IT-Sicherheit

- Sicherheit vernetzter Systeme -

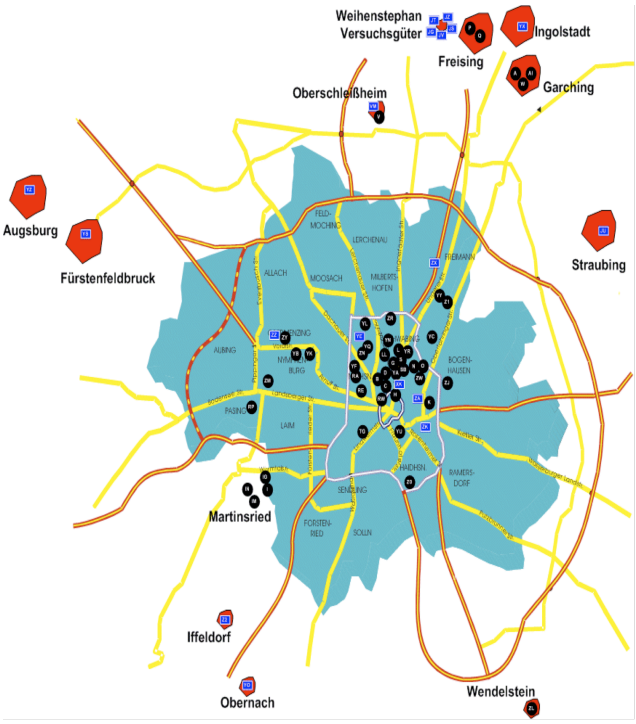
Kapitel 16: Beispiele aus der Praxis des LRZ

Inhalt

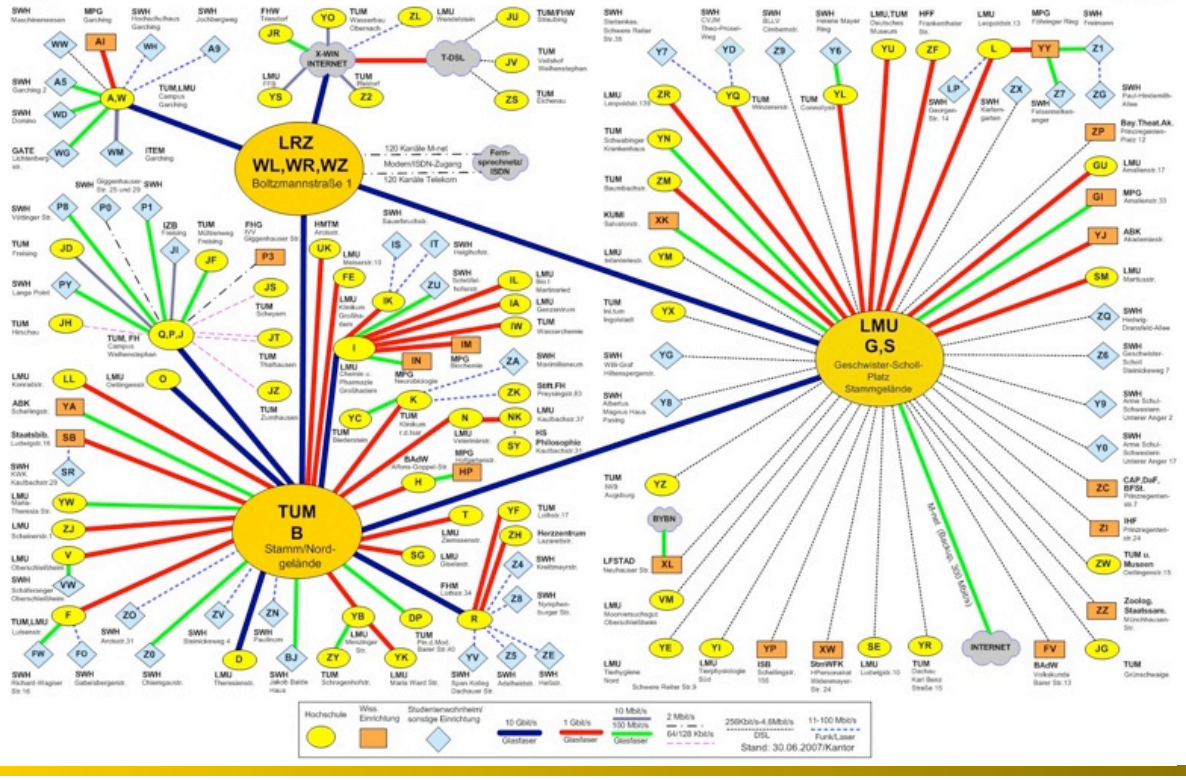
1. Struktur des Münchner Wissenschaftsnetz (MWN)
2. Virtuelle Firewalls im MWN
3. NAT-o-MAT: generisches IDS
4. NYX: Lokalisation im MWN

