Informationsveranstaltung für Netzverantwortliche im MWN

http://www.lrz.de/services/schulung/unterlagen/netzverantwortliche/

Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring

Agenda

- MWN PC
- Aufgaben eines NV
- 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

- Nützliche Informationen und Werkzeuge für NV: https://www.lrz.de/services/schulung/unterlagen/netzverantwortliche/nv-basiswissen-2019.pdf

Hinweis für TUM Netzverantwortliche

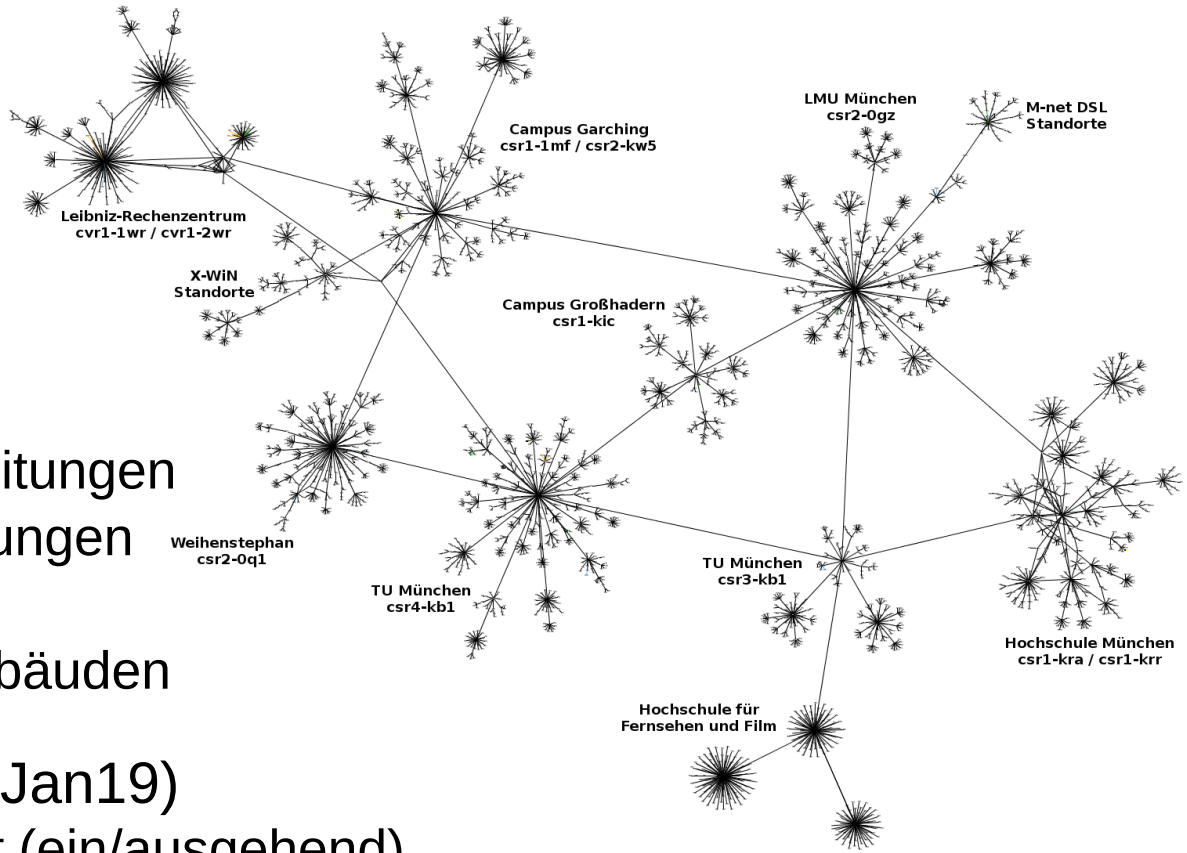
- Die hinterlegten Kennungen werden auf TUM Kennungen umgestellt (falls noch keine TUM Kennung hinterlegt ist)
- Automatisiert, Netzverantwortlicher muss nichts machen.
- Hinweis-Mail wenn Umstellung erfolgt ist

Agenda

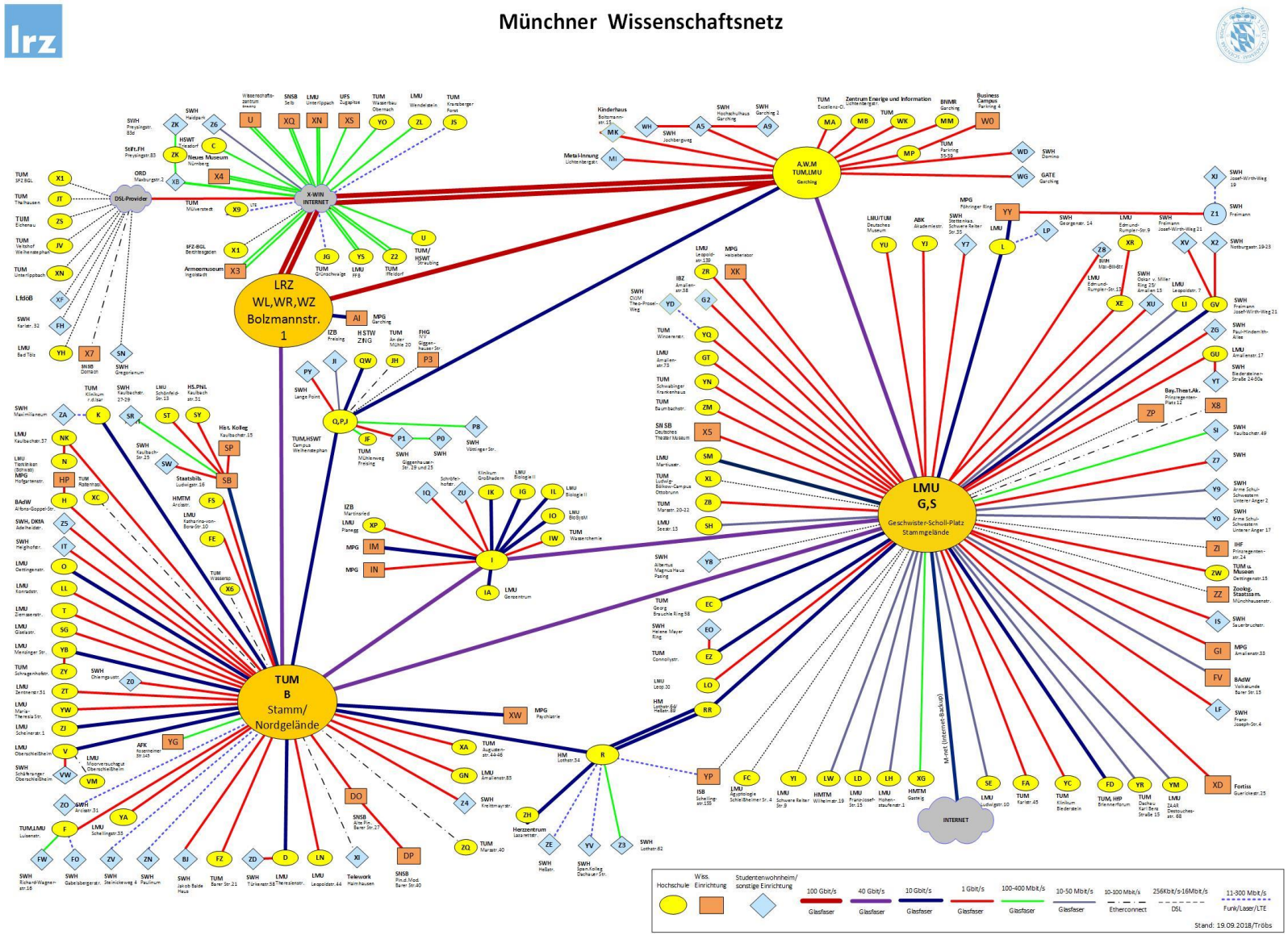
- MWN PC
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - ISO 20k/27k Zertifizierung
  - LWL Ausschreibung
  - Switch-Auswahl
  - WLAN-Auswahl
  - WLAN, Eduroam of Campus, @BayernWLAN
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - InHPC
  - NIP
- Dienste im MWN
- Sicherheitsmonitoring

