

Eliminate Both:
1. Storage of Sensitive Data in the DMZ
2. Direct Links between DMZ and Your Network

DMZ Network

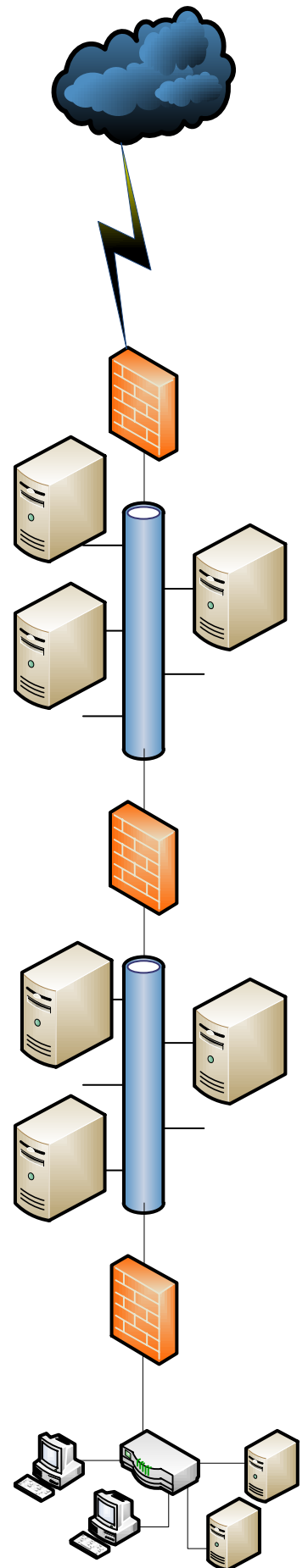
1. All devices accessible from the Internet reside in this zone
2. No private or sensitive data is stored in this zone
3. DNS servers that forward requests to Internet DNS servers
4. Microsoft Edge Transport Server to handle mail flow; configured to use LDS Lightweight Directory Services instead of full AD.
5. Examples: FTP, Web, SMTP, and VoIP servers
6. Xen Access Gateway or Microsoft RDS Gateway Server with no AD data

Intermediary Zone Network

1. Eliminates the direct link from your internal network to the DMZ
2. Application proxy able to decrypt, examine, and re-encrypt packets
3. Intermediary database servers query data from internal database servers to send to the web servers in your DMZ
4. DNS servers forward requests to DNS servers in the DMZ
5. Zone may contain limited data if required

Internal Network

1. Exchange Server, AD Servers, SQL Servers, etc.
2. Clients
3. DNS servers forward requests to DNS in the Intermediary Zone
4. Internal network preferably segmented into additional internal filtered subnets to control, filter, and segment your internal traffic



Note relating to the “firewalls” in the diagram above: You may choose to use screened subnets on a single firewall. Using individual filtering devices is more secure.