Münchner Wissenschaftsnetz (MWN)

- Netz für alle Münchner Universitäten und Forschungseinrichtungen
- Hohe Datenraten
  - 220 / 434 TByte Internet Daten / Monat (Stand Dez. 07 / Dez. 08)
    - 130 / 222 TB Eingehgend
    - 90 / 212 TB ausgehend
  - 1,97 / 2,97 PByte Daten im MWN / Monat (Stand Dez. 07 / Dez. 08)
  - Kernnetz mit 10 Gbit/s
- Starke räumliche Verteilung
  - 60 Standorte
  - 440 Gebäude
- Große Nutzerzahl
  - 100.000 potentielle Nutzer
  - Ca. 68.000 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)

Firewalls im MWN

- Bisher Aufgabe der Lehr- und Forschungseinheit
  - LFe beschafft
  - LFe betreibt FW vor dem Institutsnetz
  - ➡ Kosten und Administrationsaufwand voll bei der LFe
  - ➡ Total Cost of Ownership (TCO) hoch
- Idee: LRZ bietet „Firewall-Dienst“ für Institute des MWN
  - \+ dadurch Senkung der TCO bei der LFe
  - \- Betrieb dedizierter Appliances beim Institutsnetz nicht umsetzbar
  - zentrale Lösung
  - (logisch) dezentral einsetzbar

➡ virtuelle Firewall als Dienst

Virtuelle Firewalls im MWN

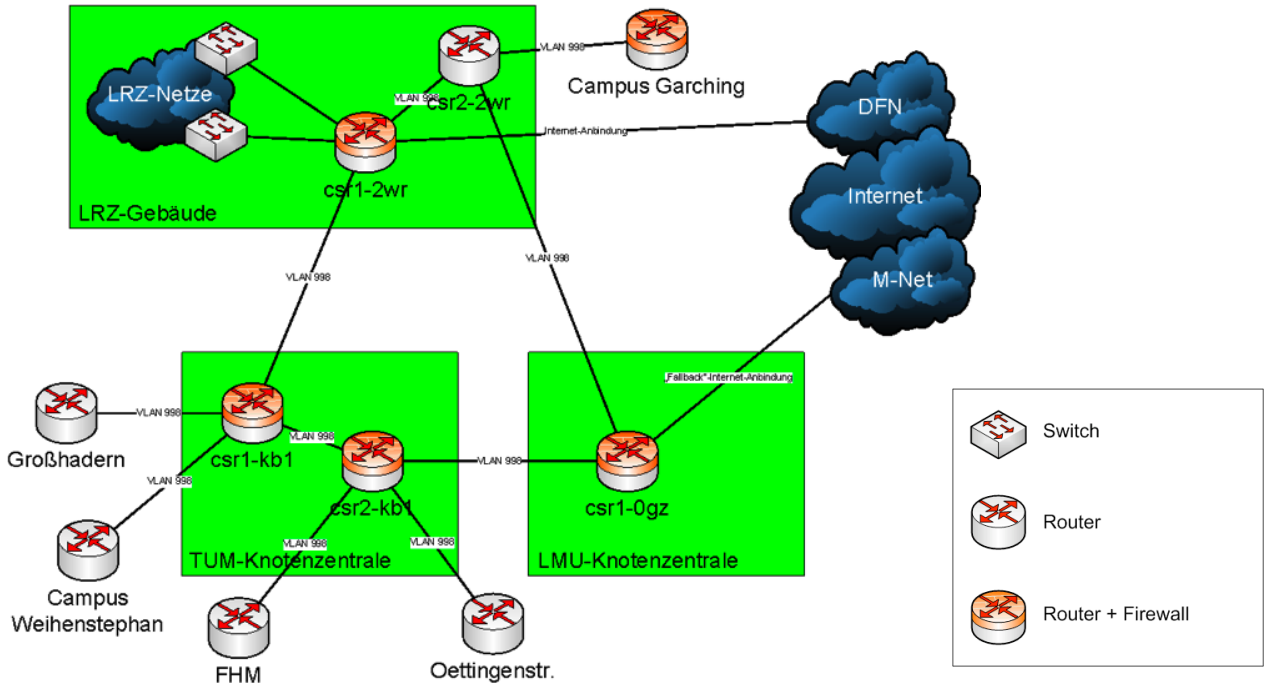
- Firewall-Blade: Einschübe in Kern-Router
  - Technisch äquivalent zu Cisco PIX
  - Mandantenfähig, d.h. logisch **„eigene“ Firewall** pro Kunde
- Filter
  - Paketfilter: Stateful
  - Applikation: HTTP, SIP, …
- LRZ stellt Grundkonfiguration bereit
- Anpassung durch den Kunden
- LRZ-Service (Kosten übernimmt LRZ)
  - Anschaffung
  - Installation
  - Wartung
- Total Cost of Ownership (TCO) für den Kunden
  - Betrieb
  - Überwachung