MWN - Überblick

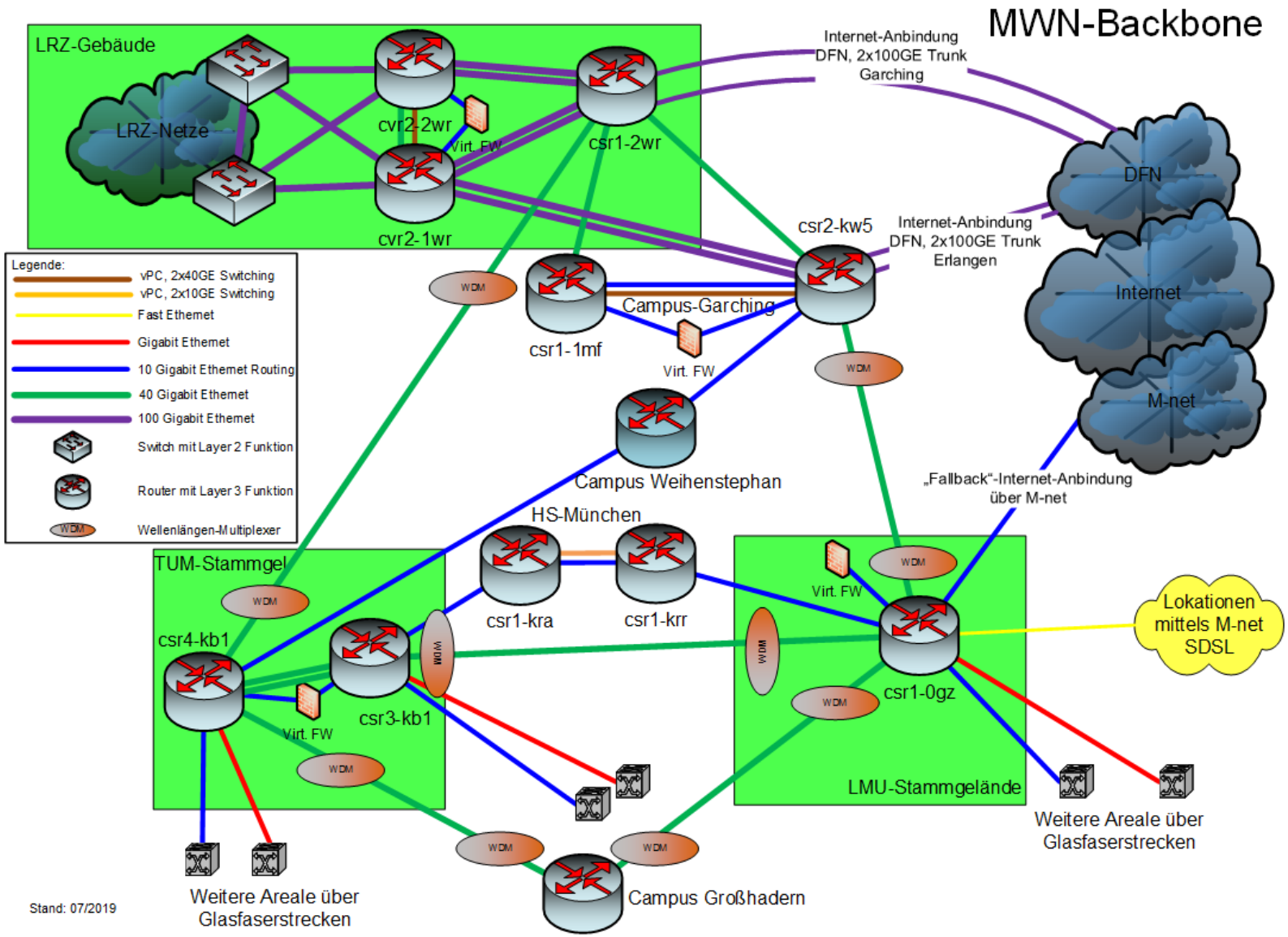
- Kommunikationsnetz für Münchner Hochschulen
  - 136.000 Studenten
  - 30.000 Mitarbeiter
- Kennzahlen
  - 14 Core-Router
  - 72 Standort-Router
  - 1.800 Switches
  - 4.400 Access points
  - 77 gemietete dark fibre Leitungen
  - 40+ private dark fibre Leitungen
  - > 200.000 Endgeräte
  - 59 Lokationen mit 600 Gebäuden
- Übertragene Daten (Nov. 18, Jan19)
  - 3.400 / 1.200 Tbyte/Monat (ein/ausgehend)
  - 45 PByte/Monat über Backbone



MWN 2019

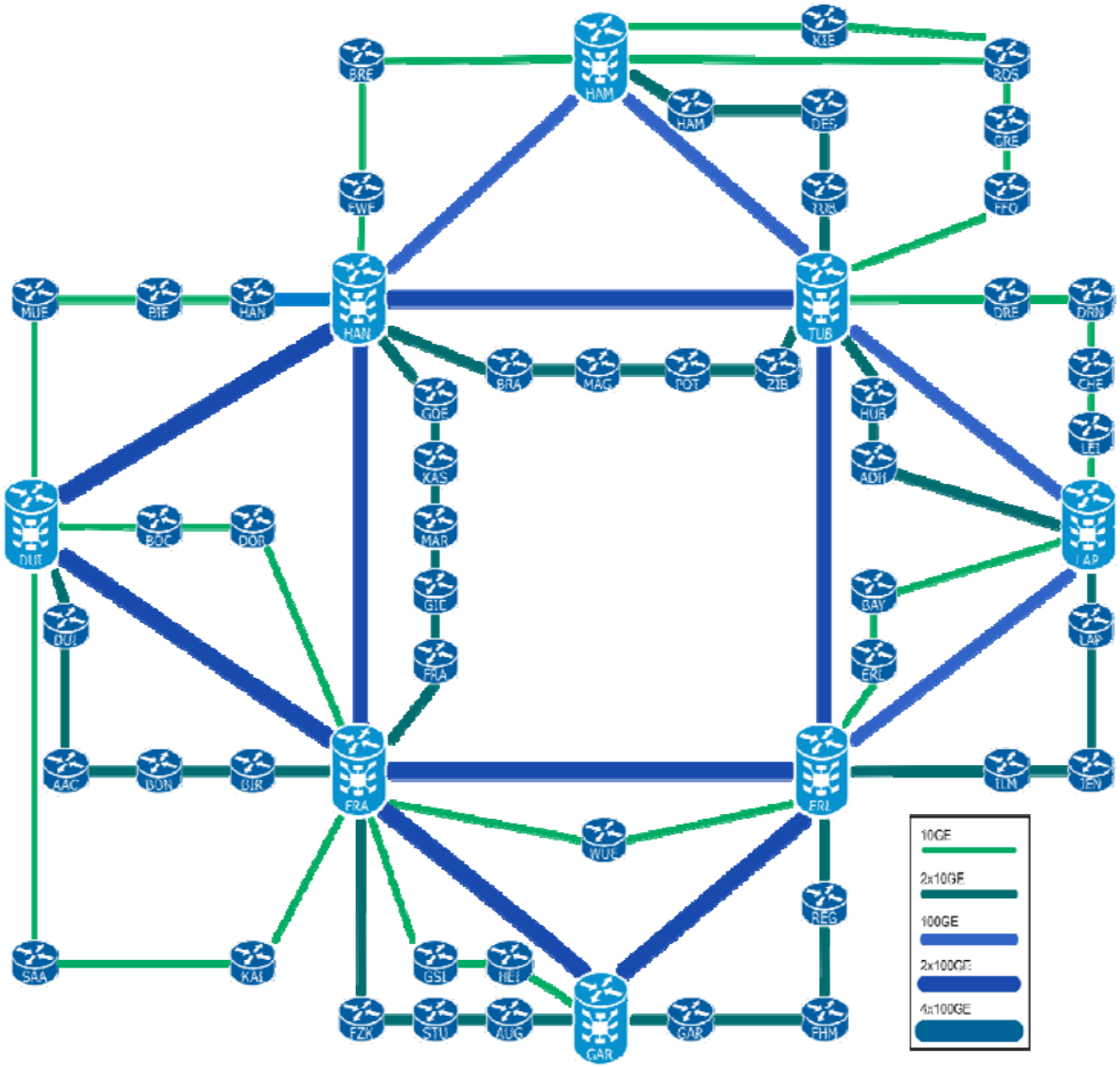

Münchner Wissenschaftsnetz
LRZ
WL,WR,WZ
Bolzmannstr.
1
TUM
B
Stamm/
Nordgelände
LMU
G,S
Geschwister-Scholl-Platz
Stammgelände
Q,P,J
I
R
A,W,M
TUM,LMU
Garching
X-WIN
INTERNET
DSL-Provider
INTERNET
Hochschule
Wiss. Einrichtung
Studentenwohnheim/
sonstige Einrichtung
100 Gbit/s
Glasfaser
40 Gbit/s
Glasfaser
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

- MWN PC
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - ISO 20k/27k Zertifizierung
  - LWL Ausschreibung
  - Switch-Auswahl
  - WLAN-Auswahl
  - WLAN, Eduroam of Campus, @BayernWLAN
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - InHPC
  - NIP
- Dienste im MWN
- Sicherheitsmonitoring

ISO 20k/27k Zertifizierung

- Das LRZ hat die ISO/IEC 20000 und ISO/IEC 27000 Zertifizierung bestanden!
- Erstes wissenschaftliches Rechenzentrum in Deutschland mit dieser Zertifizierung!
- ISO 9001 Qualitätsmanagement-Anforderungen
  - 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

- MWN PC
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - ISO 20k/27k Zertifizierung
  - LWL Ausschreibung
  - Switch-Auswahl
  - WLAN-Auswahl
  - WLAN, Eduroam of Campus, @BayernWLAN
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - InHPC
  - NIP
- Dienste im MWN
- Sicherheitsmonitoring

LWL Ausschreibung

- Alle LWL Strecken im MWN wurden neu ausgeschrieben (Optionen auf Strecken)
- Jede Strecke ist ein eigenes Los
- Eine Rahmenvereinbarung wird mit allen Providern angestrebt die eine Strecke gewonnen haben.
- Bei neuen Strecken gibt es einen Wettbewerb zwischen allen Providern die RV-Teilnehmer sind.

Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - ISO 20k/27k Zertifizierung
  - LWL Ausschreibung
  - Switch-Auswahl
  - WLAN-Auswahl
  - WLAN, Eduroam of Campus, @BayernWLAN
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - InHPC
  - NIP
- Dienste im MWN
- Sicherheitsmonitoring

Switch-Auswahl

- Rahmenvertrag für HP-Switches läuft aus und ist überbucht
- Auswahl und Tests von Switches
  - Cisco, HP und Huawei im Test
  - Andere Hersteller bereits im Vorfeld ausgeschlossen
    - Erfüllen wichtige Punkte der Anforderungen nicht
  - Der Sieger ist … Huawei
    - Sehr breite Produktpalette
    - 100 GE auch auf Edge-Switches verfügbar
    - Einheitliche Management Oberfläche
    - Bestes Lizenzmodell
  - Ausschreibung für Lieferanten läuft
    - Neuer Vertrag Oktober 2019

Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - ISO 20k/27k Zertifizierung
  - LWL Ausschreibung
  - Switch-Auswahl
  - WLAN-Auswahl
  - WLAN, Eduroam of Campus, @BayernWLAN
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - InHPC
  - NIP
- Dienste im MWN
- Sicherheitsmonitoring

