IT-Sicherheit

- Sicherheit vernetzter Systeme -

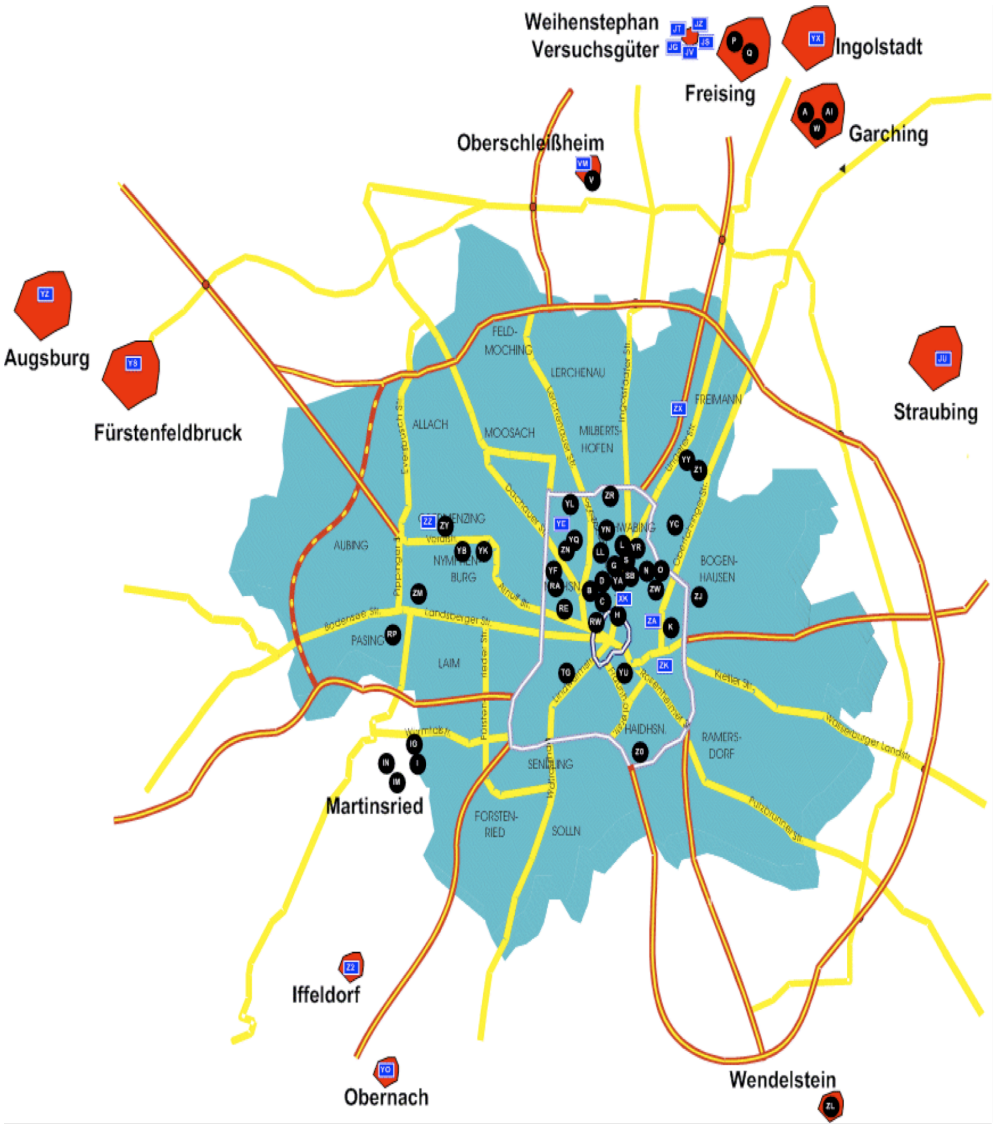
Kapitel 16: Beispiele aus der Praxis des LRZ

