IMPLEMENTIERUNG DES TOR-EXIT-NODES AN DER JKU

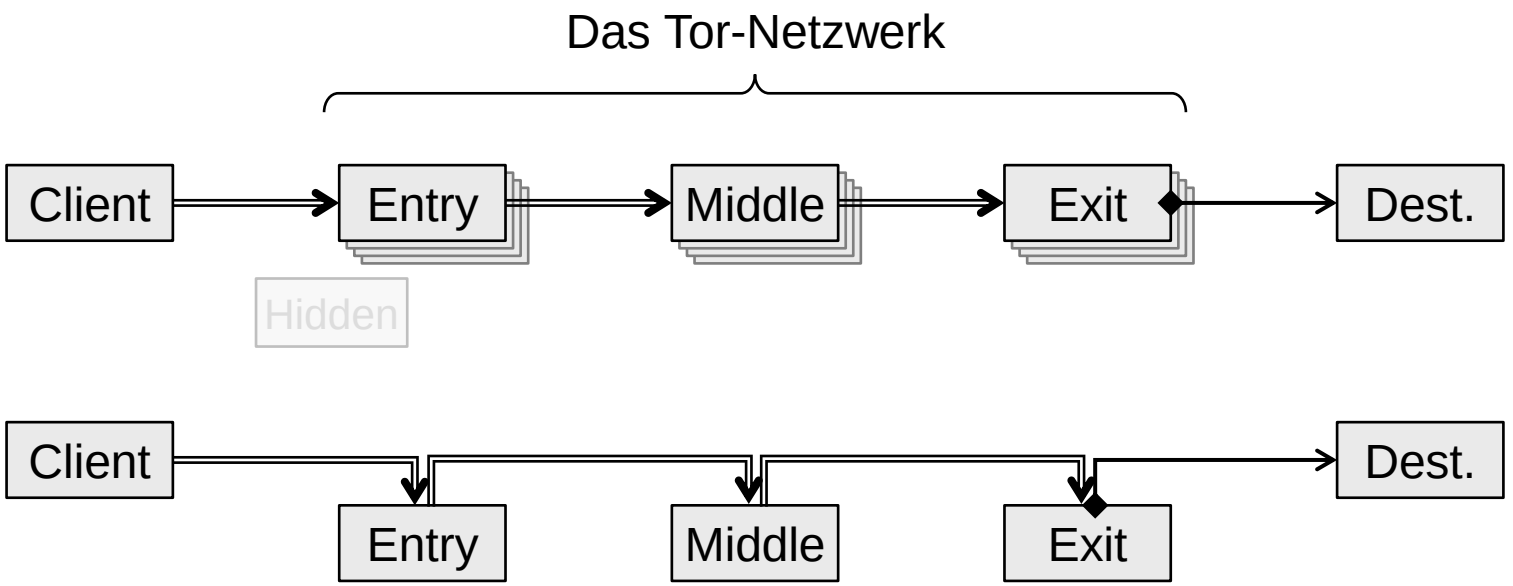
Rudolf Hörmanseder

4.12.2015: Schutz der Privatsphäre im Internet

Konfiguration Überblick: Vom Kern zum Umfeld und zurück

- Rollen / Eigenschaften
- Konfiguration:
  - Bandbreite
  - Relay
- Betrieb Relay
- Relay → Exit
- Exit Policies
- Upstream-Provider
  - IP-Adresse(n)
  - DNS + Reverse DNS
  - WHOIS + Abuse
- Abuse Reaktion
  - Beispiel
  - Exit Policy
- Firewall
  - Zwei Interfaces
  - Ports
  - L7-Analyse
  - Logs
- Projekt
  - Sicherheitsüberlegungen
  - Topologie

TOR-SERVER: ROLLE(N)



- “Stable”
- “Beginner”
- by Config.

https://www.torproject.org/

TOR-SERVER: EIGENSCHAFTEN IM TOR-NETZ

Modi

- Relay only (Exit-Policy „reject *:*“)
- Relay + Exit

- Zuerst:
  - Nur Middle Relay
- Stable
  - Weighted MTBF über Median bzw. >= 7 Tage
  - auch als Entry Guard
- Exit-Policy

https://www.torproject.org/

TOR-SERVER: VERWENDETE BANDBREITE [1v3]

