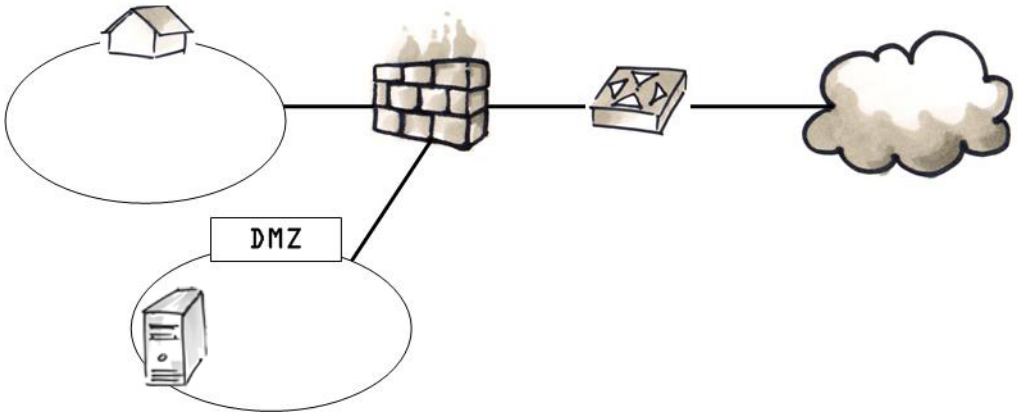
Kontrollfragen

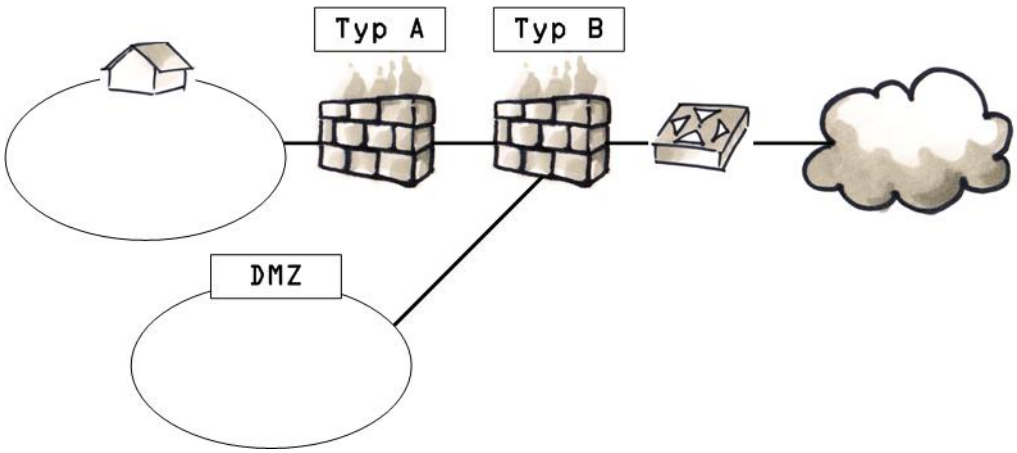
Firewall Architekturen

1. Architektur



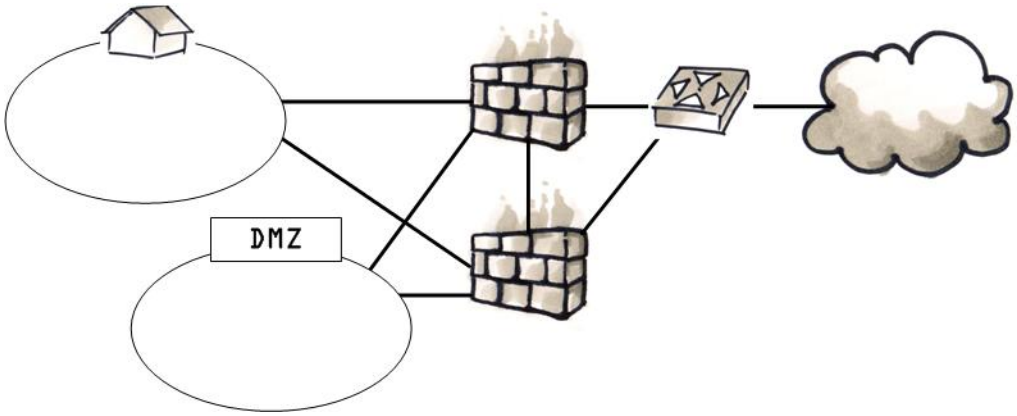
- □ Klassisches Modell für die Businessintegration eines Lieferanten (Stichwort B2B)
- □ Klassisches Modell für die Betreibung eines FTP- oder Web-Servers
- □ Klassisches Modell für die Betreibung eines ERP-Datenbankserver