Inhalt

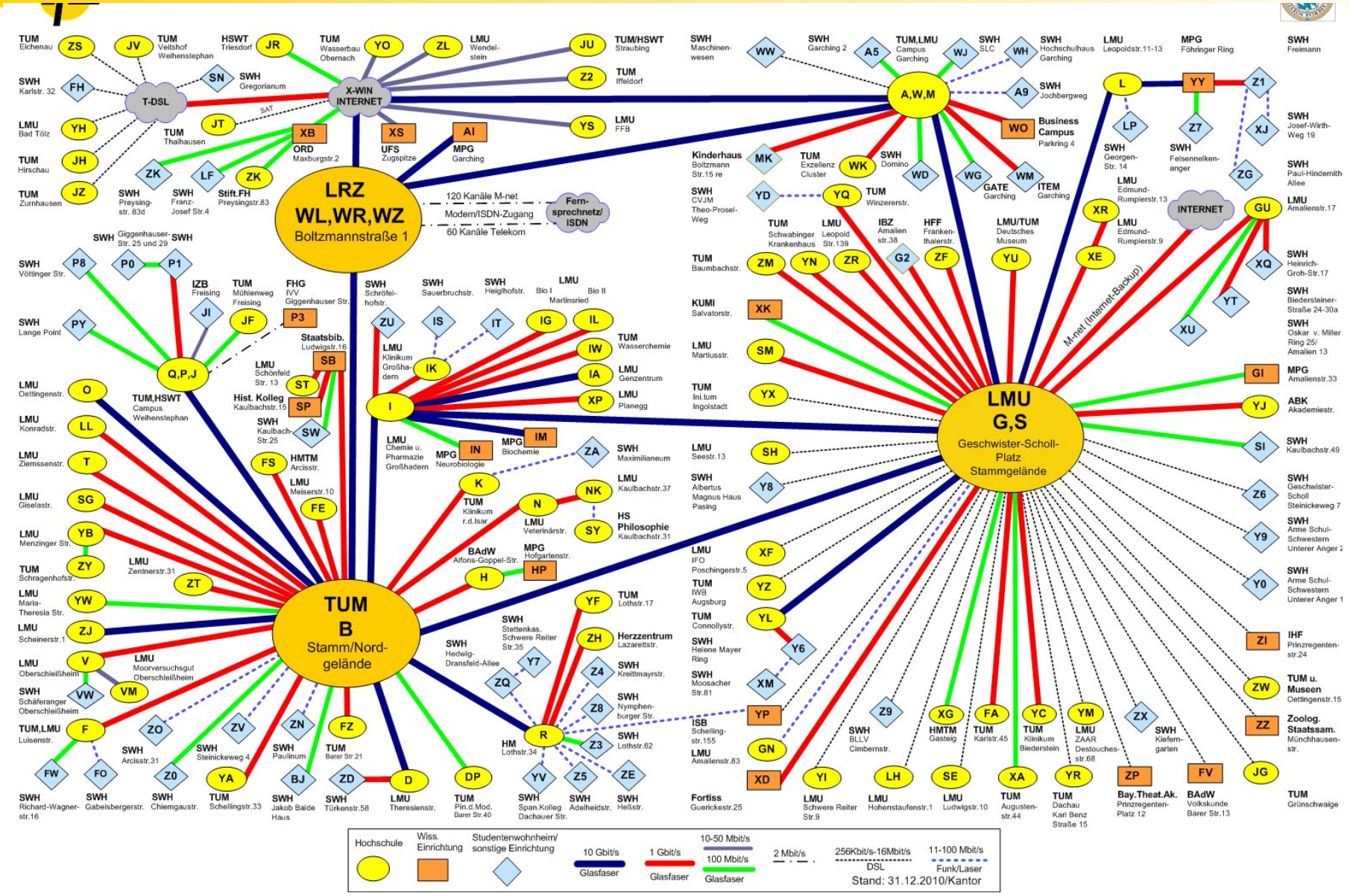
1. Struktur des Münchner Wissenschaftsnetzes (MWN)
2. Virtuelle Firewalls im MWN
3. NAT-o-MAT: generisches IDS
4. Nyx: Lokalisierung im MWN

Münchner Wissenschaftsnetz (MWN)

- Netz für alle Münchner Hochschulen und Forschungseinrichtungen
- Hohe Datenraten
  - 434 / 1.100 TByte Internet Daten / Monat (Stand Dez. 08 / Okt. 11)
    - 222 / 700 TB eingehend
    - 212 / 400 TB ausgehend
  - 2,97 / 12,2 PByte Daten im MWN / Monat (Stand Dez. 08 / Okt. 11)
  - Kernnetz mit 10 Gbit/s
- Starke räumliche Verteilung
  - 60 Standorte
  - > 500 Gebäudegruppen
- Große Nutzerzahl
  - > 100.000 potentielle Nutzer
  - > 80.000 angeschlossene Rechner
- Private und öffentliche IP-Adressen