Virtuelle Firewall: Die Hardware

- Firewall-Blade (Zusatzmodul für Cisco-Router)
- Leistungsmerkmale pro Modul
  - Gesamte Bandbreite: ca. 6 Gbit/s
  - Anzahl virtueller Firewalls: maximal 250
  - Filterregeln: ca. 11.000

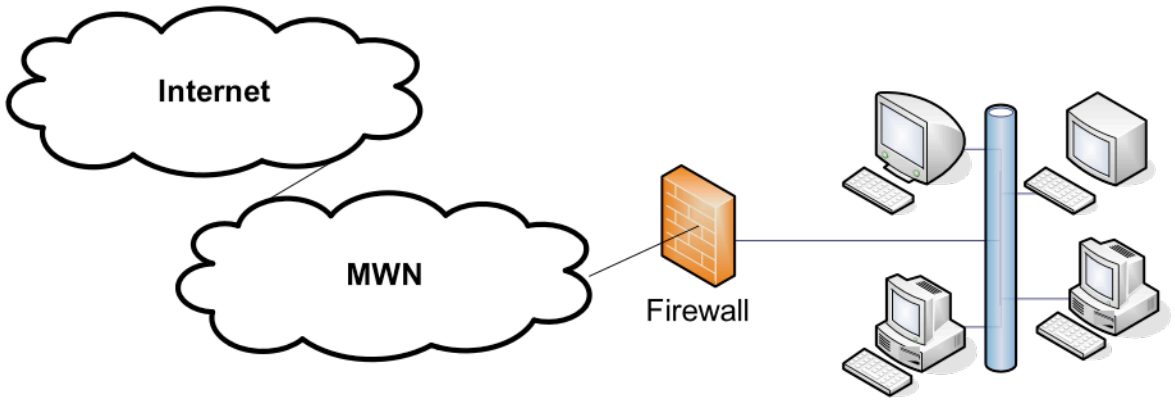
- Aktuelles System
  - 5 + 1 Module
  - 20 virtuelle Firewalls pro Modul (Lizenzierung)
- Ausfallsicherheit
  - „Cold Standby“: Im Schadensfall Austausch des defekten Modules mit Reserve-Modul
  - Perspektive: High Availability durch redundante Module pro Router

