Leibniz Universität
IT Services

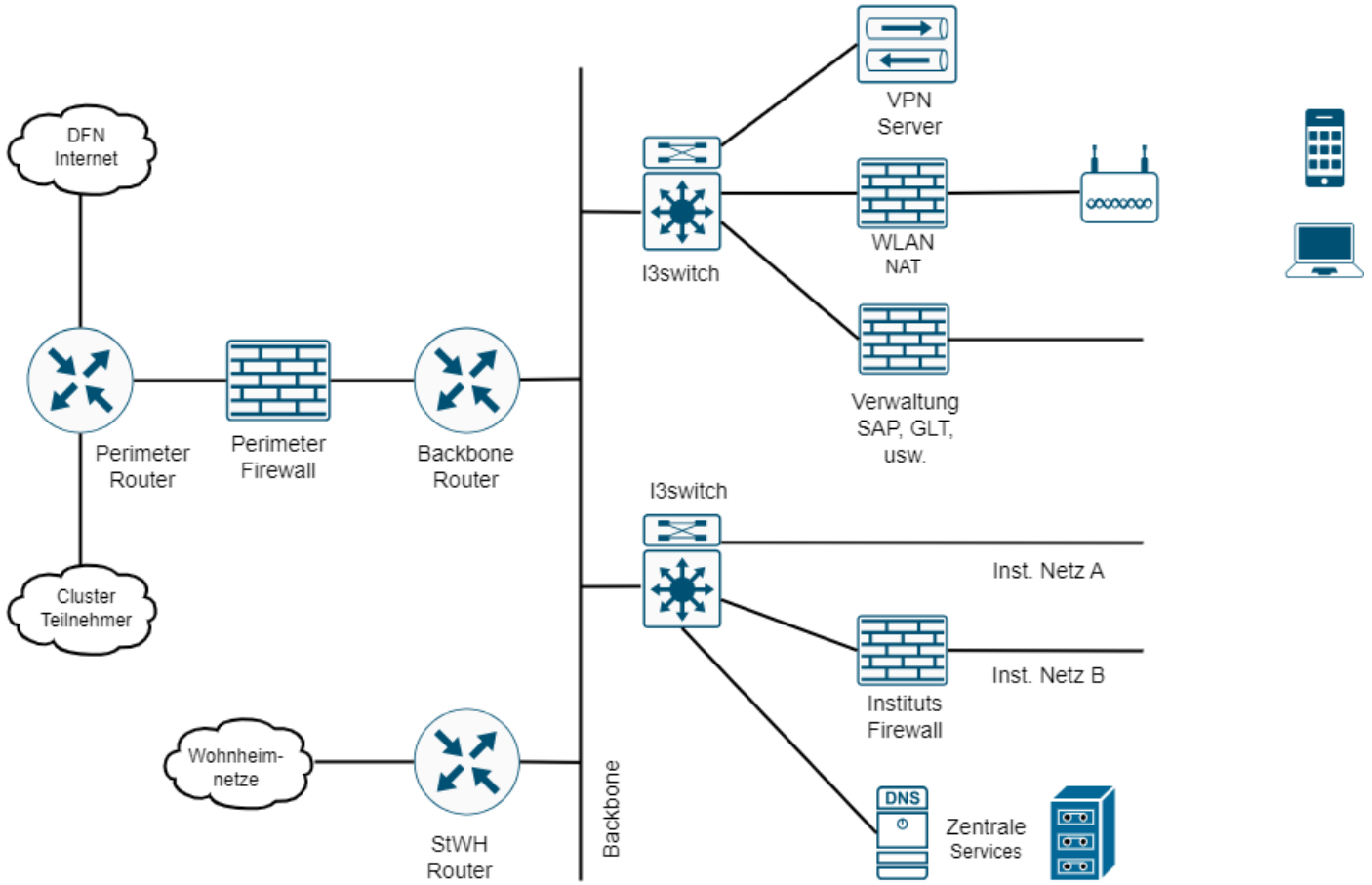
Leibniz
Universität
Hannover

Netzschutz-Firewall

Agenda

- Netzaufbau
- Firewall-Struktur
- Geräte im Institutsnetz
- Einführung Netzschutz
- Zuständigkeiten
- Auszug Konfiguration
- Einsicht/Änderungen beantragen
- Netzwerkeinstellungen
- Netzschutz und Instituts-VPN
- Einordnung und Zusammenfassung