WLAN-Auswahl

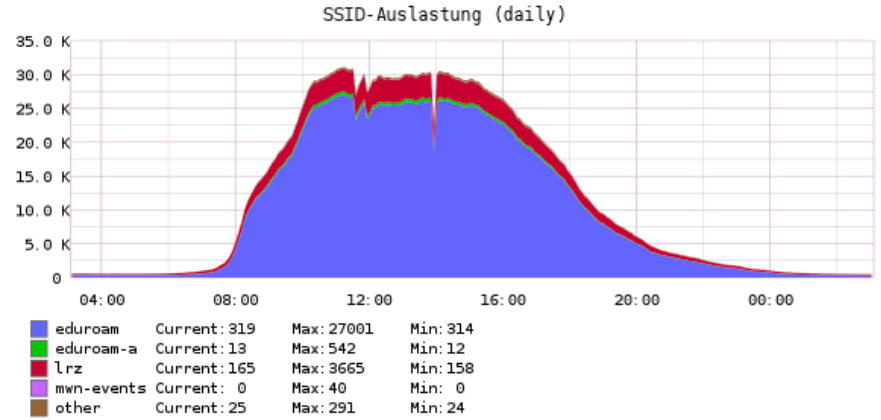
- Rahmenvertrag für Alcatel-Lucent (Aruba) APs ausgelaufen
- Auswahl und Test von Accesspoints
  - Viele Hersteller angeschrieben
    - Die meisten erfüllten die Anforderungen nicht.
  - Fünf Hersteller wurden getestet
    - Der Gewinner ist … HP-Aruba
    - Schwenk von Alcatel-Aruba auf nativ Aruba hauptsächlich wegen des besseren Supports
    - Ausschreibung des Lieferanten läuft.
    - Neuer Vertrag im Oktober 2019

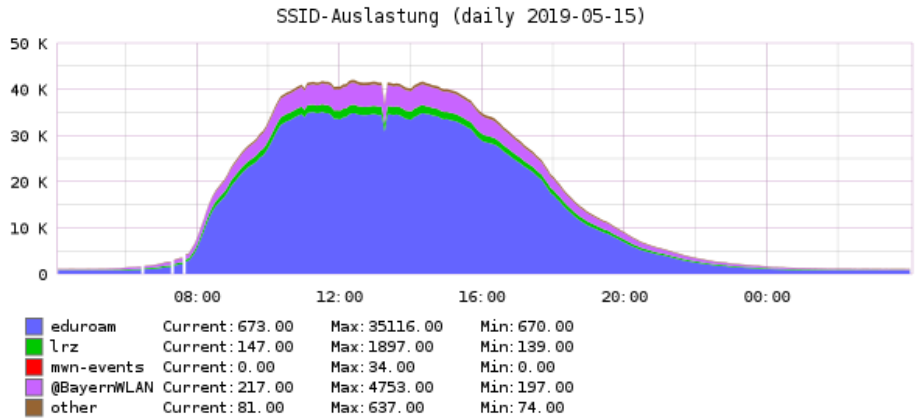
Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - ISO 20k/27k Zertifizierung
  - LWL Ausschreibung
  - Switch-Auswahl
  - WLAN-Auswahl
  - WLAN, Eduroam of Campus, @BayernWLAN
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - InHPC
  - NIP
- Dienste im MWN
- Sicherheitsmonitoring

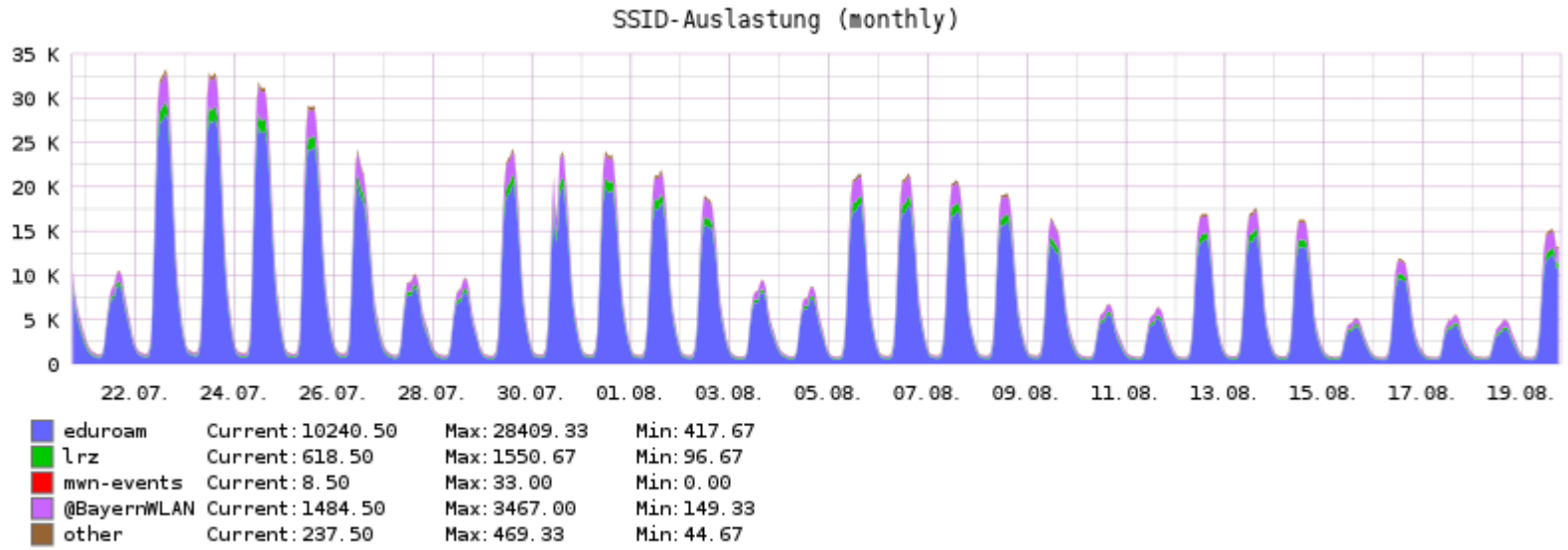
Entwicklung WLAN im MWN

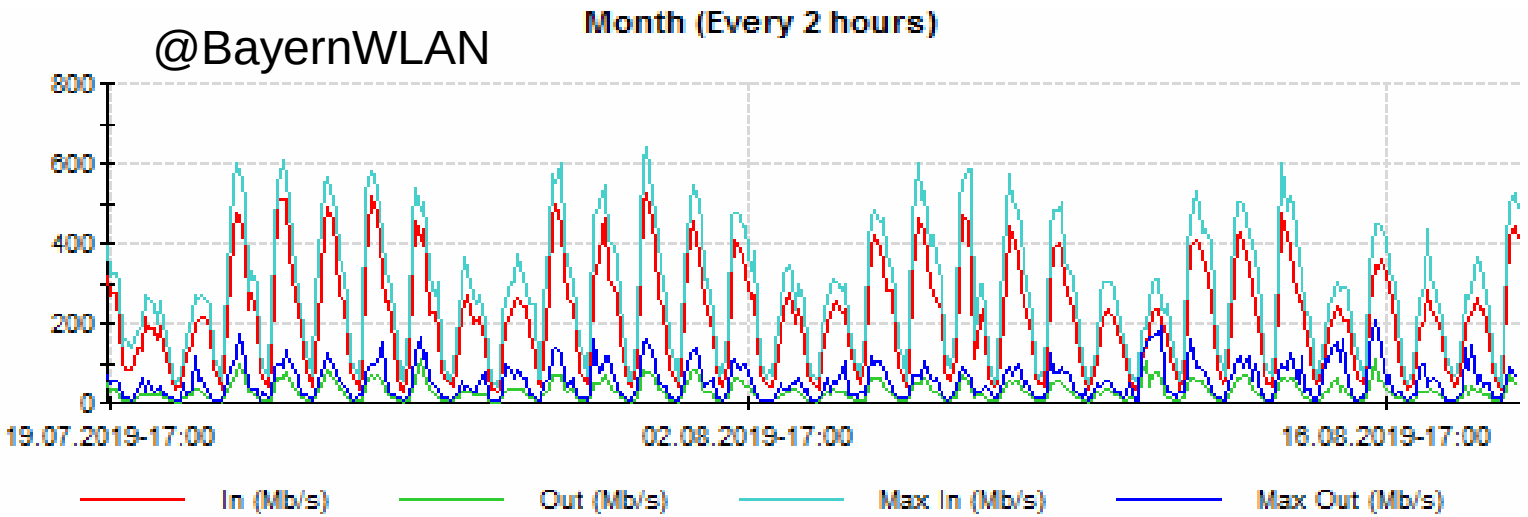
- Entwicklung seit letzten NV-Treffen (2016)
- Anzahl der APs
  - 2010: 1.412 APs
  - 2013: 2.066 APs
  - 2016: 3.095 APs
  - 2019: 4.393 APs
- Anzahl der gleichzeitigen Nutzer
  - 2010: 3.760
  - 2013: 12.228
  - 2016: 33.184
  - 2019: 44.366





WLAN, EDUROAM, @BayernWLAN





Startseite Kontakt Impressum Datenschutz Inhaltsübersicht Suchen ... Vorlesen

Bayerisches Staatsministerium der Finanzen und für Heimat

AKTUELLES SERVICE THEMEN MINISTERIUM

Aktuelles › Pressemitteilungen

Pressemitteilung Nr. 133
München, 14.06.2019

FÜRACKER: ZIELMARKE VON 20.000 BAYERNWLAN-HOTSPOTS VORZEITIG GEKNACKT!

20.000ster Hotspot in der Stadtbücherei Ingolstadt in Betrieb genommen

Der Freistaat Bayern hatte sich das Ziel gesetzt, bis Ende 2020 mit einem engmaschigen Netz von 20.000 kostenfreien BayernWLAN-Hotspots ausgestattet zu sein. Im Fokus stehen dabei vor allem Kommunen, touristische Highlights, Hochschulen und Behördenstandorte. „Diese angestrebte Marke haben wir mit der Inbetriebnahme des Hotspots in der Stadtbibliothek Ingolstadt nun sogar schon eineinhalb Jahre früher geknackt. Damit ist der Freistaat Nr. 1 unter den Flächenländern in Deutschland", freute sich Finanz- und Heimatminister Albert Füracker und betonte: „Auch wenn wir schon jetzt viel erreicht haben, machen wir natürlich weiter. Wir werden auch künftig insbesondere die ländlichen Gemeinden tatkräftig beim Aufbau von digitaler Infrastruktur unterstützen."