MWN-Struktur



MWN: Randbedingungen

- LRZ zuständig für den Betrieb des MWN
- KEINE administrative Kontrolle über angeschlossene Endsysteme
  - Systeme werden von LFEs oder Instituten betrieben
  - Keine Einflussmöglichkeit auf eingesetzte/einzusetzende Systeme
  - Keine normative Kontrolle bzgl. eingesetzter Software
- Private IP-Adressen
  - werden verwendet
  - MWN-internes Routing privater Adressen
  - Systeme von extern nicht erreichbar
  - Network Address Translation (NAT)

Nat-O-Mat

- Randbedingungen für Sicherheitsanalyse u. -konzepte im MWN
  - Keine administrative Kontrolle über angeschlossene Systeme
  - Betrieb mobiler Systemen im MWN und in fremden Netzen
  - Infizierte Systeme können nicht völlig ausgeschlossen werden (Grundrauschen)
- Nat-O-Mat:
  - NAT-Gateway für Netze mit privaten IP-Adressen
  - Generisches Intrusion Prevention System
  - Dynamische Bandbreitenbeschränkung
- ➡ Ziele bei der Entwicklung
  - Reduktion der manuellen Administration
  - Automatisierung soweit wie möglich
  - Einfache Festlegung von Policies
  - Abschaffung der verschiedenen Proxies
  - Keine speziellen Clients erforderlich
  - Keine Vorkenntnisse bei den Benutzern

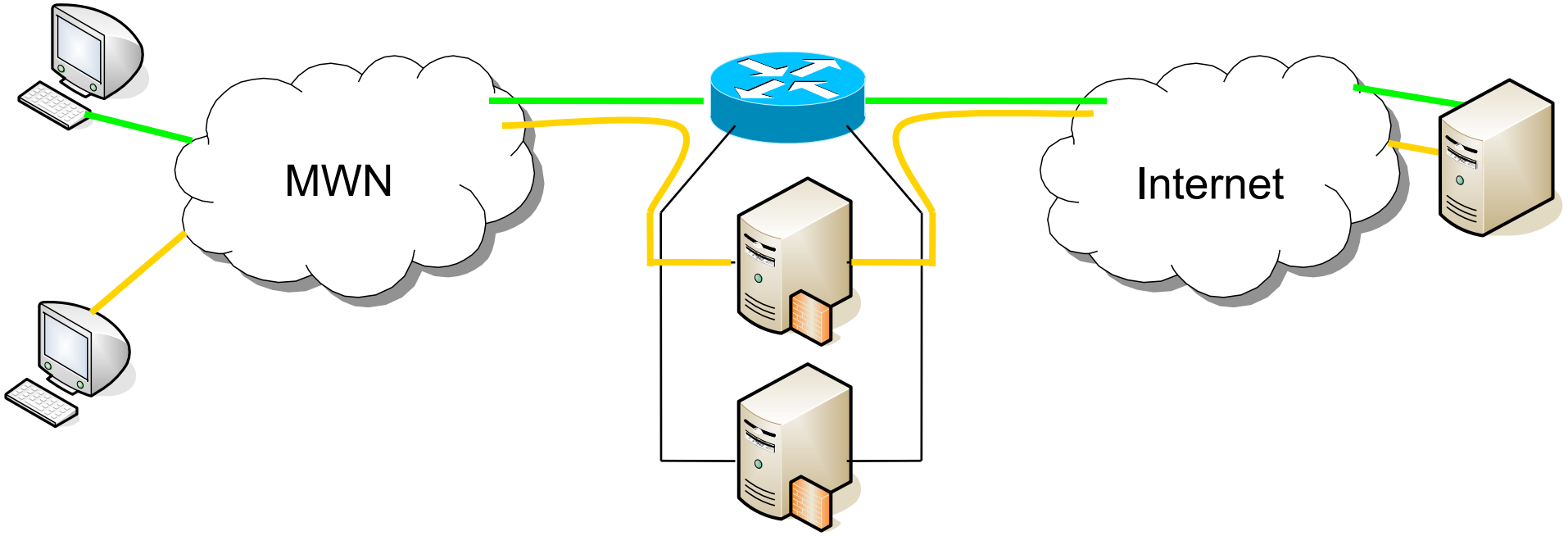
Nat-O-Mat: Idee

- Erkennung von Auffälligkeiten durch
  - Analyse des Kommunikationsverhaltens (z.B. Paketraten)
  - Zahl der Kommunikationspartner
- Minimierung der „teuren“ Aktionen
  - „Deep Packet Inspection“, d.h. vollständige Protokollanalyse
  - Nur für Pakete, die nicht eindeutig als „gut“ bzw. „böse“ klassifizierbar
- Begrenzung der “False Positive”-Rate
  - durch sanfte Sperrungen (sog. Softlimits),
  - Begrenzung der erlaubten Paketrate / Bandbreite
  - Vollständige Sperrung nur im Fall einer Eskalation

