs, you can use partitioning to correctly identify which client calls get directed to which Adabas database.

- You can use partitioning to group client calls to an Adabas database, thus reducing the number of actual connections required for that database. This can be especially useful if you are using Entire Net-Work on the mainframe to access a specific Adabas database. Simply remove the access URL entries for the databases from the appropriate partition.

- If your Software AG product supports the use of SSL, you can use impose real security requirements on calls made by clients in specific partitions.

Partitions can be defined for a Directory Server in the System Management Hub. For complete information on maintaining partitions and the targets in them, read *Maintaining Partitions* and *Maintaining Targets*.

Suppose you configure your network as depicted in the following diagram:
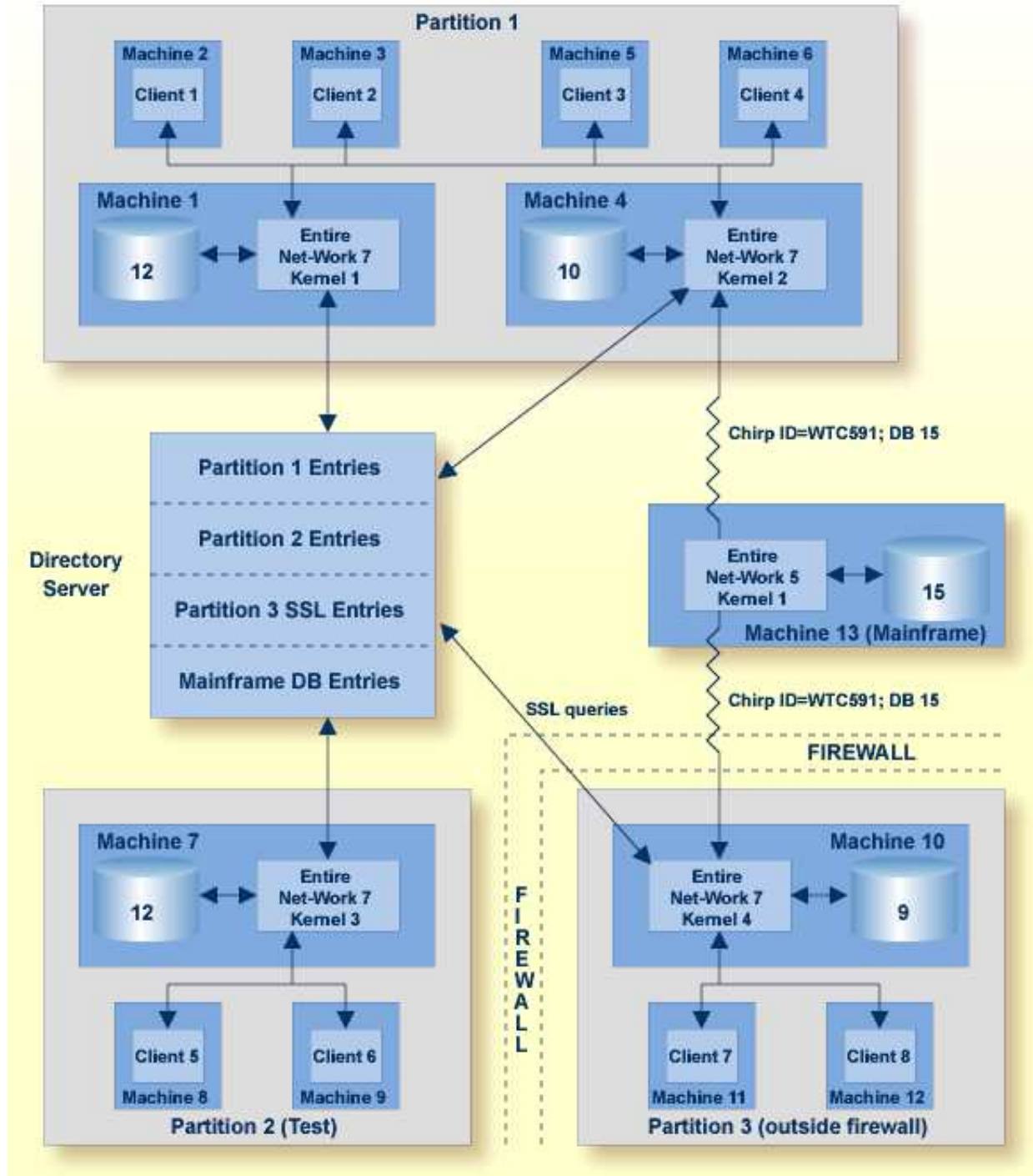
In this diagram, partitioning is used to:

- Restrict calls for Database 12 (on Machine 1) and Database 10 (on Machine 4) to clients 1 through 4 in the Partition 1 partition.

- Restrict calls for Database 12 on Machine 7 to clients in the Partition 2 (Test) partition.

- Establish a test environment. The Partition 2 (Test) partition has been set up as a testing partition. Only clients 5 and 6 are included in it and use Database 12 on Machine 7.

- Group calls to Database 15 on the mainframe. The calls to this database are grouped by the Kernel 2 in Partition 1 and Kernel 4 in Partition 3, thus reducing the number of connections necessary for the database.

- Impose security, via SSL, on the clients who are outside the firewall. Clients in Partition 3 are outside the company firewall. Security restrictions are also enforced when accessing Database 9, which is also outside the security firewall.

Partitions are assigned after installation using Software AG's System Management Hub (SMH).