Integration der virtuellen FW im MWN



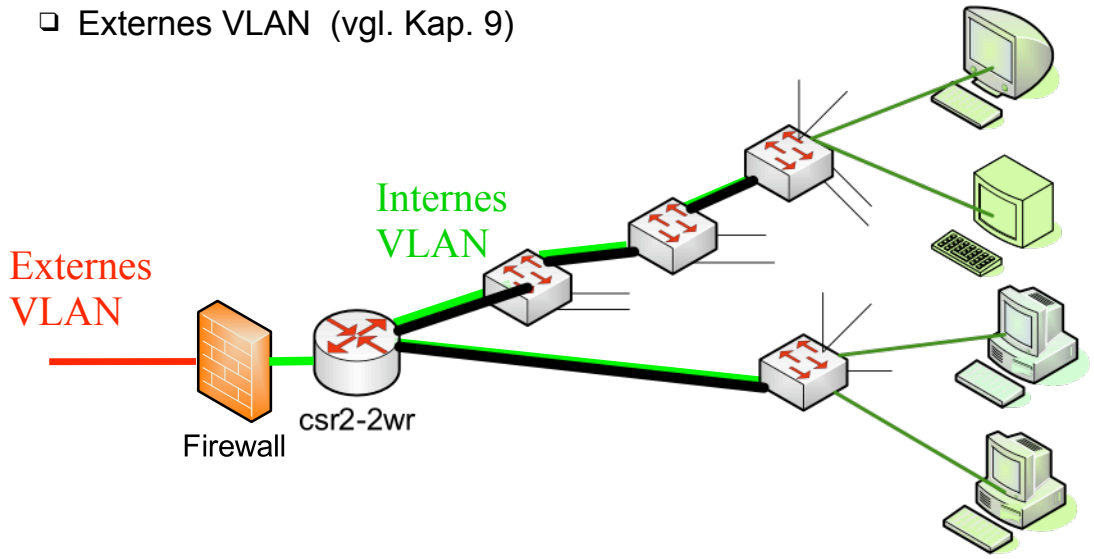
Integration der virt. FW b. Kunden: logische Sicht

- Platzierung der Firewall unmittelbar „vor“ dem Kundennetz



virtuelle FW beim Kunden: technische Sicht

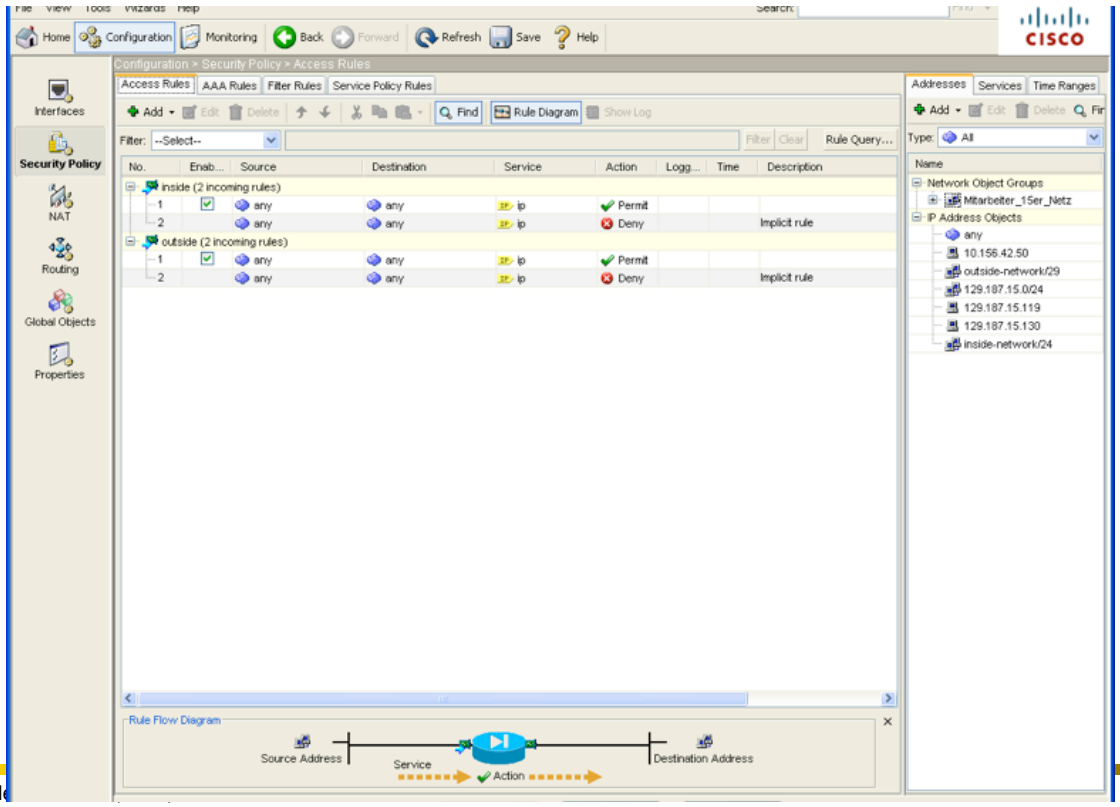
- „Platzierung“ der virtuellen Firewall vor Institutsnetz durch
  - Internes und
  - Externes VLAN (vgl. Kap. 9)



