Firewalls

Suppose you have a corporate network and you are designing the firewall layout. You have the following servers that you intend to deploy: an internal Wiki-like database running over HTTP/HTTPS, a public webserver, a server used to store git repos accessed over ssh, along with some number of client workstations. Assume you will use a screened subset firewall with separate exterior and interior routers.

1. Which servers will be present on the perimeter network?
2. Which servers will be present on the internal network?
3. Draw a layout of the network indicating the different services and routers.
4. Write firewall rules for the two routers. You may use shorthands for hostnames of the machines instead of arbitrarily giving them IP addresses, such as `IN-A` and `IN-B` to refer to two internal network machines A and B, and wildcards like `IN-*` to refer to all internal network machines.
5. Suppose you wanted to install a honeypot to serve as a fake `ssh` and `HTTP/HTTPS` servers. Where would you put it and what rules need to change in the firewall to support it?
6. Suppose you wanted to monitor employee's use of the Wiki-like database and the public webserver, e.g., to track which clients use it, when, and how much, but suppose that you cannot change the servers themselves to start recording this data themselves, but you have a router that supports rules to `LOG` traffic metadata (akin to `ALLOW` and `DENY`). How would you change your architecture to support this?