Nat-O-Mat: Komponenten

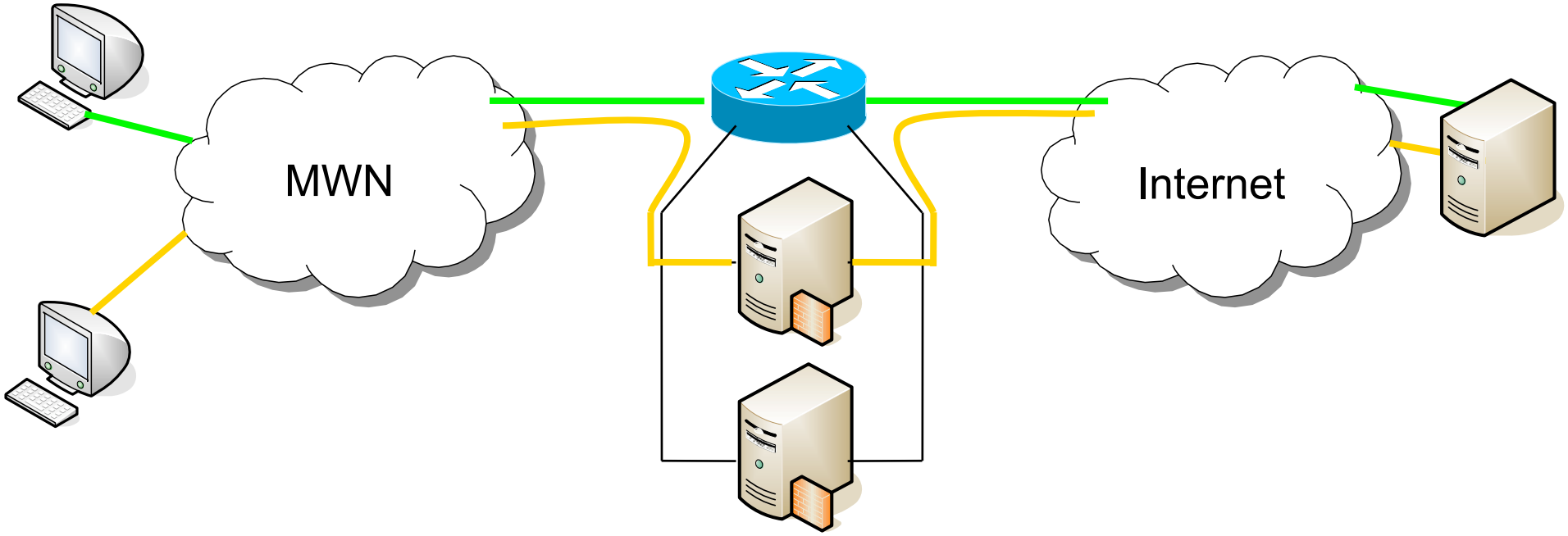
- Router
- Stateful Firewall
- NAT-Gateway
- Intrusion Detection & Prevention System (IDS/IPS)
- Status & Incident Reporting
- User Information
- Lösung für Hochverfügbarkeit und Skalierbarkeit

Einbindung ins Netz



- NAT-o-MAT ist selbständiger Router
- Umleitung ausgewählter Pakete per Policy-based Routing zum NAT-o-MAT

Einbindung ins Netz



- Verkehr wird analysiert, parametrisiert und ggf. gefiltert
- Erlaubter Verkehr wird über WAN-Router weitergeleitet

Verkehrsanalyse

- Verhalten von Hosts im Netzwerk klassifizierbar durch
  - Rate erfolgloser Verbindungsaufbauversuche
  - Anzahl aktiver Kommunikationspartner
  - Paketrate und Bandbreite
  - Typische Ports
  - Typische Signaturen
- Problemstellung:
  - Welche Kombination obiger Parameter liefert griffige Anhaltspunkte?
  - Wo liegen die Grenzwerte?
- Festlegung der Grenzen anhand empirischer Daten

Analyseklassen

1. Anzahl der Kommunikationsverhältnisse
   - z.B. Anzahl von IP-/UDP-/TCP-Flows
   - Unterscheidung bestätigt / unbestätigt
2. Paketraten und Bandbreiten
   - z.B. pro Quell-IP-Adresse oder pro Verbindung,
   - Traffic-Shaping für P2P-Protokolle
3. Signaturen
   - Art und Verwendung von diversen Protokollen (z.B. P2P)
   - zur Erkennung von Viren, Bot-Netzen