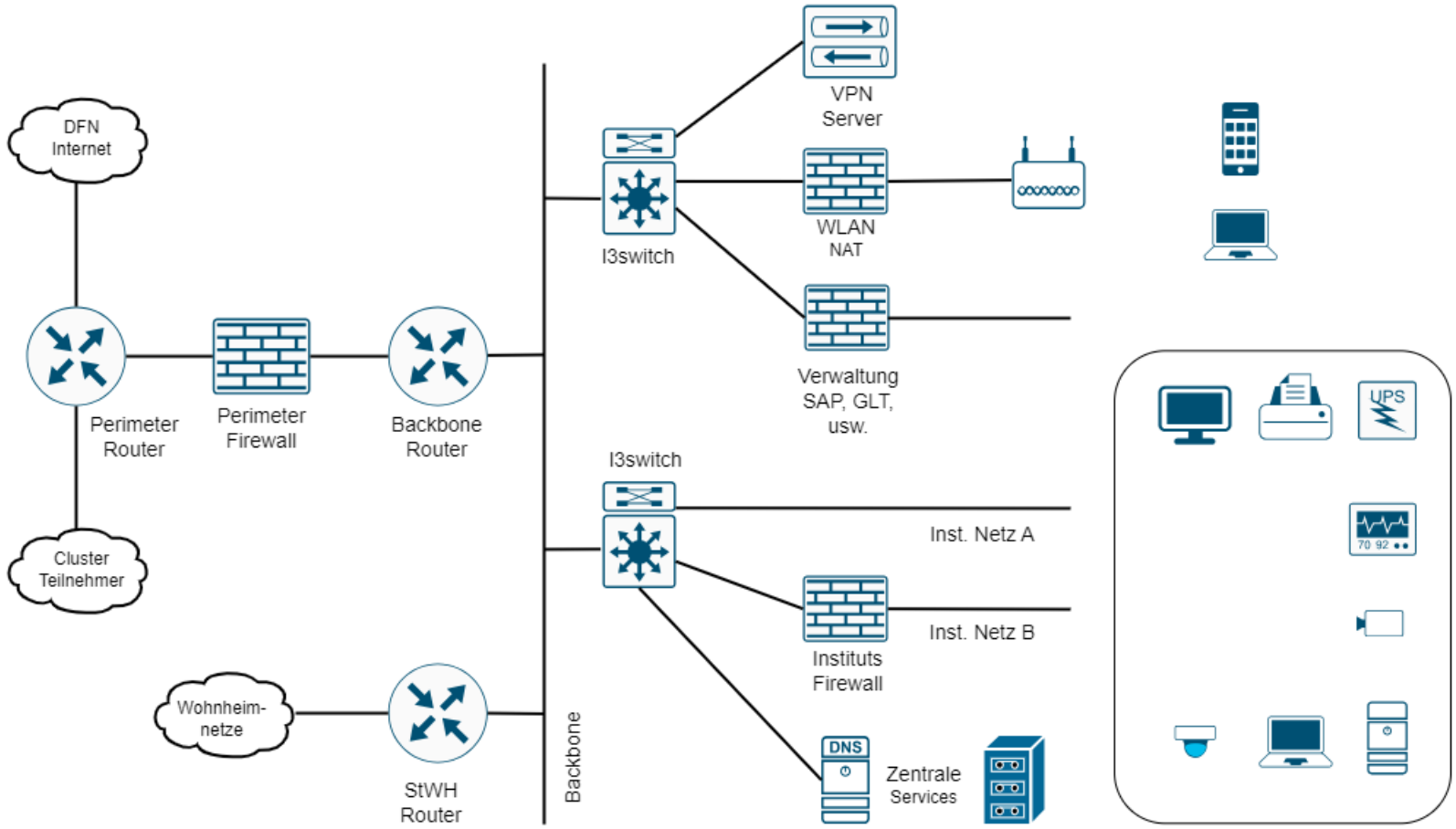
Vereinfachter Netzaufbau I



Firewall-Struktur

- GWFW
  - Perimeterfirewall
  - Zuordnung IP zu einer Kategorie
  - Client, Server, Device Kategorien
- Netzschutz
  - Institutsfirewall
  - Default alles raus / nichts rein
  - Lokaler Verkehr, innerhalb eines Subnetzes wird nicht reglementiert
  - Subnetzübergreifender Verkehr unterliegt Regelwerk

Vereinfachter Netzaufbau II



Geräte im Institutsnetz I

- Aktuelle, gut betreute Rechner -> eher kein Problem
  - Aber nicht zu sicher fühlen

- Problematischer:
  - Drucker, NAS, USV usw.
  - Multimedia Geräte, Überwachungskameras usw.
  - Messgeräte, usw.