- „Wir machen weiter“
- Freistaat fördert Kommunen für BayernWLAN in ÖPNV-Bussen
  - aktuell 900 Busse in ganz Bayern versorgt
- Mai 2019: Mehr als 7 Mio Nutzer im BayernWLAN
- Von den 20.236 APs sind von den Hochschulen: **12.837**

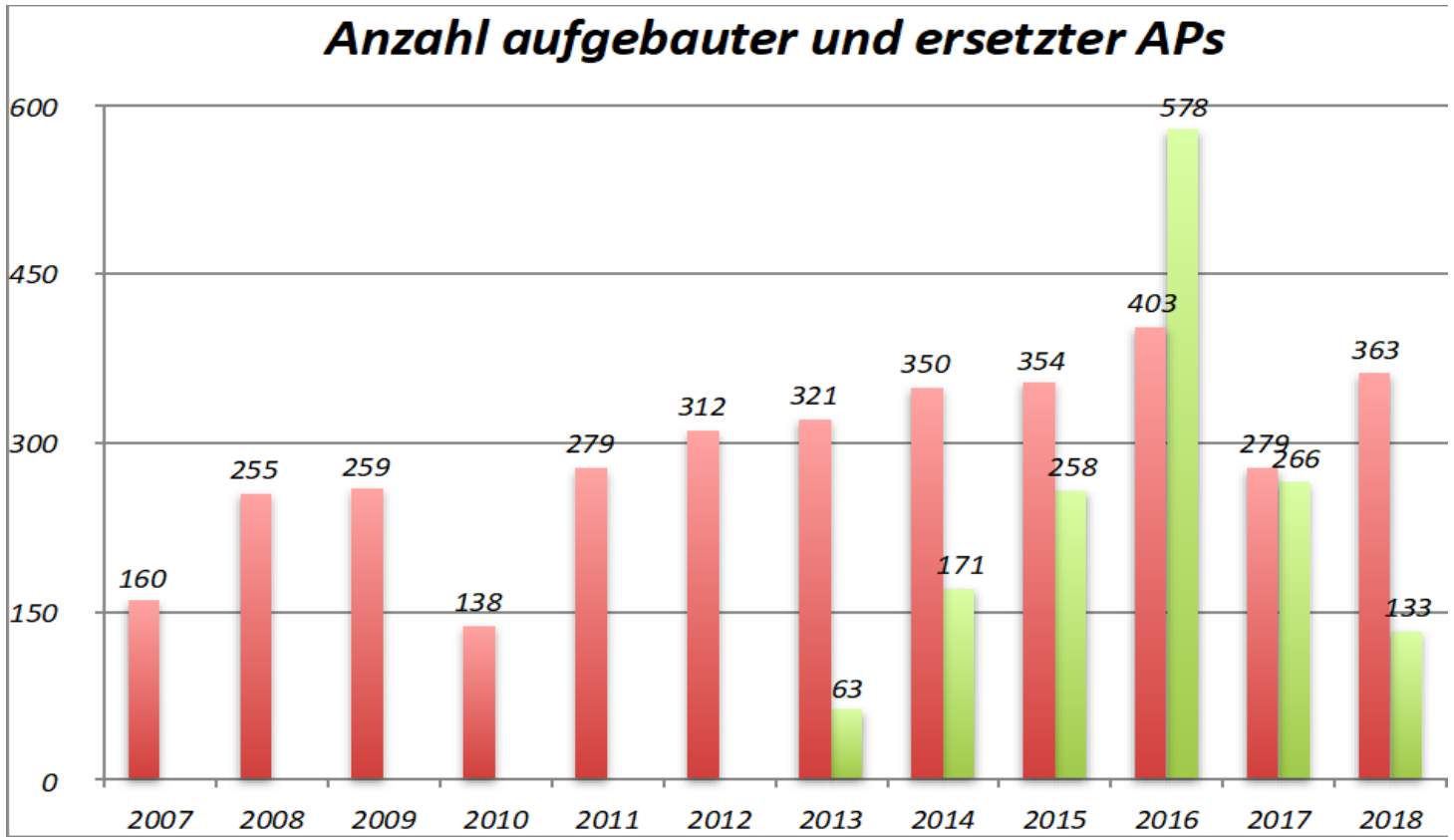
- Eduraom-Map: https://map.eduroam.de
- Bayern-WLAN Map: https://www.wlan-bayern.de/

WLAN-Technik

- Controller-basierte APs von Alcatel-Lucent (seit 2013)
  - APs werden über Controller administriert und provisioniert
  - Controller nur noch am TUM Stammgelände und im LRZ (Garching)
  - Ausfallsicher: Master-Controller im LRZ kann bei Ausfall eines Controllers übernehmen
- „kleine“ APs (Aruba 303) bis 10 Nutzer ausreichend
- „große“ APs (Aruba 325) bis 100 Nutzer
- Ende des Jahres neue APs der Aurba 550er Serie
  - „Wi-Fi 6“: Bessere Versorgung in Umgebungen mit vielen Clients (hoffentlich!)

WLAN Herausforderungen

- Gemischte WLAN-Infrastruktur (HP, Alcatel)
- Probleme durch alte APs mit neuen Clients
- Alle alten HP APs sollen bis Ende 2019 ersetzt werden



WLAN: hochbelastete Bereiche

- Nachverdichtung in hoch belasteten Bereichen:
  - Bibliotheken
  - Staatsbibliothek
  - Große Hörsäle
- 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 versorgen
- Wünsche nach APs über Ticket am Service-Desk: https://servicedesk.lrz.de

Veranstaltungs-WLAN: mwn-events

- Kein offenes WLAN mehr für Veranstaltungen
- Gesicherte SSID mwn-events
- Beantragung über Formular, unter: http://www.lrz.de/wlan
- Zugangsdaten pro Veranstaltung (Benutzername, Passwort)
- Entsprechendes Profil erhältlich über: http://www.lrz.de/services/netz/wlan/mwn-events/
- Erfahrungen:
  - Rückläufig
  - @BayernWLAN als Ersatz

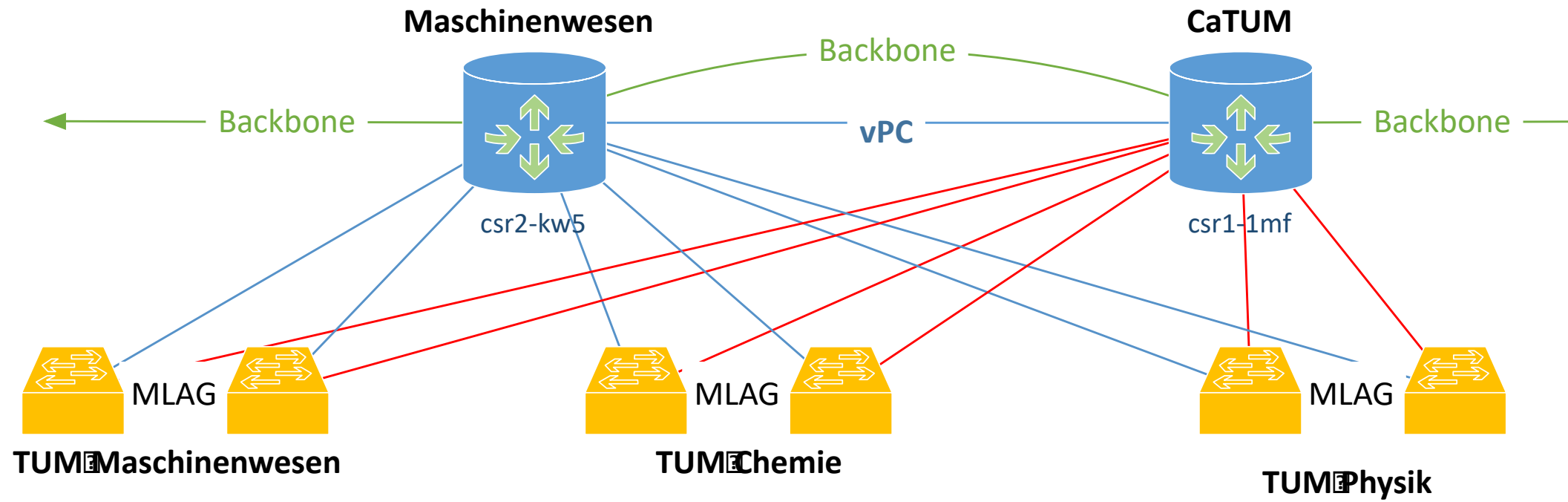
Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - ISO 20k/27k Zertifizierung
  - LWL Ausschreibung
  - Switch-Auswahl
  - WLAN-Auswahl
  - WLAN, Eduroam of Campus, @BayernWLAN
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - InHPC
  - NIP
- Dienste im MWN
- Sicherheitsmonitoring

Router Redundanz-Konzept im MWN

- Seit 2016 wird der Campus Garching redundant von Router-Pärchen versorgt.
- Das gleiche streben wir für Weihenstephan, Großhadern, TUM-Stammgelände und LMU-Stammgelände an.
- Ist immer dort möglich wo genügend Glasfasern und redundante Trassen vorhanden sind
- Nächster Redundanz-Standort wird Weihenstephan sein.

