Considerations when setting up the Firewall:

1. Define clear security policy.
2. Determine the network topology.
3. Configure the inbound and outbound rules.
4. Implement application-level filtering. Restrict application access such as email, web browsers etc.
5. Regularly update the firewall rules.
6. Monitor the firewall logs.
7. Implement the additional security measurement such as IDS.
8. Firewall must have the capacity to handle all potential peaks.
9. When the traffic is too high the firewalls must drop the unprocessed packets.
10. Logs and alarms must be configured accordingly.
11. Implement multi-layer firewalls if possible.
12. Firewalls with packet inspection are better than the packet filter implementation.
13. Stateful firewalls are better than stateless.
14. Most of all, have extra attention to implement firewalls rules such as the order.