  Oft nicht im Fokus, keine Updates, oft lange Laufzeit, kein Patchmanagement

Geräte im Institutsnetz II

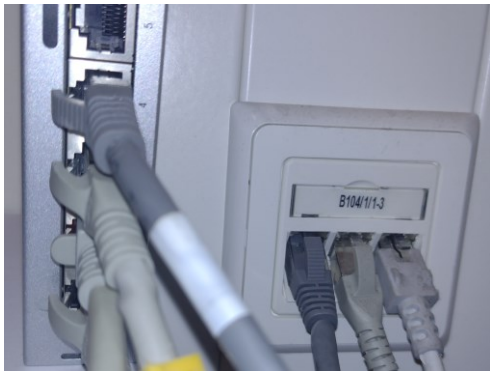
- NMAP ins Institutsnetzwerk ohne Netzschutz

```
user@host:~$ nmap -n 192.168.97.9 | fgrep open
1947/tcp open  sentinelsrm
3389/tcp open  ms-wbt-server
5054/tcp open  rlm-admin

user@host:~$ nmap -n 192.168.97.19 | fgrep open
4000/tcp open     remoteanything
```

Geräte im Institutsnetz III

- Unbekannte Server im Netzwerk
  - Miniswitch
    - Webserver, SSH
    - Beispiel Ubiquiti
    - Default Account, auch über Netzwerkgrenzen zugreifbar



  - Remotemanagementcard
    - Zwei MACs am Port
    - Per DHCP IP zugewiesen
    - Default Account

Einführung Netzschutz I

- Vorher 1 bis 2 Beratungsgespräche
  - Überblick verschaffen
  - Ablauf absprechen
  - Termin vereinbaren
  - eventuell Netz und IPAM mitinvolviert
- Regelwerk melden (Default-Regelwerk vom LUIS)
- Umstellung (z.B. 10 bis 12 Uhr, oft nur kurze Unterbrechung)
- Testphase
- Änderungen in den ersten Wochen -> direkt anrufen

Einführung Netzschutz II

- Regelwerk (Beispiele)
  - Teilnahme am Bacula Backup?
  - Remotezugriff?
    - RDP, SSH?
    - Weltweit oder VPN?
  - Zugriff vom WLAN, Nachbarinstitut?
  - Lizenzserver?
  - Bei Adressenänderung -> eventuell SAP-PCs betroffen
  - LUIS-DNS -> Zugriff auf DC notwendig?
  - Zwei freie IPs für die Firewall im Netz notwendig

Zuständigkeiten I

- LUIS
  - Betreibt Hardware (Austausch, Umbau, Erweiterung)
  - Betreibt Software (Updates)
  - Bei Problemen Kontakt mit Hersteller TAC
  - Richtet virtuelle Firewalls ein
    - I.d.R. transparente Firewalls
  - Pflegt das Regelwerk und berät
  - Troubleshooting

Zuständigkeiten II

- Institut
  - Legt Regelwerk fest
  - Meldet Veränderungen
    - Neue Einträge
    - Alte löschen lassen
  - Unterstützt bei der Fehlerbeseitigung
  - Ist für die Systeme im Netz verantwortlich

Auszug der Firewall-Konfiguration

inside_access_in

#	Mode	Protokoll	Quell Host	Quell Port	Ziel Host	Ziel Port	Options
1.1	**permit**	tcp	any		_LUIS-Endpoint-Protection_HG	_LUIS-Endpoint-Protection_tSG	
	Zugriff auf zentr. Managementserver der Enspointprotection - 2022-08-10-SK						
1.2	**permit**	udp	0.0.0.0	eq bootpc	255.255.255.255	eq bootps	
	DHCP-Discover oder Request zum Relay - Standard Freigabe - RRZN-DHCP-Service - 2015-05-18-HH/SK						
1.3	**permit**	udp	any	eq bootpc	_DHCP-RRZN-HG	eq bootps	
	laengerung oder Freigabe - Standard Freigabe - RRZN-DHCP-Service - 2015-05-18-HH/SK						
			any	eq bootps	_DHCP-RRZN-HG	eq bootps	
1.5	**permit**	udp	any		_TFTP-RRZN-HG	eq tftp	
	TFTP Zugriff auf Appconf - Standard Freigabe - RRZN-PXE-Service - 2015-05-18-HH/SK						
1.6	**permit**	tcp	any		13[redacted]0/25	_WinFS-tSG	
	Standard Freigabe fuer Zugriff auf RRZN-Fileservices - 2015-05-13-HH/SK						
1.7	**permit**	udp	any		13[redacted]0/25	_WinFS-uSG	
	Standard Freigabe fuer Zugriff auf RRZN-Fileservices - 2015-05-13-HH/SK						

- Rescourcen

Vom LUIS gepflegte Gruppen

_LUH-filter-proxy_tSG (tcp)

FW-Uebergreifend: Proxy-Port fuer Proxynutzung

eq 3129

_LUH-secure-proxy_tSG (tcp)

FW-Uebergreifend: Proxy-Port fuer Proxynutzung

eq 3131

_LUH-web-proxy_tSG (tcp)

FW-Uebergreifend: Proxy-Port fuer Proxynutzung

eq 3128

_LUIS-Endpoint-Protection_tSG (tcp)