Redundante Versorgung von Gebäuden



Legende

neuer Switch

Router Bestand

MLAG = Mul<-Chassis Link Aggrega<on

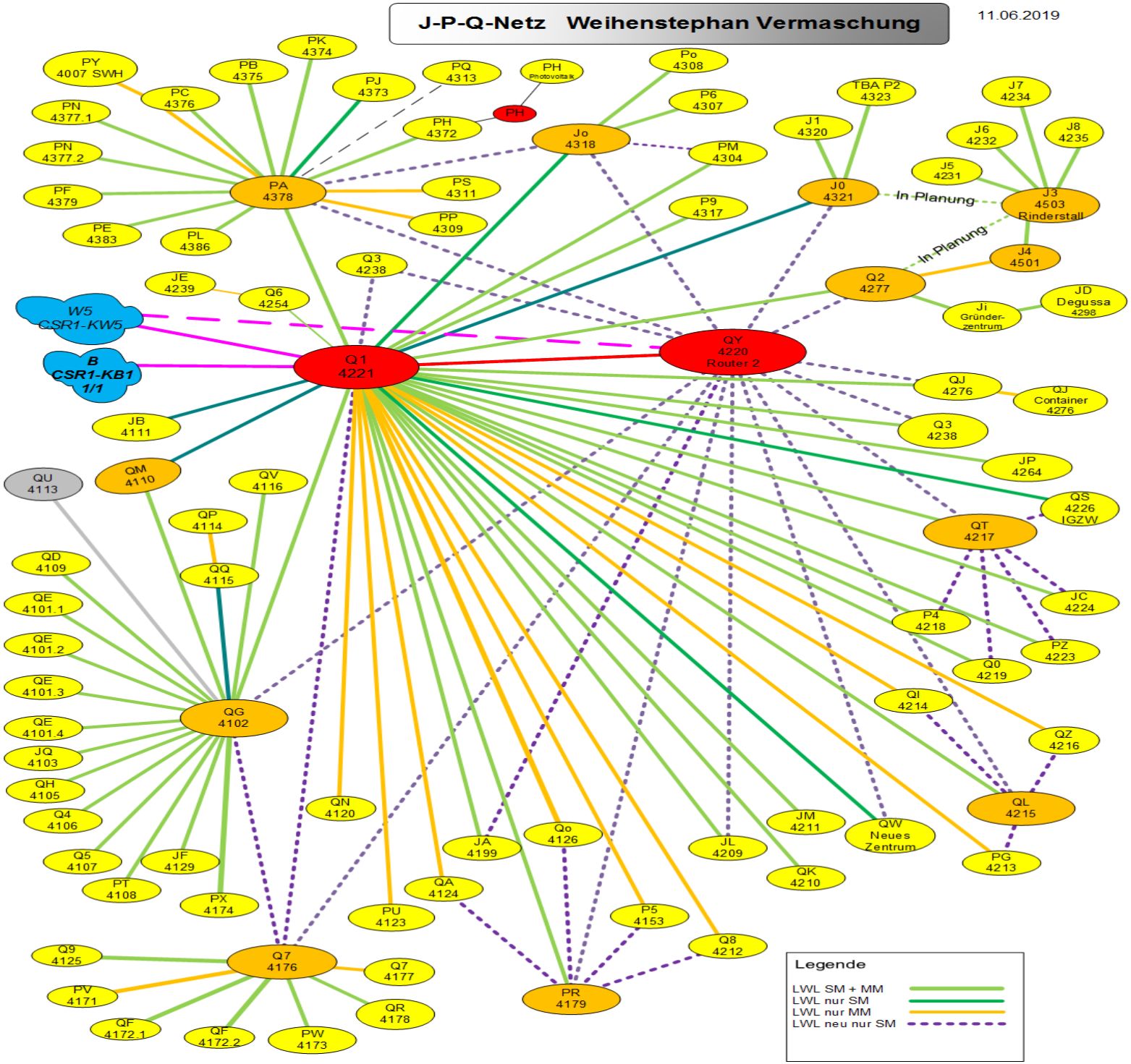
vPC = virtueller Port-Channel

alte Trasse

neue Trasse

Erhöhung der Redundanz am Campus Weihenstephan

- LWL-Ertüchtigung (gestartet 2015)
  - Sehr viele Gebäude nur mit Multimode versorgt
  - Single-Mode-Nachrüstung
  - Anbindung der Gebäude über zwei Faserpaare (selbe Trasse, unterschiedliche Leerrohre) (2016)
- 2. Routerstandort
  - Auswahl eines zweiten Router-Standortes (Bibliothek)
  - Verstärkung der Querverbindung Bibliothek – Telefonzentrale



Erhöhung Redundanz am Campus Großhadern

- Zweiter Aufpunkt BMC (Biomedizinsches Centrum)
- Aufbau eines zweiten Routers
- Alle Gebäude per Glasfaser zu diesem Gebäude
- Bisher ca. 20% realisiert

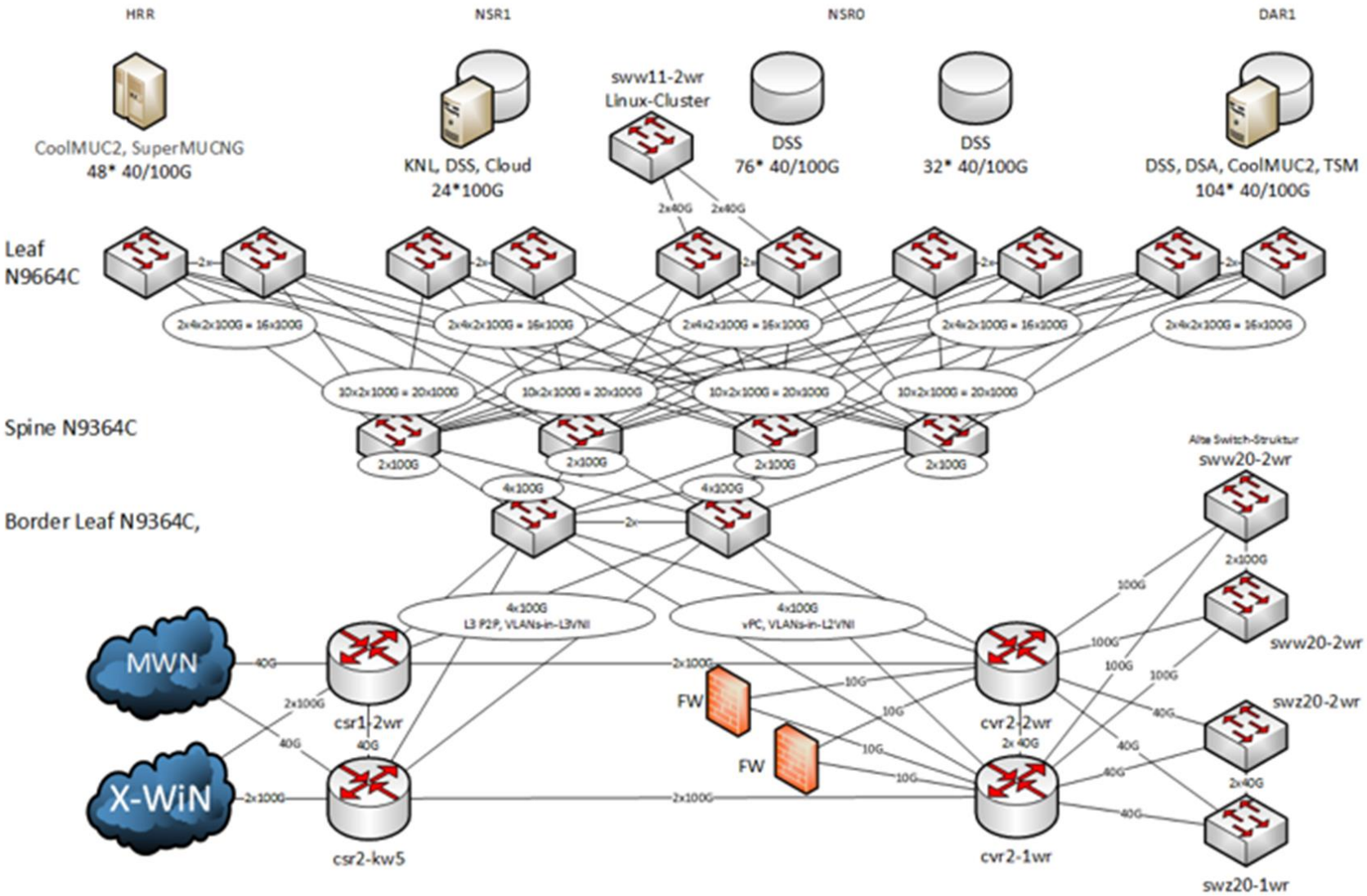
Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - ISO 20k/27k Zertifizierung
  - LWL Ausschreibung
  - Switch-Auswahl
  - WLAN-Auswahl
  - WLAN, Eduroam of Campus, @BayernWLAN
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - InHPC
  - NIP
- Dienste im MWN
- Sicherheitsmonitoring

InHPC (100GE – Jülich,Stuttgart,LRZ)

- Mitte/Ende 2017:
- Bedarf an >> 200 40G/100G Ports für SuperMUC NG und DSS-Anbindung,
- auf 6 Brandabschnitte verteilt
- SuperMUC-Switches/Hausrouter (N7k) Aufrüstung nicht bezahlbar
- Vergleich von zwei Lösungen:
- „Dicke Berta“ mit klassischem modularen Router mit hoher Port-Dichte
- Leaf-Spine Lösung mit fixen Systemen nah am Endhost

InHPC (Leaf+Spine)



InHPC (Leaf+Spine)

- Bandbreiten:
  - Leafpaare mit je 1,6 Tbit/s am Spine
  - jeweils 96x 100G/40G Ports
  - 1:6 Oversubscription bei 100G
  - Border mit je 400 Gbit/s am Spine
  - Je 200G zum MWN und LRZ
  - keine Oversubscription
- Noch genug freie Ports,
- Sonst Skalierung in die Breite oder in die Höhe
- Protokolle
  - VXLAN (Overlay) und BGP EVPN (Control Plane)
  - Konfiguration nicht mehr ganz einfach zu verstehen

Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
  - MWN Überblick
  - ISO 20k/27k Zertifizierung
  - LWL Ausschreibung
  - Switch-Auswahl
  - WLAN-Auswahl
  - WLAN, Eduroam of Campus, @BayernWLAN
  - Backbone (WDM, Ausfallsicherheit, Redundanz)
  - InHPC
  - NIP
- Dienste im MWN
- Sicherheitsmonitoring

Netzinvestitionsprogramm V (NIP V)

- Standorte 2017
  - Leopoldstr. 15
  - Richard-Wagner-Str. 10
  - Akademiestr.1 / Ludwig 33
  - Schellingstr. 3
- Standorte 2018:
  - Schellingstr. 5, 7, 9, 10, 12
  - Amalienstr. 52, 83
  - Veterinästr. 13
  - Ludwig 33
  - Leo 3

- Standorte 2019
  - Schellingstraße 5, 7, 9, 10
  - Historicum
  - Richard Wagner-Straße 10
  - Ludwigstraße 33
  - Akademiestraße 1
  - Amalienstraße 83
  - Bereich Geschwister-Scholl-Platz Süd

Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewalls
  - Incident und Change Management
  - VPN und Secomat
  - E-Mail/Exchange
- Sicherheitsmonitoring