Administration

- Kunden-Interface:
  - Administration:
    - GUI (Java basiert)
    - Command Line Interface (CLI) ; über ssh verfügbar
    - Befehlssatz: Cisco PIX
  - Überwachung:
    - Logging über GUI zugänglich
    - Weiterleitung von Events auf syslog-Server
- Adminstration durch LRZ
  - Rechtevergabe an FW-Ressourcen
  - Installation der FW-Instanz
  - Initiale Konfiguration
  - Sicherung der Konfigurationen
  - Rückkehr in Initialzustand oder definierten Zustand nach fehlerhafter Konfiguration durch den Kunden

Nutzerinterface: Konfiguration



Nutzerinterface: Überwachung

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
  - Generische 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

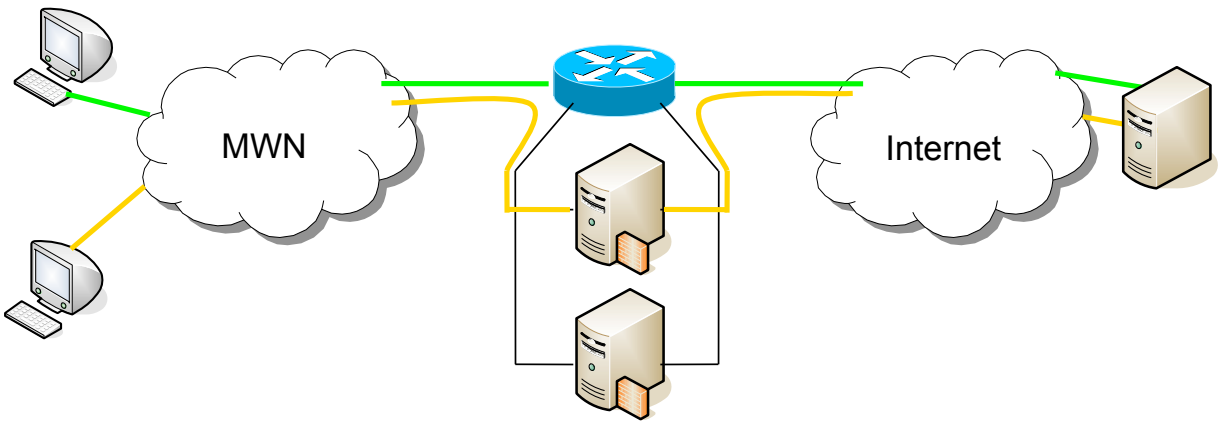
Nat-O-Mat: Idee

- 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 Packete 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

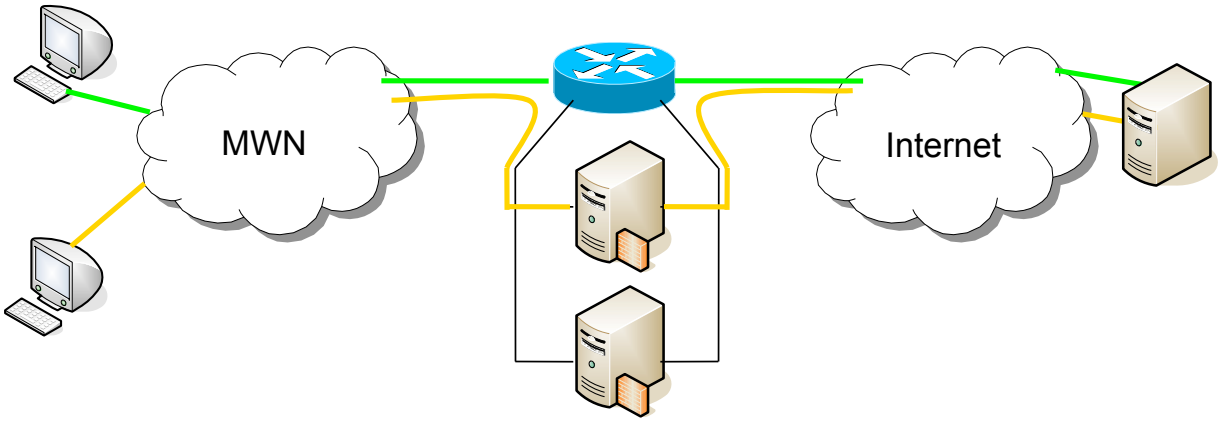
- Router
- Stateful Firewall
- NAT-Gateway
- Intrusion Detection & Prevention System (IDS/IPS)
- P2P-Traffic Shaper
- Status & Incident Reporting
- User Information
- Lösung für Hochverfügbarkeit und Skalierbarkeit