Limits müssen sein

- Wie / Wo werden diese überprüft bzw. erzwungen?
- Trivial bei 100% eines 10 oder 100 Mbps-Links
- Was aber tun z.B. bei 50 Mbps (1/2) oder 200 Mbps (1/5)

Einstellungen im Tor-Server: „Token Bucket“

- BandwidthRate <Bytes_per_Second>
- BandwidthBurst <Bytes>
- MaxAdvertisedBandwidth <Bytes_per_Second>
- …

https://www.torproject.org/docs/tor-manual.html.en

TOR-SERVER: VERWENDETE BANDBREITE [2v3]

Bei Traffic-Limits je Zeiteinheit (z.B. monatlich)

- AccountingMax <bytes>
- AccountingRule sum | max
  Summe R+W oder Maximum (R, W)
- AccountingStart day | week | month [day] HH:MM
  - Tageslimit / Wochenlimit / Monatslimit
  - Default: "month 1 0:00"

Reaktion:

- Fast ausgeschöpft: Keine neuen Verbindungen mehr annehmen
- Voll ausgeschöpft: Hibernation

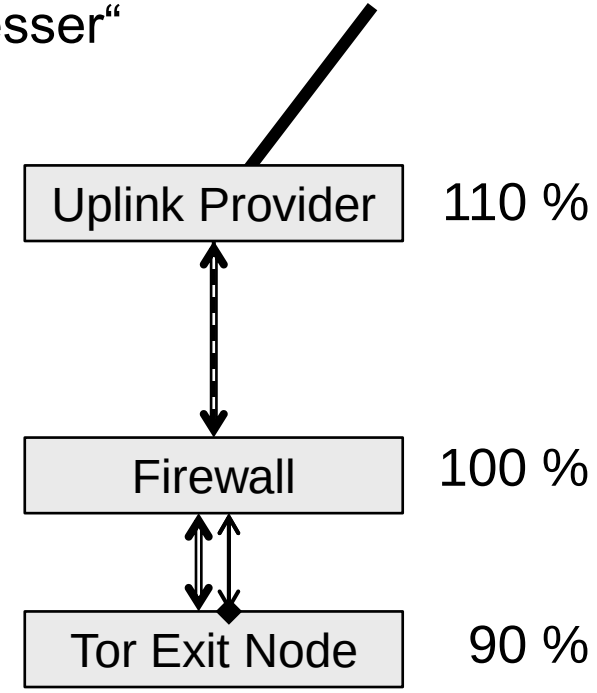
https://www.torproject.org/docs/tor-manual.html.en

TOR-SERVER: VERWENDETE BANDBREITE [3v3]

Überprüfung der Bandbreite findet am besten mehrfach statt:

Slogan: „Vertrauen ist gut, Misstrauen ist besser“

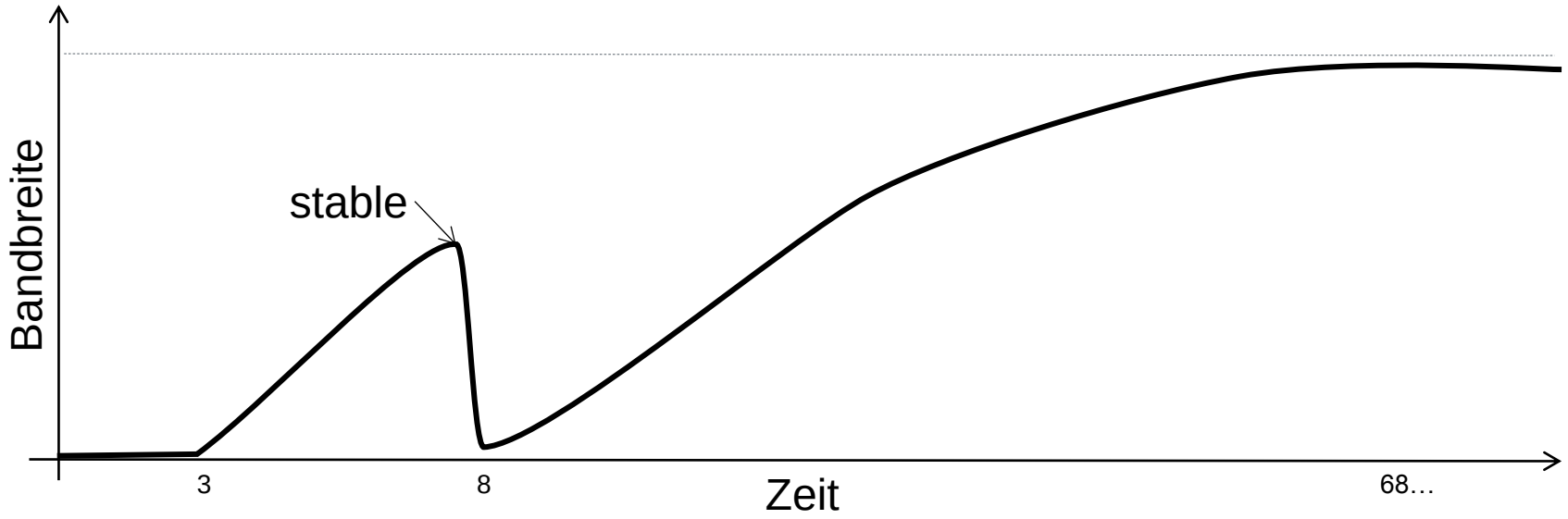
- Bei „unserem“ Uplink-Provider
- In einer Firewall direkt vor Tor
- Im Tor-Server selbst



https://www.torproject.org/docs/tor-manual.html.en

TOR-SERVER: FROM „MIDDLE“ TO „ENTRY GUARD“

- „Eile mit Weile“ ist die Devise
- Mit der Zeit wird man “stable”
- Damit auch als Entry-Node “Guard” geeignet



https://blog.torproject.org/blog/lifecycle-of-a-new-relay

TOR-SERVER: BETRIEB REINER RELAIS-KNOTEN

- Bandbreitenfrage (bereits gelöst)
- Datentransfer ohnehin verschlüsselt
- Weitergabe der Daten nur an andere Tor-Server
- Kein Datentransfer zu Endknoten

Konsequenz: Eigentlich keine Probleme zu erwarten

Es gibt aber trotzdem Security-Incident-Tickets;

Beispiel dafür %

TOR-SERVER: TICKET BENUTZUNG PORT 22

Sehr geehrte Damen und Herren,
wir müssen davon ausgehen, dass es mit/auf dem Rechner mit IP-Adresse <ip> / <reverse-dns-name> ein Sicherheitsproblem gibt:
Ausgehende Angriffe.

Folgende Informationen liegen uns dazu vor:
Unsere Netzwerkstatistiken zeigen auffallende ausgehende Verbindungen zu port 22 (ssh). Daher ist ein ssh-Scan oder eine Brute-Force-Attacke auf Passwörter anzunehmen.

Mögliche Fehldiagnosen:
- legitimer Kontakt mit vielen ssh-Servern (z.B. eines Clusters)
- Nutzung von Port 22 durch andere Protokolle
…

Auslöser hier: Verbindungen zu mehr als X verschiedenen Netzen (/24 bei ipv4 und/oder /48 bei ipv6) innerhalb von Y Stunden

TOR-SERVER: DER WEG ZUM EXIT-NODE

- Als “interner” Knoten des Tor-Netzwerkes:
  `ExitPolicy reject *:*`

- Von 0% auf 110% wäre damit
  ~~`ExitRelay 1`~~
  ~~`ExitPolicy accept *:*`~~

- ABER: Das bewährt sich nicht;
- Typischerweise verwendet man eine eingeschränkte Exit-Policy
- Beispiele dazu
  - https://trac.torproject.org/projects/tor/wiki/doc/ReducedExitPolicy
  - http://www.bsdnow.tv/tutorials/tor
  - Eigene Recherche z.B. unter https://torstatus.blutmagie.de (was machen andere Exit-Nodes?)

