FIREWALL ARCHITEKTUR FÜR KLEINERE HOCHSCHULEN

BWCAMPUSNETZ, UNIVERSITÄTS-IT MANNHEIM, 2025

AGENDA

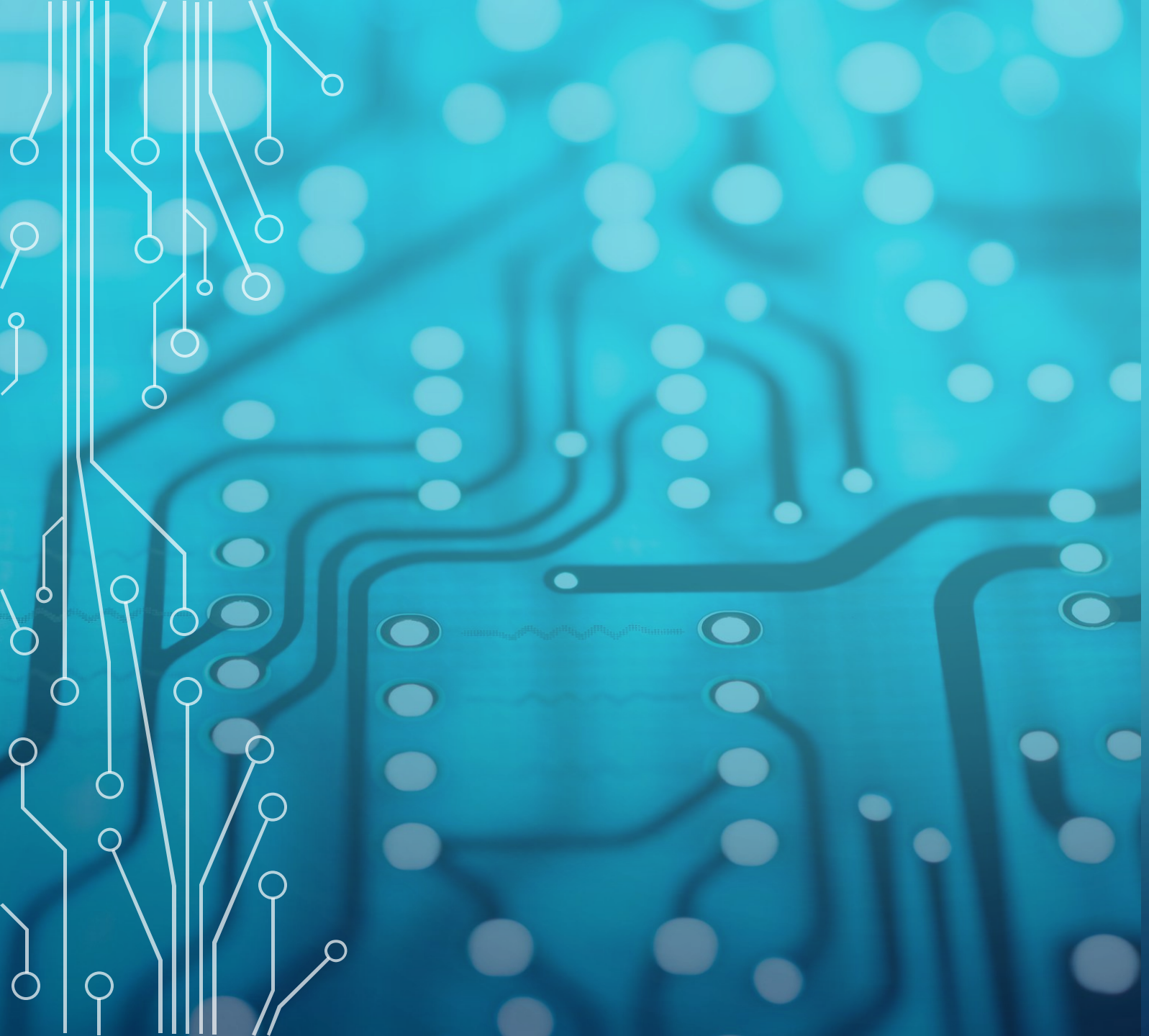
- **Situation**
- Lösung der Universitäts-IT Mannheim
- Blueprint
- Fragen und Diskussionen