FW-uebergreifend: TCP-Port(S) fuer zentrale Endpoint Protection Loesung

eq 7074 eq 8443 eq 8444

_LUIS-IT-Sec-PortScan_tSG (tcp)

FW-uebergreifend: tcp-Ports fuer Sicherheitsscans

eq 3389

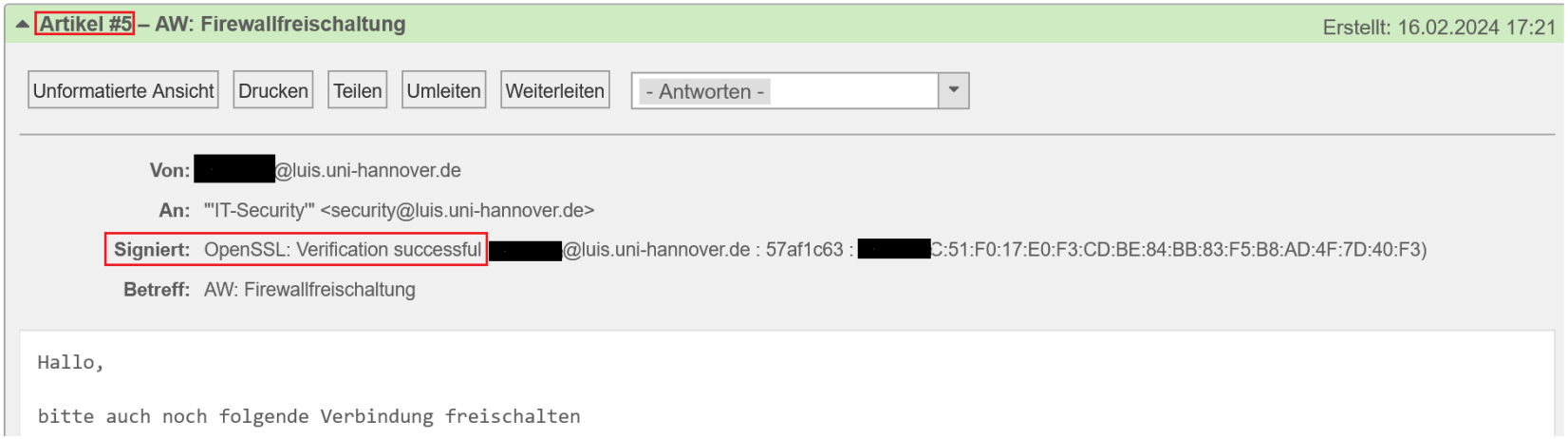
_Mail-abruf-tSG (tcp)

FW-uebergreifend: zum Abholen und Lesen von Mail

eq 993 eq 995 eq imap4 eq pop3

Änderungen beantragen I

- Mit signierter Mail an support@luis.~
- Nur durch IT-Beauftragten
- Keine alten Tickets „aufwärmen“
- Ein Ticket je Wunsch



Änderungen beantragen II

- Quell und Ziel IP (oder Netz, WLAN, VPN, LUH, Internet…)
- Portnummer(n)
- Protokoll (TCP, UDP, ICMP usw.)
- Hintergrund
- Kommentar

Netzwerkeinstellungen

- Mehrere IPv4 Subnetze in einem VLAN
  - Keine Verwendung von nicht gemeldeten Subnetzen
  - Rechner nicht Dual- / Multihomed
- WLAN und LAN nicht gleichzeitig
  - Parallelschaltung zur Firewall
  - Macht oft Probleme
- Verwendung von passender Netzmaske und Gateway

Netzschutz und VPN

- Netzschutz und Instituts-VPN (zwei Geschmacksrichtungen)
  - VPN terminiert im Instituts-Netz
    - IP Adressen aus dem Instituts-Netz werden benötigt
    - Voller Zugriff der VPN-Nutzer auf ALLE int. Ressourcen
  - VPN terminiert im LUH Netz
    - VPN-User bekommt IP aus einem VPN-Netz
    - Netzschutzregeln notwendig
    - Möglichkeit den Zugriff am Netzschutz zu reglementieren
      - Admin bekommt vollen Zugriff
      - Mitarbeiterin z.B. nur RDP auf ihren Rechner

Einordnung

- Firewall ist nur ein Baustein
- Kann getunnelt werden
- Weitere Maßnahmen notwendig wie z.B.
  - IT-Awereness
  - Backup
  - Bitdefender
  - Aktuelle Systeme
  - Nur das Notwendige (aktivieren, bereitstellen, nutzen)
  - weitere

Zusammenfassung

- Noch kein Netzschutz? -> Beantragen
- Sonst: Regelwerk anfordern
- Regelwerk aufräumen
- Inventur machen, aufräumen
- IPAM nutzen

- Diskussion