Analyse des Verkehrsverhaltens; Beispiel

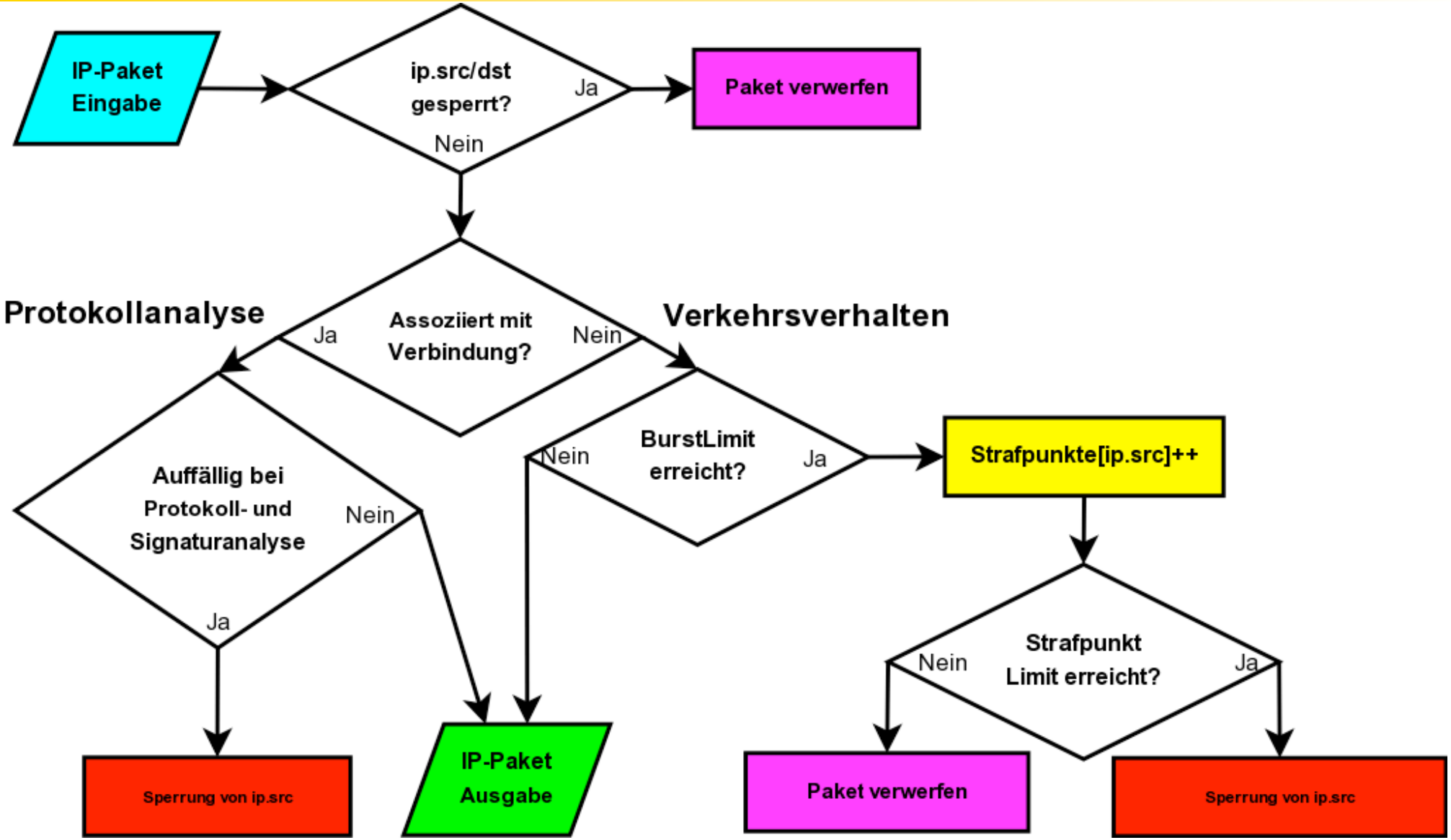
- IP-Pakete; keinem bestehenden Flow zuzuordnen:
  - Pakete mit hoher Rate von einem Host an viele Hosts
    ⇨ **(mgl.) Denial of Service (DoS) / Netscan**
  - Pakete von vielen Quellen zu einem Ziel-Host
    ⇨ **(mgl.) Distributed Denial of Service (DDoS) / Portscan**