SITUATION, ZIELE UND NICHT-ZIELE

- Situation
  - Nicht mehr zeitgemäße Lösung mit ACLs auf Routern (stateless Firewall)
- Ziele
  - Sicherheit erhöhen durch eine zeitgemäße Lösung
  - Einfache, kosteneffiziente Firewall-Lösung (stateful mindestens)
  - BSI IT-Grundschutz erfüllen
- Nicht-Ziele
  - Security-Proxys, P-A-P Struktur
  - Aufbrechen von Security Traffic
  - Open Source (Personalsituation)

ANFORDERUNGEN GEMÄß BSI IT-GRUNDSCHUTZ

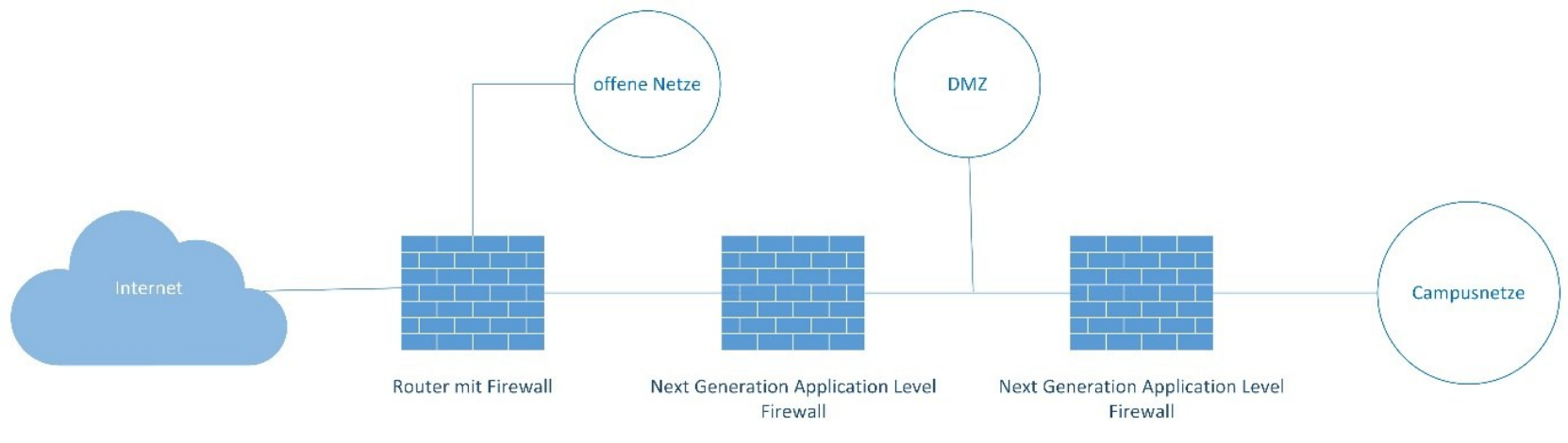
- Weitgehend sinnvolle Anforderungen auch für ein Campusnetz
- Umsetzung:
  - Schutzbedarfsermittlung nach BSI-Standard
  - DMZ für externe Services, Intranet für interne Bereiche
  - VPN-Zugang separat mit eigener Firewall
  - Segmentierung nach Schutzbedarf
  - Whitelisting: alles verboten, gezielt freigeben



AGENDA

- Situation
- **Lösung der Universitäts-IT Mannheim**
- Blueprint
- Fragen und Diskussionen