Einbindung ins Netz



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

Einbindung ins Netz



NAT-o-MAT

- Verkehr wird analysiert, parametriesiert 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

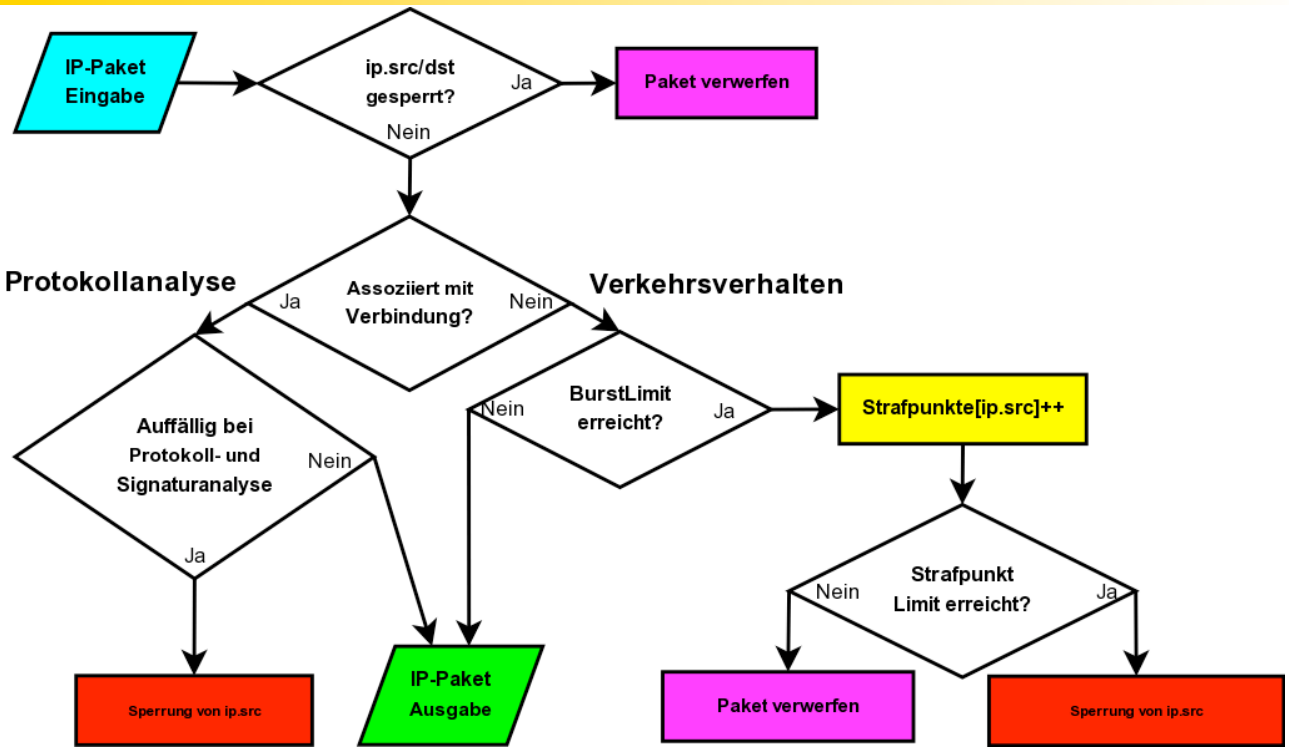
Analyse des Verkehrsverhaltens; Beispiel

- 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
   - Inkrement 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**
Port-Scan: 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: All Blocked Hosts

NAT-O-MAT

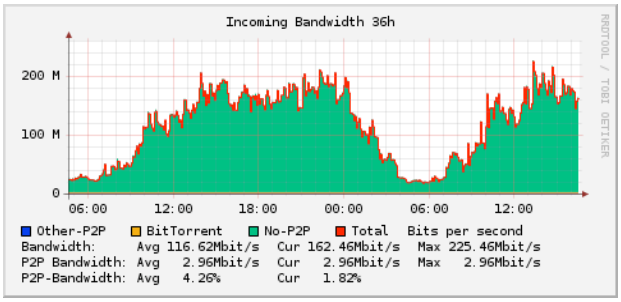
- All Blocked Hosts
- Top Packet Rates
- Top Blocked Ports
- Top P2P-Users
- Bandwidth Graph
- Top Blocked Hosts