- IP-Pakete; aus bestehendem Flow: (Protokoll und Signaturanalyse)
  - Typischen Signaturen von Würmern und Viren
  - Shell-Code
  - Bot-Netz Kommunikation
  - P2P-Protokollen

Policy Enforcement (PE); Grundlagen

- Strafpunkte pro IP-Adresse
  - bezieht sich auf die Verstöße eines gleitenden Zeitfensters (z.B. die letzten 15 Minuten)
  - Limits für Sperrung, Freischaltung, Benachrichtigung
- Automatische Sperrung und Freischaltung
  - basierend auf Strafpunktekonto mit gleitendem Zeitfenster
  - transparentes Verfahren für den Benutzer
  - Keine manuelle Intervention notwendig
- Traffic Shaping für P2P Protokolle

Policy Enforcement; Ablaufdiagramm



PE: 4-stufiges Eskalationsprinzip

1. Bei kurzzeitigen Überschreitungen: 30 Versuche/s
   - Keine Einschränkung unterhalb der “Burst-Bedingung”
2. Bei Überschreitung der “Burst-Bedingung”: 31. Versuch
   - **Soft-Limit:** Blockierung der verursachenden IP-Pakete
   - Erhöhen der Strafpunkte 1 Punkt je 10 Versuche/s
3. Bei Erreichen des Strafpunkt-Limits: 120 Punkte
   - **Hard-Limit:** Sperrung der verursachenden IP-Adresse
   - Erzeugung einer benutzerbezogenen Hinweisseite
4. Bei anhaltendem Verstoß und hoher Strafpunktzahl: > 1000 Punkte
   - Email-Benachrichtigung an eine verantwortliche Person mit vollständigem IDS-Report (an interne Verursacher)

❑ **Beispiel**
Portscan: eine Absender-IP auf einen Ziel-Port (auf mehreren Ziel-Systemen)

Automatischer Warnhinweis

No Internet

Lieber Nutzer,

Ihr Rechner wurde aufgrund exzessiver Überschreitung der erlaubten Paketrate **automatisch an der Nutzung des Internets gehindert**. Sehr wahrscheinlich ist Ihr Computer von einem **Wurm oder Virus befallen**! Auch P2P-Software (zum Filesharing, wie z.B. Gnutella, Kazaa, BitTorrent) kann in ungünstigen Fällen zu dieser Meldung führen.

Um wieder Zugriff auf die Internetdienste zu erhalten, beenden Sie eventuell laufende P2P-Software und versichern Sie sich bitte, dass Sie einen aktuellen Virenscanner auf Ihrem System installiert haben.

Weitere Informationen erhalten Sie unter: http://www.lrz-muenchen.de/services/security/antivirus/ und http://www.lrz-muenchen.de/services/netzdienste/nat-o-mat/

Dear User,

your computer has been **suspended from internet access** due to exceeding our packet rate limits. Most likely your computer is **infected by a worm or virus**! This message might also be caused by some P2P software used for file sharing like Gnutella, Kazaa, BitTorrent.

To regain internet access please disable any P2P software and make sure you have installed an up to date virus scanner. Further information can be found on: http://www.lrz-muenchen.de/services/security/antivirus/ and http://www.lrz-muenchen.de/services/netzdienste/nat-o-mat/

Status Report for 129.187.47.34 (gesperrt/blocked)

Überschreitungen Number of hits	Protokoll Protocol	Zielport und Grund der Sperrung Destination port and suspension reason
105	ICMP	Zu viele Pings
63	TCP	25 SMTP, Versenden von zu vielen Spam- oder Virenmails
33	TCP	6600-6699 WinM / Napster Filesharing
21	TCP	53 DNS, Zu viele DNS Anfragen

Die Sperrung wird aufgehoben, sobald die Summe aller Überschreitungen unter 120 fällt. Technisch bedingt kann die automatische Freischaltung bis zu 15min dauern.

Internet access will be granted again if the total of all hit numbers falls below 120. Due to technical reasons re-enabling your access can take up to 15min.

powered by lrz

PE: Traffic Shaping

- Bandbreiten- und Paketratenbegrenzung für P2P-Protokolle (z.B. Filesharing via Kazaa oder Bittorrent)
- Verschiedene Bandbreitenklassen möglich:
  - Pro Protokoll
  - Pro Verbindung
  - Pro Adresse
  - Pro Subnetz
- Z.Zt. realisiert: Gemeinsame Bandbreitenklassen für alle Nutzer:
  - 2Mbit/s für BitTorrent
  - 1Mbit/s für alle anderen P2P-Protokolle