FIREWALL ARCHITEKTUR UNIT

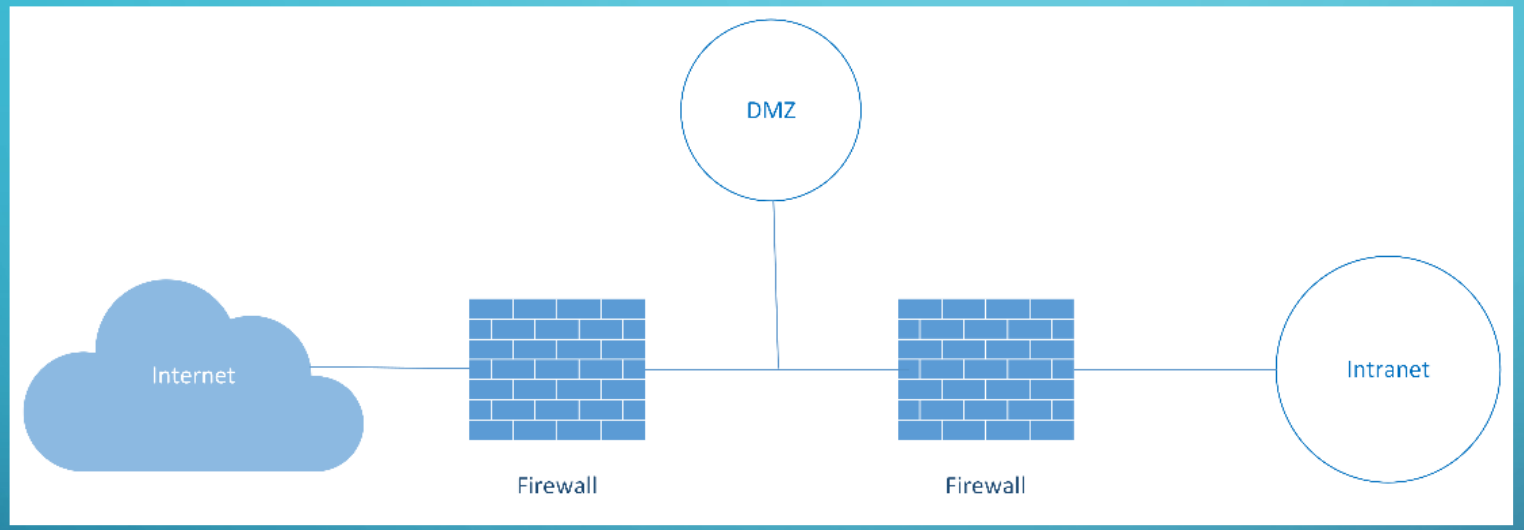


- Besonderheiten:
  - Zusätzliche vorgelagerte Firewall im Border-Router
  - Next Generation Firewalls mit Layer-7-Analyse und IDS/IPS erhöhen die Sicherheit
  - Konfiguration erfolgt stufenweise, Traffic Analyse unterstützend

AGENDA

- Situation
- Lösung der Universitäts-IT Mannheim
- **Blueprint**
- Fragen und Diskussionen

FIREWALL-ARCHITEKTUR



- Typische Architektur mit DMZ
- KISS – je einfacher desto besser
- Besondere Bedarfe (VPN, public Netze,…) dazu

INSTALLATION UND KONFIGURATION

- Ziel ist Whitelisting: Alles verboten, gezielt freigeben
- Traffic-Analyse zur Regeldefinition
- Stufenweise Inbetriebnahme zur Fehlersuche
- Kommunikation/Zusammenarbeit mit Admins und Service Desk wichtig
- Spezialisten zur Unterstützung empfehlenswert

PROZESSE – BENÖTIGT MAN

- Regelmäßige Updates und Regelüberprüfung
- Audits und Logfile-Auswertung
- Dokumentation und Schulung der Mitarbeiter

AGENDA

- Situation
- Lösung der Universitäts-IT Mannheim
- Blueprint
- **Fragen und Diskussionen**

FRAGEN UND DISKUSSION