2. Architektur



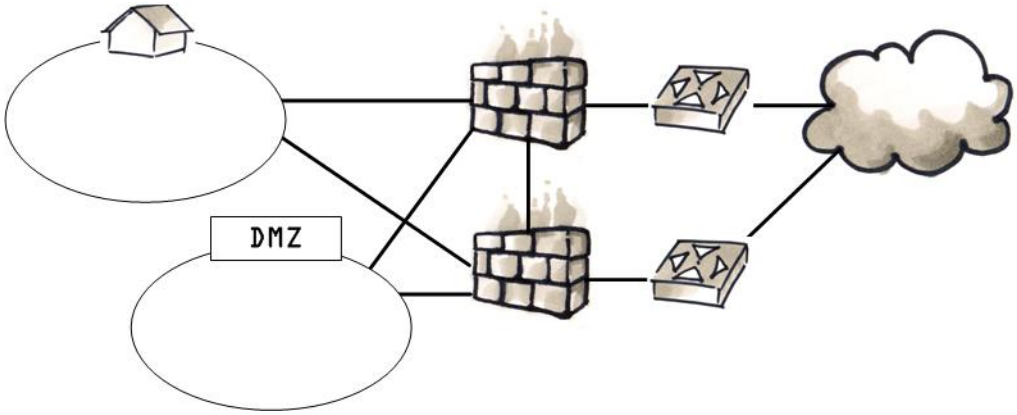
- □ Klassisches Modell für eine redundante Betreibung des Internetzugangs
- □ Klassisches Modell für die Betreibung einer Firewallinfrastruktur mit hoher Sicherheit
- □ Klassisches Modell für die Betreibung eines Firewall-Clusters

3. Architektur



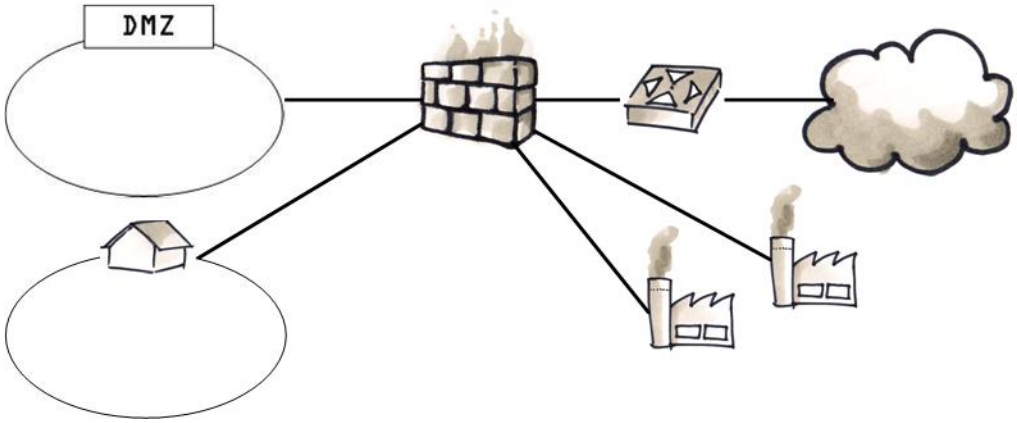
- □ Klassisches Modell für die Betreibung eines Firewall-Clusters
- □ Klassisches Modell für die Betreibung einer *high-availability* Firewall-Lösung
- □ Klassisches Modell für eine redundante Betreibung des Internetzugangs

4. Architektur



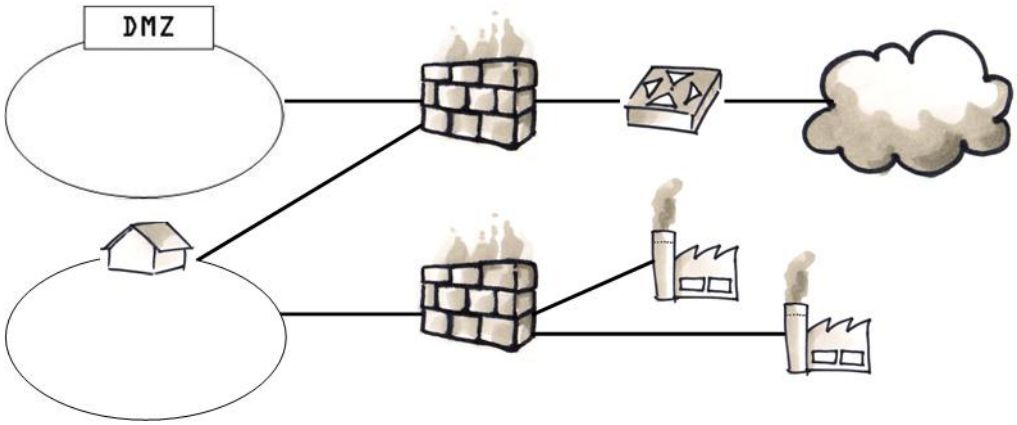
- □ Klassisches Modell für die Betreibung einer Firewallinfrastruktur mit hoher Sicherheit
- □ Dieses Konstrukt macht nur Sinn, wenn Sie zwei unterschiedliche ISPs verwenden
- □ Klassisches Modell für ein kleines Unternehmen z.B. im Sanitärbereich (< 10 Mitarbeiter)

5. Architektur



- □ Diese Architektur eignet sich zum Beispiel für Handelsfirmen mit einer B2B-Integration
- □ Diese Architektur ist unsicher, da ein Partner auf alle Server Zugriff hat
- □ Beim Ausfall der Firewall ist kein B2B-Zweig betroffen

6. Architektur



- □ Klassisches Modell für die Betreibung einer *high-availability* Firewall-Lösung
- □ Diese Architektur eignet sich zum Beispiel für Handelsfirmen mit einer B2B-Integration
- □ Die dedizierte Firewall ist am falschen Netz (DMZ statt LAN) angeschlossen, da die ERP-Server typischerweise in der DMZ stehen