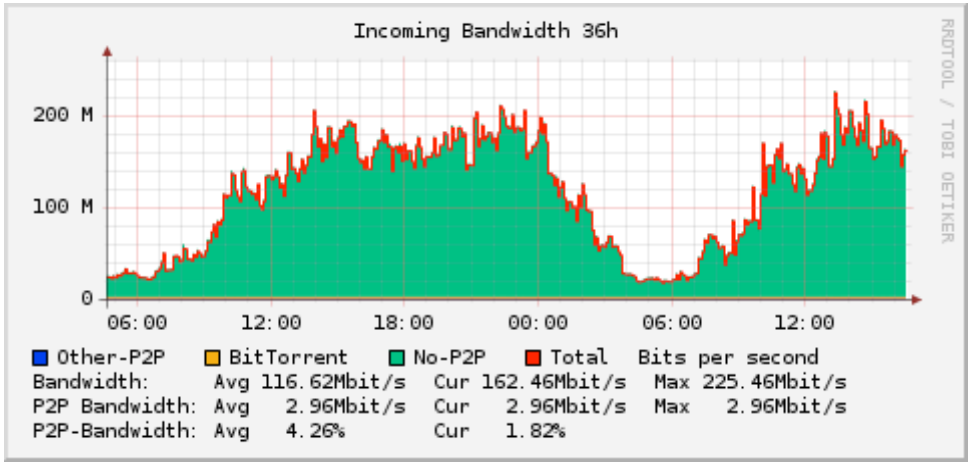
Load Balancing & High Availability

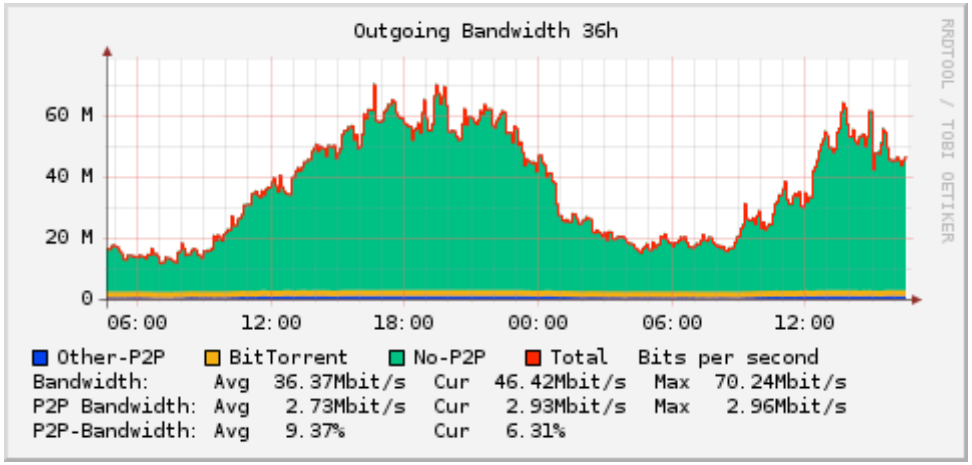
- Betrieb als Cluster aus gleichberechtigten Nodes
- Zuordnung von Subnetzen zu einem Node
- Jeder Node kann Funktion eines anderen übernehmen.
- Selbsttests und gegenseitige Prüfungen zur Sicherstellung der Funktionalität