Virtuelle Firewalls im MWN

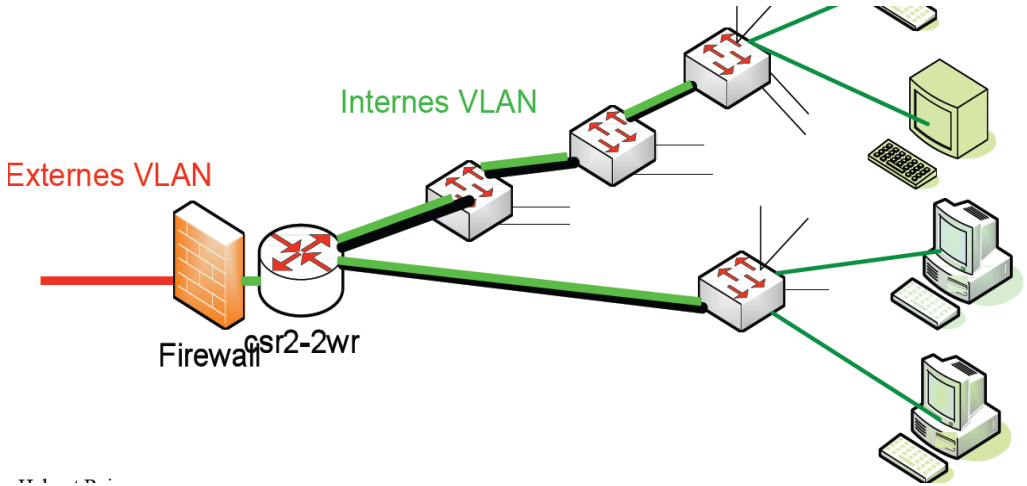
- Fünf Standorte (Q,B,G,W5/MF,LRZ)
- Redundante Hardware, VMWare Virtualisierung
  - 16 physische Hosts, 448 virtuelle Maschinen
  - HA: Jeder Kunde erhält Firewall-Paar (Neu: ausfallfreie Updates im laufenden Betrieb möglich)
  - VPN-Möglichkeit: VPN in eigene (d.h. Lehrstuhl-) Netze realisierbar, Rechte/Kennungen kann Masteruser verwalten (über das LRZ-ID-Portal)
- Firewall-Authentifizierung mit SIM/AD-Kennungen, die der Masteruser verwalten kann. Keine gesonderten Firewall-Kennungen.
- Java-freie Web-Oberfläche
- Hohe Flexibilität durch Zusatzpakete (LRZ wird nicht alles unterstützen!)
- Kommerzieller Support erhältlich; aktive Entwicklergemeinde

pfSense-Logo; Quelle: Screenshot

Integration der virtuellen Firewalls im MWN

- Standortkonzept wird beibehalten (B,G,W5/MF,LRZ, Q)
- Gemischte Hardware. HP Server DL380 (56 cores, 128 GB RAM)
- Virtualisierung mittels ESXi 6.7.0
- 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 möglich
- 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 (ca. 6 mal pro Jahr, siehe Newsletter und LRZ Kursangebote)
- 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.

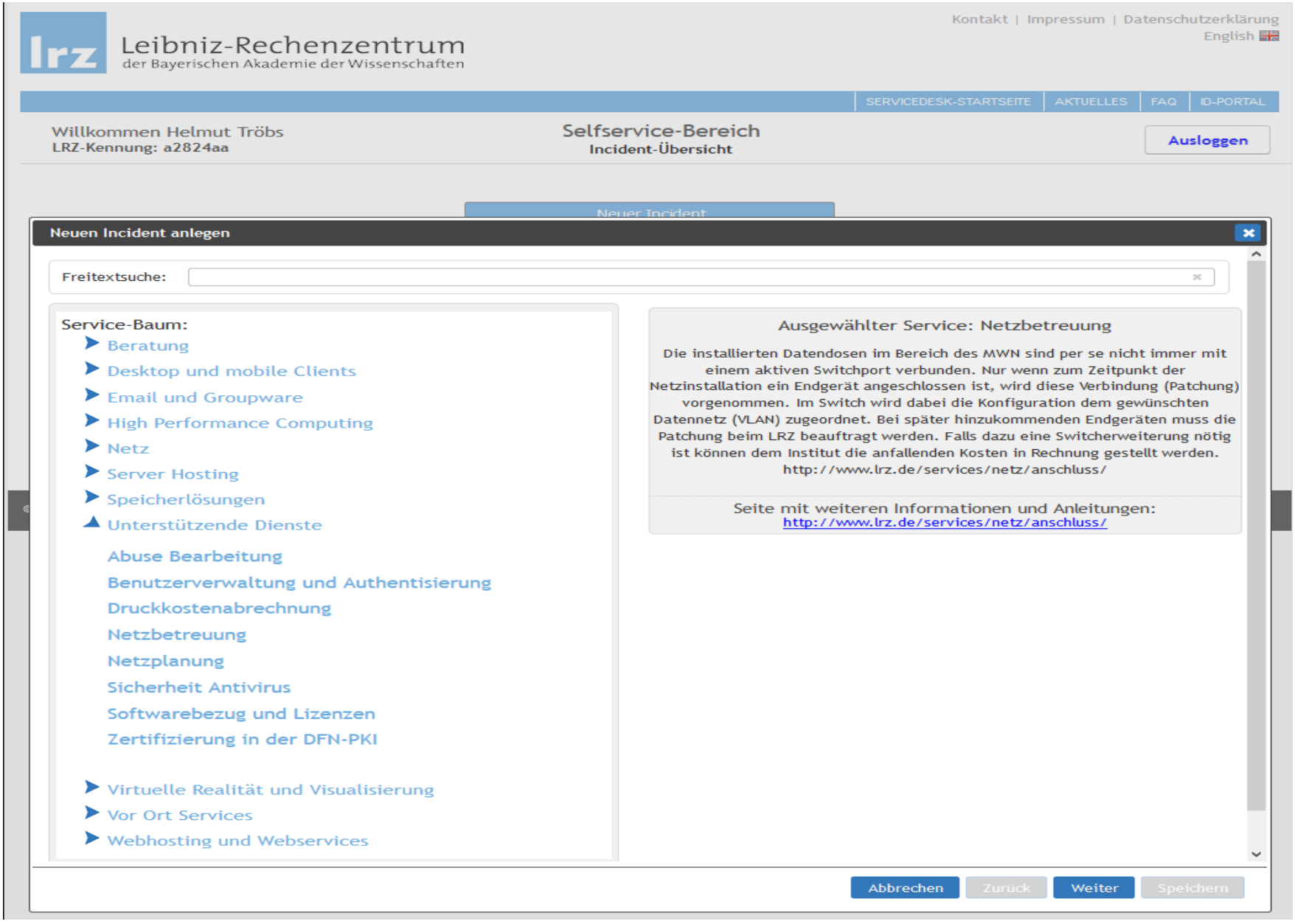
Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewalls
  - Incident und Change Management
  - VPN und Secomat
  - E-Mail/Exchange
- Sicherheitsmonitoring

Incident und Change Management

- LRZ ist bestrebt ein Service Management nach ISO 20000 zu betreiben (Zertifiziert seit Mitte 2019)
- Störungen und Service Requests werden über Tickets erfasst
- Ticket über Self-Service Portal oder Hotline erfassen
  - https://selfservice.lrz.de
  - 089 / 35831 – 8800
- Aus Service Request (z.B. Wunsch nach WLAN) wird i.d.R. ein Change
  - Abwicklung und interne Koordinierung von Änderungen an der Infrastruktur

Incident-Selfservice



Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewalls
  - Incident und Change Management
  - VPN und Secomat
  - E-Mail/Exchange
- Sicherheitsmonitoring

VPN im MWN

- Zugang zu internen Diensten im MWN
  - Zuordnung meist über IP-Adressen und nicht über Kennungen
- Verschiedene Betriebsysteme und Clients werden unterstützt (siehe Tabelle nächste Folie)
  - Oft erfolgt die Installation des Clients direkt vom VPN-Server
- IP-Adresszuordnung über die Kennung
  - HM, HSWT, LMU, TUM, LRZ
- ab AnyConnect 4.x:
  - Unterstützung von mehr Clients, z.B. iOS
  - Neues Lizenzmodell:
    - nicht mehr maximale Anzahl von Verbindungen pro Server
    - pro Nutzer ist eine Lizenz nötig (dieser kann aber mehrere Geräte verwenden)

Vergleich von verfügbaren Clients zu Betriebssystem

	Cisco AnyConnect	Cisco Ipsec	openConnect (OSS)	Ipsec (vpnc) (OSS)
Android	Google Play		Google Play	Google Play (vpncilla)
iOS	App Store	Integriert		
Linux	Webdeploy		Repository	Repository
macOS	Webdeploy	Integriert	MacPorts, etc	MacPorts, etc
Windows	Webdeploy	bis Windows 7	Openconnect_gui	Shrew VPN Client

https://asa-cluster.lrz.de

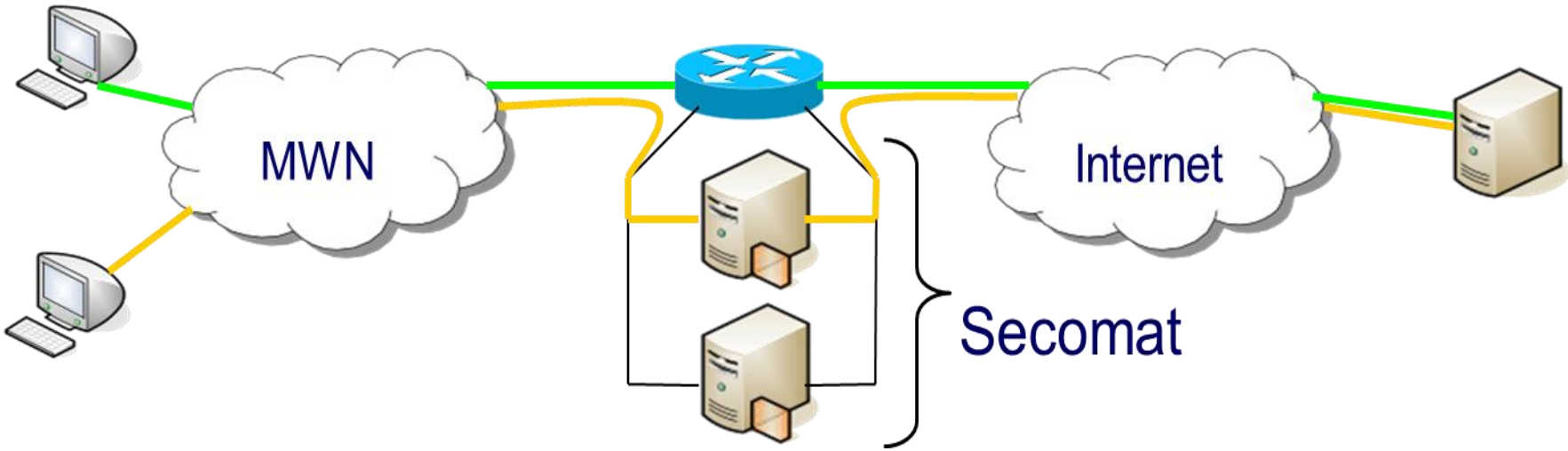
VPN im MWN

- Auto-Reconnect nach Ruhezustand
- IPv6 Client-IP bei AnyConnect und openConnect
- IPv6 Verbindung zum Server (DS-Lite DSL Nutzer)
  - direkte IPv6 Verbindung zum Server
- Split-Tunneling deaktivieren: „!“ vor die Kennung setzen
- Bei Problemen: FAQs lesen und Servicedesk kontaktieren.