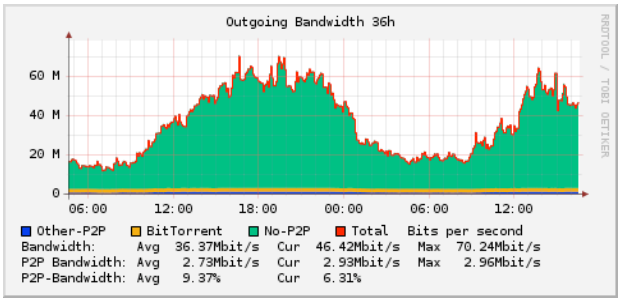
Search Criteria: (e.g. SMTP or ICMP) . Submit Query

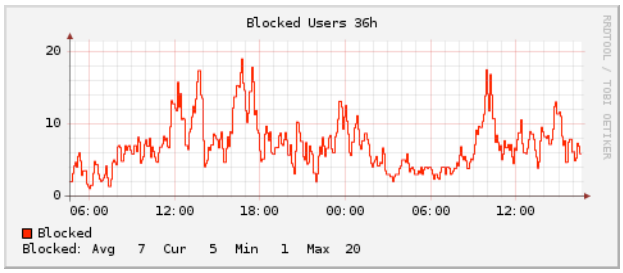
Looking for . (scope 15min, hard limit 120):

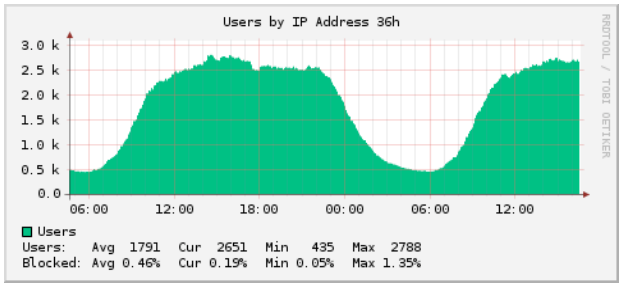
Score	IP-Address	State	Hostname
896	10.150.154.104	blocked (26.10. 16:28)	r154104.olydorf.swh.mhn.de.
866	10.148.131.178	blocked (26.10. 16:26)	r3178.fr4.swh.mhn.de.
435	10.151.1.75	blocked (26.10. 16:18)	jona.jmh.mhn.de.
180	129.187.100.230	blocked (26.10. 16:23)	e230.tum.vpn.lrz-muenchen.de.
112	10.148.216.105		r216105.cgs.swh.mhn.de.
106	10.149.93.122		r093122.fna.swh.mhn.de.
104	10.155.17.130		
104	10.148.72.48		r072048.hh.swh.mhn.de.
88	10.150.166.53		r166053.olydorf.swh.mhn.de.
74	10.148.55.8		r07008.sb1.swh.mhn.de.
62	10.150.151.32		r151032.olydorf.swh.mhn.de.

Management-Interface: Bandbreiten









Realisierung: Software

- **Linux-Distribution:** SuSE 10.0
- **Kernel 2.6.16** mit IPP2P- und L4/L7-Patches
- **Linux-HA:** Redundanz und Ausfallsicherheit
- **IP-Tables:** Realisierung von Firewallregeln
- **IDS-BRO mit ALS:** Protokolle und Signaturen
- **TC:** Verwaltung von HTB-Bandbreitenklassen
- **Perl und Shell Skripte**
  - Einrichtung von IP-Tables und Bandbreitenklassen
  - Analyse von Log-Files
  - Policy Enforcement
  - Realisierung eines Webinterface

NYX: Lokalisierung von Systemen im MWN

Security-Vorfälle und Abuse-Bearbeitung

- IP-Adressen werden dem LRZ als auffällig gemeldet (Abuse)
  - SPAM
  - Urheberrechtsverletzung
  - Angriffe gegenüber fremden Systemen
- IP-Adressen fallen an Monitoring- und Intrusion-Detection-Systemen auf:
  - Rechner sind von Bot-Net-Clients befallen („Trojaner“)
  - Portscans über große Netzbereiche

⇨ Rechner müssen lokalisiert und ggf. „gesäubert“ werden
→ informieren des zuständigen Netzverantwortlichen