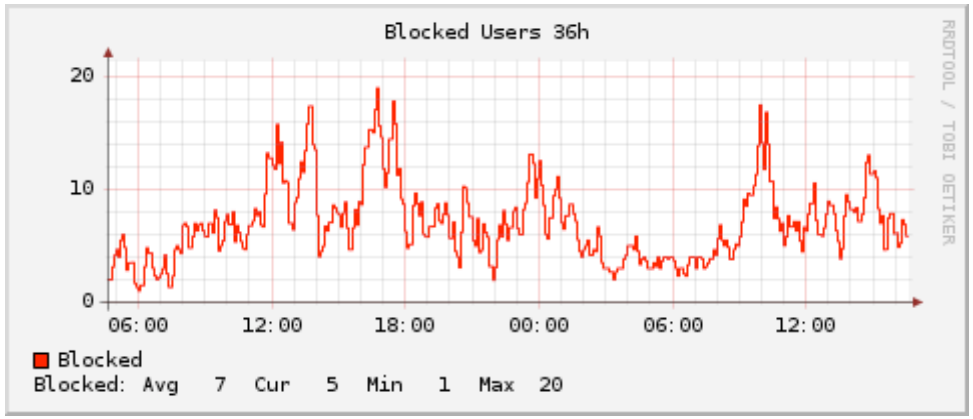
Management-Interface

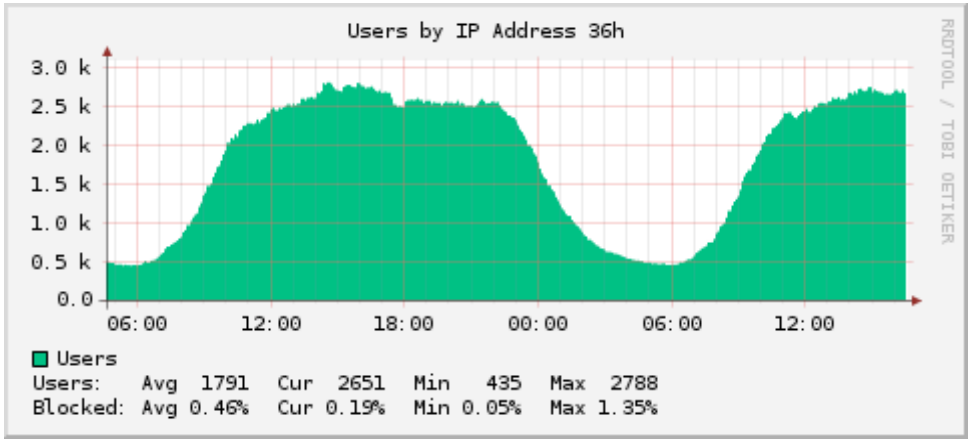
- Analyse des laufenden Verkehrs:
  - Top-Listen aller auffälligen Rechner
  - Suchfunktionen
- Reporting:
  - Verteilung von Bandbreiten
  - Anzahl aktiver Verbindungen
  - Anzahl IP-Adressen.
- Detaillierte Benutzerinformation bei Verstoß

Management-Interface: Bandbreiten









Praktikum IT-Sicherheit

1. Grundlagen von TCP/IP-Netzwerken
2. Gefährdungspotentiale, Hacking und Schutzmaßnahmen
3. Paketfilter-Firewall (Linux Netfilter)
4. Verschlüsselung und VPNs (IPSEC, OpenVPN)
5. Sicherheit von Diensten
   - DNS
   - Mail
   - FTP
   - WWW (Apache)
   - SSH (OpenSSH)
6. Application Level Gateways (Squid)
7. Circuit Level Gateways (SOCKS)
8. Intrusion Detection (Snort)

ISO 27001 Personenzertifizierung ?

- Seminar zur Vorbereitung auf die ISO/IEC 27001 Foundation Zertfizierung
- Offizielle Prüfung durch den TÜV (mit Kosten verbunden)
- Evtl. als Kompaktseminar

- Interesse?

- Thema des Kompaktseminars:

IT Service Management

3 ECTS
"IT-Kompetenz"
LMU Informatik (Bachelor)

Theorie

- Fehlermanagement und Entstörung
- Change und Release Management
- Konfigurationsmanagement
- Capacity Management
- Management der Informationssicherheit
- …

Simulation

Managen Sie im Planspiel die IT-Systeme und Dienste eines Flughafens!

- Termin: 10. bis 13. April 2012 (letzte Ferienwoche)
  - Teilnahme an ISO/IEC 20000-Zertifizierungsprüfung (am letzten Tag) möglich
  - Begrenzte Teilnehmerzahl, Anmeldung jetzt möglich
- Webseite:

www.nm.ifi.lmu.de/itsm

TÜV SÜD Akademie

Wie geht's weiter?

- Lehrveranstaltungen an unserer LFE:
  - Grid / Grid II
  - Rechnernetze
  - Verteilte Systeme
- Praktika
  - Grid-Praktikum
  - Rechnerbetriebspraktikum
  - IT-Sicherheit
- Seminare:
  - Prozessorientiertes IT-Service Management anhand von Unternehmensbeispielen
- FoPra / SEP
- Diplomarbeit
- Bachelor / Masterarbeiten

Studentische Arbeiten, Beispiele

- Fopra / Bachelor Arbeiten
  - Erkennung von Innentätern
  - Effizientes Management von Router-ACLs (Packet-Level-Firewall)
  - Evaluation aktueller Security Information und Event Management (SIEM) Lösungen
  - *Erweiterung der „Eduraom-App“ für IOS (iPhone, iPad)*
- Diplomarbeit / Master-Arbeit
  - Sicherheitskonzept für IPv4/IPv6 Dual-Stack Netze