Secomat

- Transparentes NAT-Gateway mit integriertem, automatischem Abuse-Monitoring und Traffic-Shaping
  - Umleitung per Policy based Routing (private Adressen, Eduroam, VPN, ausgewählte Subnetze)
  - Steuerung Volumina und Bandbreiten (z.B Begrenzung P2P)
  - 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.

Secomat



Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
  - Virtuelle Firewalls
  - Incident und Change Management
  - VPN und Secomat
  - E-Mail/Exchange
- Sicherheitsmonitoring

E-Mail/Exchange TUM

- TUM: Migration des Service 'Mail' von mailin.lrz.de zu TUM Exchange
  - Die Nutzung des E-Mail-Servers 'mailin.lrz.de' durch die TUM wird zum 31.12.2019 beendet.
  - LRZ-Kennungen aus Master User Projekten können Mail-Box-Inhalte und ausgewählte E-Mail-Adressen zu TUM Exchange migrieren oder endgültig löschen bzw. verfallen lassen. Für die Migration wird ein Assistent in TUMonline bereitgestellt.
  - Die Maildomain lrz.tu-muenchen.de wird zum 31.12.2019 gelöscht. lrz.tum.de bleibt erhalten.
  - Die betroffenen Master User und Benutzer werden auch noch via E-Mail informiert
  - Mehr dazu im TUM-Wiki: https://wiki.tum.de/x/wgd1DQ

E-Mail/Exchange LMU

- LMU: Nutzung von MS Exchange ohne extra Lizenzkosten jetzt möglich
  - Auch die LMU hat mittlerweile ein Campus-Agreement mit Microsoft, damit ist die Lizenzierung abgedeckt
  - Exchange bietet Groupware-Funktionen:
    - neben E-Mail u.a. persönliche und gemeinsame Kalender, Kontakte und Aufgaben
    - Gruppenverteiler
    - shared Mailboxen
    - Mehr dazu: https://doku.lrz.de/x/DQEOAQ
  - ABER: bevor Exchange genutzt werden kann, müssen die LRZ- und LMU-Kennungen eines LRZ-Projekts konsolidiert werden.
    - Mehr dazu: https://doku.lrz.de/x/j4JlAg

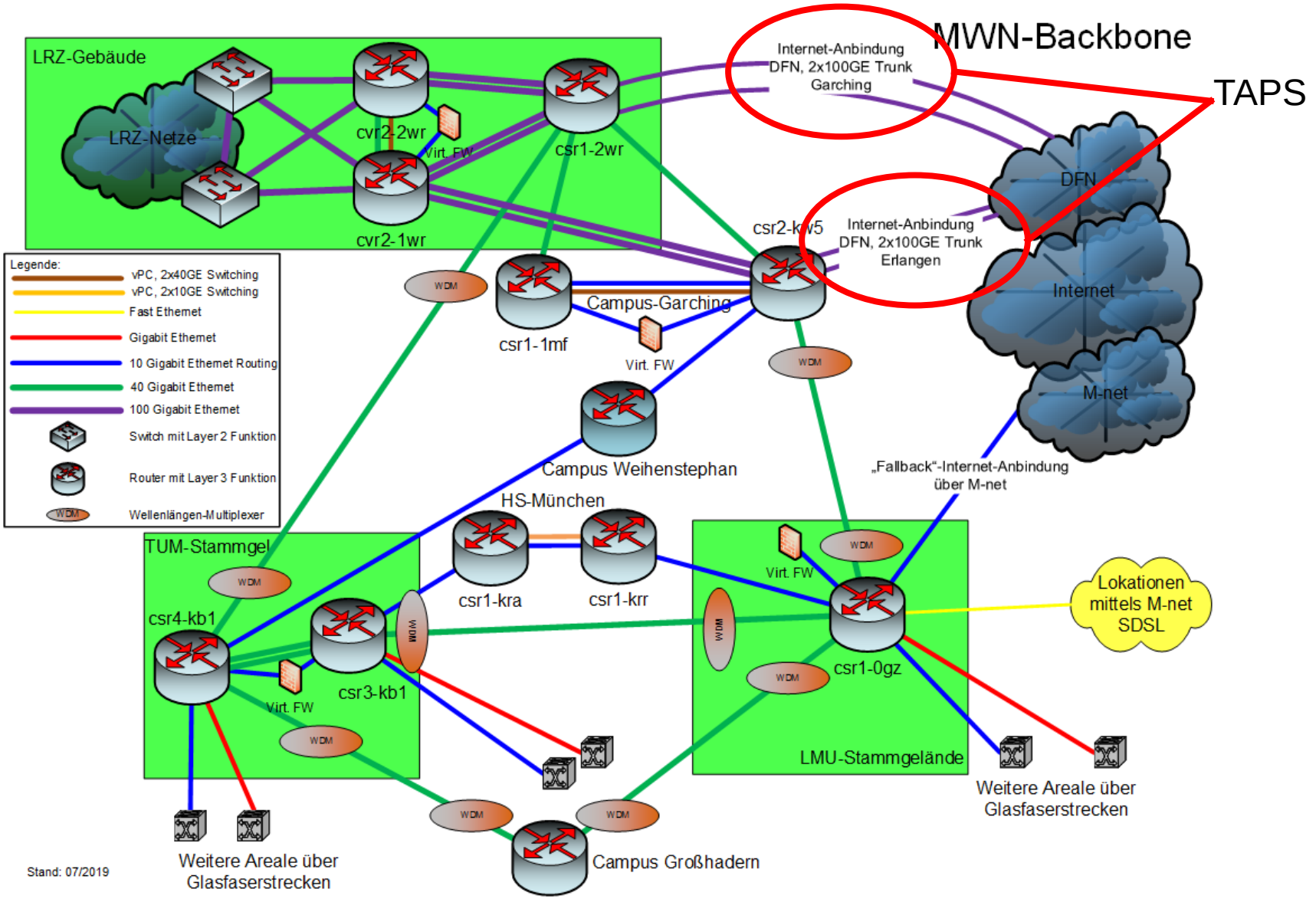
Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security Information & Event Management (SIEM)
  - Verwaltung gesperrter IP-Adressen
  - Self-Service-Web-Portal NeSSI
  - DFN-CERT-/CERT-Bund-Meldungen

Security Information & Event Management (SIEM) am LRZ

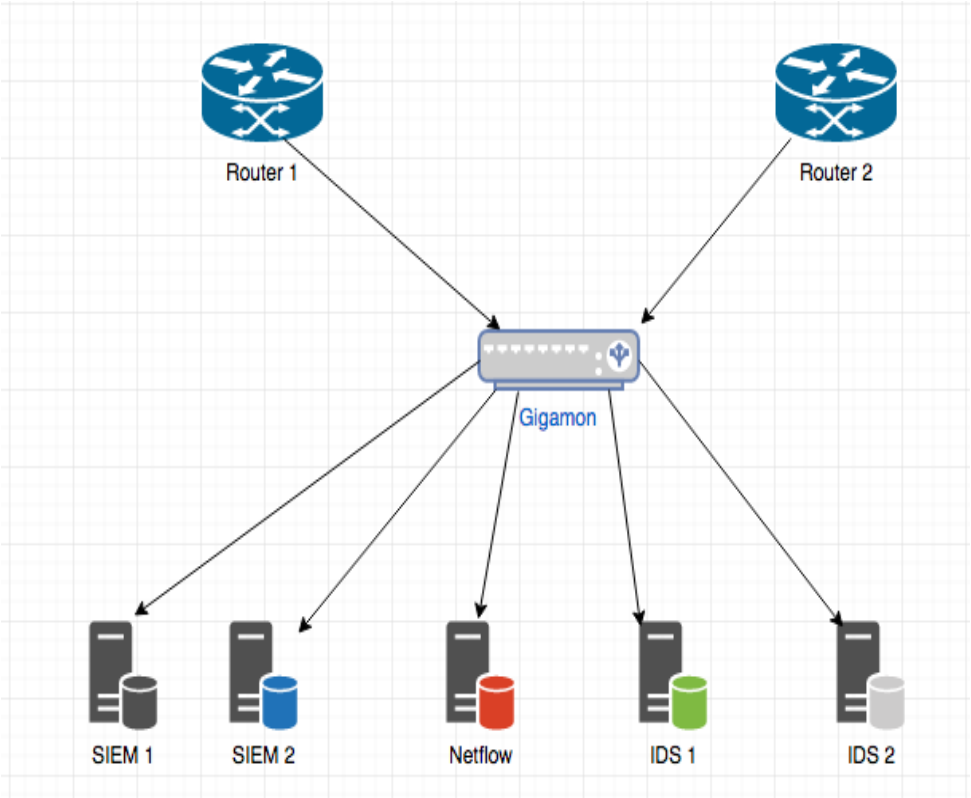
- Motivation für den SIEM-Einsatz:
  - Zahlreiche Quellen für Security-Events, z.B. Suricata IDS, Netzkomponenten- und Server-Logfiles, …
  - Automatisierung und Vereinheitlichung von Aggregation, Korrelation, Auswertung und Reaktion
  - Erkennung von Abuse Ereignissen bevor ein Trigger von „außen“ erfolgt.
  - Schutz des Internet vor unseren Systemen