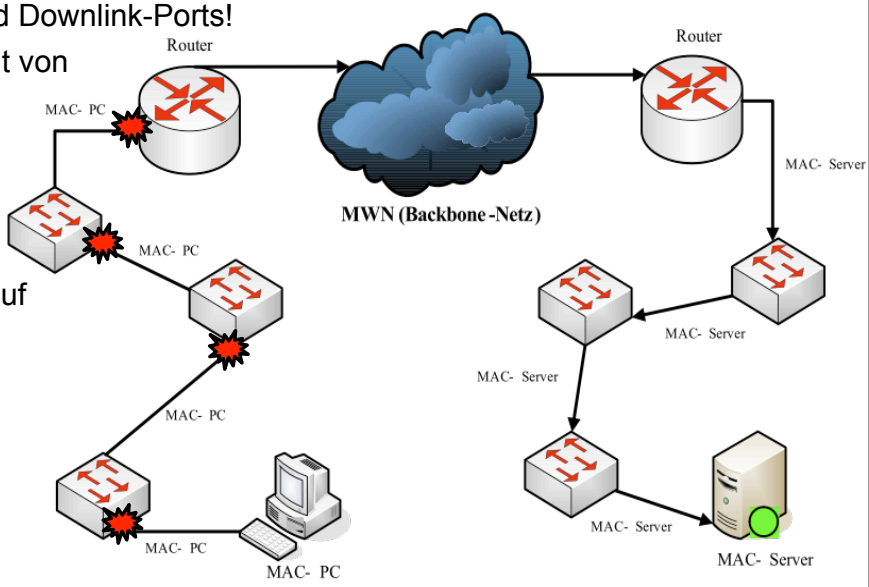
- Lokalisierung: Name des Edge-Switches und Nummer des Anschlussports

Topologieerkennung

- Reine Erkennung von Up- und Downlink-Ports!
- Problem: CDP und LLDP nicht von allen Netzkomponenten unterstützt
- Problem: ohne Filterung Datenflut
  - Beispiel: MAC des PCs taucht 4x auf
- Problem: hohe Komplexität bei großen Netzen
  → Heuristiken nur teilweise wirksam

⇨ Maschinelles Lernen zur Topologieerkennung

- „supervised learning“
- Manuell annotierte Daten zum Lernen („Seed“)



NYX: Reslisierungsidee

- Benutzereingabe: IP-Adresse oder MAC-Adresse
- Nyx-Ausgabe: Edge-Switch und Switch-Port

⇨ Datenmodell:

IP-Adresse ↔ MAC-Adresse ↔ Switch ↔ Switch-Port

- Relationale Datenbank
  - **ARP-Tabelle (Router)**
  - **MAC-Tabelle (Switch)**
- Parallelisierung der Datenakquisition und –verarbeitung:
  - Voll automatisiert
  - Garantie der Echtzeit
  - Skalierbarkeit

Maschinelles Lernen zur Topologieerkennung

Interface ID	#MACs	%Traffic	LLDP ?	Tagged ?	SW/RT MAC ?	Up-/Downlink ? (man. Annotation)
1000007	491	13	Ja	Ja	Nein	Ja
2000017	1	33	Nein	Nein	Nein	Nein
3000023	4	25	Nein	Ja	Nein	Nein
4000046	43	45	Nein	Nein	Ja	Ja
5000008	38	22	Nein	Nein	Nein	Nein*
6000023	20	1	Nein	Ja	Nein	Ja

*: Mini-Switch

- Verkehrsdaten: - Erhebung pro Switch-Port
  - keine festen Kriterien
- Kleiner Ausschnitt der Verkehrsdaten als Seed-Daten:
  - manuelle Annotation nach Realität
- Entscheidungsbaum aufgrund der Seed-Daten, statisches Lernen
- Klassifizieren von Up-/Downlink-Port mit Entscheidungsbaum

Praktikum IT-Sicherheit

1. Grundlagen von TCP/IP Netzwerken
2. Gefährdungspotentiale, Hacking und Schutzmaßnahmen
3. Paketfilter Firewall
4. Verschlüsselung und Virtuelle Private Netze
5. Sicherheit von Diensten in TCP
   - DNS
   - Mail
   - FTP
   - WWW
   - SSH
6. Application Level Gateways
7. Circuit Level Gateways
8. Intrusion Detection