Monitoring des Verkehrs



Monitoring des Verkehrs

- 400 Gbit/s Monitoring
- Taps anstatt Monitoring Ports
- Full-Duplex verdoppelt nötige Anzahl Ports auf Switch-Seite
- Unsere Anforderungen:
  - Duplizieren
  - Load-Balancing
  - Filter pro Ausgang



Auswertung

- Flowmon
  - Auswertung von Netflow Daten
  - Gut für Traffic Statistiken und Kommunikationsbeziehungen
- Suricata (Open-Source-Tool)
  - Intrusion Detection System (IDS)
  - Ergebnisse werden zu Syslog oder Splunk gesendet

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

>	5/9/19 9:17:20.000 AM	May 9 09:17:20 secco05.srv.lrz.de May 9 09:17:20 secco05 suricata[1740]: [1:1000004:0] LRZ External SSH attack 60/60sec [Classification: (null)] [Priority: 3] {TCP} 185.176.27.86:55895 -> 129.187.61.149:22 Destination_IP = 129.187.61.149 | Destination_Port = 22 | EventName = LRZ External SSH attack 60/60sec | SID = 1000004 Source_IP = 185.176.27.86 | Source_Port = 55895 | host = secco05.srv.lrz.de | source = udp:9975 sourcetype = lrz_suricata
>	5/9/19 9:17:20.000 AM	May 9 09:17:20 secco04.srv.lrz.de May 9 09:17:20 secco04 suricata[1637]: [1:2404461:5361] ET CNC Ransomware Tracker Reported CnC Server group 62 [Classification: A Network Trojan was Detected] [Priority: 1] {UDP} 129.187.9.201:31249 -> 195.22.26.248:53 Destination_IP = 195.22.26.248 | Destination_Port = 53 EventName = ET CNC Ransomware Tracker Reported CnC Server group 62 | SID = 2404461 | Source_IP = 129.187.9.201 Source_Port = 31249 | host = secco04.srv.lrz.de | source = udp:9975 | sourcetype = lrz_suricata

Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security Information & Event Management (SIEM)
  - Verwaltung gesperrter IP-Adressen
  - Self-Service-Web-Portal NeSSI
  - DFN-CERT-/CERT-Bund-Meldungen

Verwaltung gesperrter IP-Adressen (“SperrAPI”)

1. Self-Service für Anwender zur Secomat-Entsperrung

1. Verwaltung von Ausnahmelisten-Einträgen nach Meldung durch Netzverantwortliche:
   - Eintrag verhindert automatische Sperre bei Auffälligkeit
   - Netzverantwortliche werden dennoch informiert (!)
   - Gültigkeit von Einträgen:
     - Maximal 1 Jahr
     - Erinnerung an Verlängerung zwei Wochen / 48h vor Ablauf

2. LRZ-interne Web-Service-Schnittstellen und Web-Frontend erleichtern Arbeit des Abuse Response Teams

SperrAPI: Beispiele für E-Mails

From: **MWN/LRZ Abuse Response Team** abuse@lrz.de
Subject: [AUSNAHMELISTE] Vermutlich Ponmocup-infiziertes Sys 52.248.119
Date: 3 March 2016 at 17:02
To: ar-team@lrz.de
C de

Sehr geehrte Netzverantwortliche,

beim Security-Monitoring am X-WiN-Zugang ist aufgefallen, dass der in Ihrem Verantwortungsbereich liegende Rechner

IP-Adresse: 10.
FQDN: 001 enchen.de

Standort:
W4
TUM, Geb. 5500 (Bau ~5504), Maschinenwesen

Switchport:
MAC: 00:1 3:21
Device : SWG1-0W
Location: Bau 4 4-UV-EG
P
First seen: 2016-02-29 13:08:27.0
Last seen: 2016-03-03 16:50:18.0

Weitere Informationen:

Source-Port: 115
Destination-IP: 192
Destination-Port: 80

Timestamp: 03.03.2016 17:01:00

aufgrund charakteristischer Auffälligkeiten im Kommunikationsverhalten mit sehr hoher Wahrscheinlichkeit mit dem
Ponmocup-Virus infiziert ist.

Ponmocup ist in der Lage nahezu beliebigen Schadcode auf das System nachzuladen. Außerdem können Dateien auf dem System
gelöscht oder sensible Daten über das Internet verbreitet werden. Desweitern werden meist Sicherheits-relevante
Dienste beendet, wodurch der vermutete Schutz eines Systems ausgehebelt wird.

Mit freundlichen Grüßen
--

MWN/LRZ Abuse Response Team	
E-Mail: abuse@lrz.de	Leibniz-Rechenzentrum
Phone: +49 89 35831 8800	Boltzmannstraße 1
Fax: +49 89 35831 9700	D-85748 Garching, Germany

*** Diese E-Mail wurde automatisch erzeugt und an Sie verschickt ***

From: abuse@lrz.de
Subject: [SperrDB] Ausnahme endet in weniger als 2 Wochen: 141.84.69.2
Date: 7 March 2016 at 07:55
To: ar-team@lrz.de, edv@s

Sehr geehrte Damen und Herren,

wir führen eine Ausnahmeliste für IP-Adressen, die im Rahmen unseres Sicherheits-Monitorings auf keinen Fall automatisch gesperrt werden sollen.

In der Regel handelt es sich dabei um Gateways (z.B. NAT oder Firewall), die den Internet-Zugang für mehrere dahinter liegende Rechner realisieren, oder Server, die einen besonders wichtigen Dienst erbringen. Die Einträge in der Ausnahmeliste haben eine Laufzeit von einem Jahr und müssen danach verlängert werden. Bei dieser Gelegenheit wird die Aktualität der Einträge überprüft:

IP/Netz: 141.84.69.2
Gültig bis: 2016-03-20 19:50:02
Kontakt: edv@s
Kommentar: DNS-Server und Resolver, S

Um den Ausnahmelisteneintrag für diese IP-Adresse zu verlängern bzw. zu löschen, beantworten Sie bitte diese E-Mail. Sie können uns bei der Gelegenheit auch Änderungen der Kontaktdaten oder des Rechnerzwecks mitteilen.

Mit freundlichen Grüßen

- --

MWN/LRZ Abuse Response Team	
E-Mail: abuse@lrz.de	Leibniz-Rechenzentrum
Phone: +49 89 35831 8800	Boltzmannstraße 1
Fax: +49 89 35831 9700	D-85748 Garching, Germany

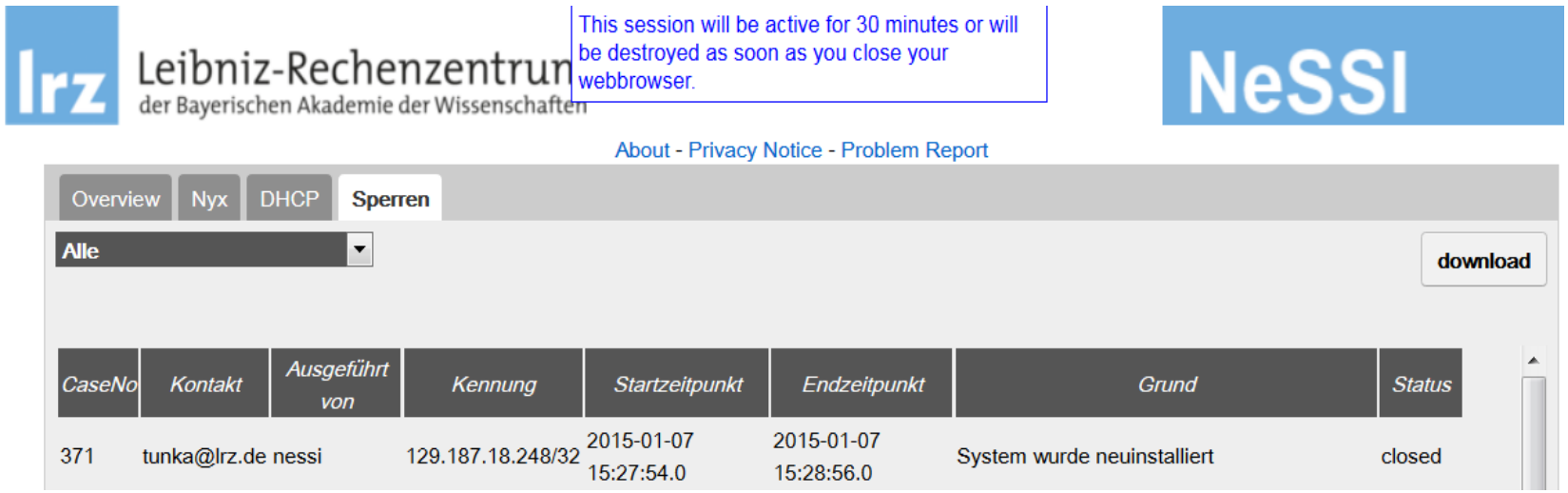
Subject enthält “[AUSNAHMELISTE]”: Reine Information, keine Sperre erfolgt!

Agenda

- MWN PC
- Aufgaben eines NV
- Neues im MWN
- Dienste im MWN
- Sicherheitsmonitoring
  - Security Information & Event Management (SIEM)
  - Verwaltung gesperrter IP-Adressen
  - Self-Service-Web-Portal NeSSI
  - DFN-CERT-/CERT-Bund-Meldungen

NeSSI – Netzverantwortlichen-Self-Service-Interface

- Web-Frontend u.a. zur Abfrage von
  - MAC-Adress-zu-Switchport-Zuordnung
  - per LRZ-DHCP zugewiesenen IP-Adressen
- Netzverantwortliche können jetzt auch gesperrte Rechner selbst entsperren
- Integration der SperrAPI-Ausnahmeverwaltung in Arbeit



DFN-CERT-/CERT-Bund-Meldungen

- Aktuelle Schwerpunkte:
  - Ungeschützte Datenbank-Server (MongoDB, Redis, …), Netzwerkdrucker etc.
  - “Offene”, für Amplification Attacks anfällige Server (DNS, NTP, SNMP, …)
  - Bluekeep (RDP Port in älteren Windows Versionen)
- LRZ Abuse-Response-Team gibt Meldungen zeitnah an Netzverantwortliche weiter
- Bitte Umkonfiguration der betroffenen Systeme oder Maßnahmen wie virtuelle Firewalls in Erwägung ziehen!


Fragen ?