TOR-SERVER: AUSSCHNITTE AUS EXIT-POLICIES

```
reject 0.0.0.0/8:*
...
reject 172.16.0.0/12:*

reject *:25
reject *:587
reject *:465
reject *:4899

reject 93.93.69.0/24:*
...
accept *:*
```

“chulak”
https://torstatus.blutmagie.de/router_detail.php?FP=b0279a521375f3cb2ae210bdbfc645fdd2e1973a

```
reject 0.0.0.0/8:*
...
reject 172.16.0.0/12:*

reject 94.242.228.107:*
reject 5.133.182.0/24:*
  ...
accept *:20-23
accept *:43
accept *:53
...
accept *: 64738
reject *:*
```

“AtomicExitLU1“
https://torstatus.blutmagie.de/router_detail.php?FP=f4b72ea6fd0eacf652b6c200611f37244f2b31f3

JKU INSTITUTE OF NETWORKS AND SECURITY

TOR-SERVER: AUSSCHNITT AUS KONFIGURATION

```
ContactInfo           <name> <email>
ORPort                9001
DirPort               9030
Nickname              <kurzbezeichnung>
RelayBandwidthRate    15 MB
RelayBandwidthBurst   20 MB

ExitPolicy reject     0.0.0.0/8:*
ExitPolicy reject     169.254.0.0/16:*
...
ExitPolicy accept     *:80          # HTTP
ExitPolicy accept     *:443         # HTTPS
ExitPolicy accept     *:8443        # ...
...
ExitPolicy reject     *:*
```

TOR-SERVER: EXIT-NODE

- Minimalanforderungen: Wann wird man Exit-Node?
  - Zwei der Ports 80 (http), 443 (https), 6667 (Internet Relay Chat)
  - Ein /8 Adressbereich

  http://tor.stackexchange.com/questions/4289/exit-node-maturity

- Aus technischer Sicht (also keine juristische Aussage):
  - Exit als Proxy (die IP des Tor-Servers wir als Source verwendet)
  - Entry via Tunneling mit Encryption
  - Transit-Weiterleitung von L4-Paketen (TCP/UDP)

TOR-SERVER: UPSTREAM-PROVIDER & IP-ADDR.

- Eigener IP-Adressbereich (eigene IP / IPs)
- Möglichst starke Trennung erwünscht
- Bei IP-Sperren soll nur Tor-Funktionalität betroffen sein
- Mit IP-Adressbereichen sind oft auch Berechtigungen verknüpft
  - Intern: Beispiele in jeder Firewall
  - Oft auch extern: Zugriff auf bestimmte Ressourcen bei Vertragspartnern von bestimmten (eigenen) IPs aus.
- Trifft generell zu:
  - ISPs
  - Firmen, Universität, …
  - auch im eigenen Bereich

https://trac.torproject.org/projects/tor/wiki/

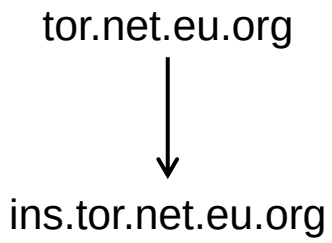
TOR-SERVER: UPSTREAM-PROVIDER & DNS [1v4]

- Eigene DNS-Namen notwendig;
  Will der ISP diese Namensauflösung machen?
- Generelles Problem bei DNS: Delegation erforderlich
- Namensauflösung <name> → <ip>
  - A bzw. AAAA Records
  - Meist nicht ganz so wichtig, Tor-Directory verwendet IPs
    aber wohin löst man „reverse“ auf …
- Namensauflösung <ip> → <name>
  - Reverse Namensauflösung
  - PTR Records
  - Muss vom ISP kommen, von dem man die IP-Adressen hat
  - Reverse Namensauflösung kann (insb. bei IPv4)
    „organisatorisch komplex“ werden

TOR-SERVER: UPSTREAM-PROVIDER & DNS [ADD]

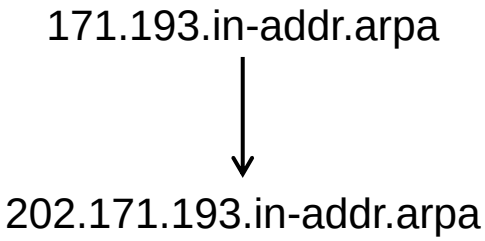
- **Delegation <name> → <ip>**

```
Zone tor.net.eu.org
ins    IN NS    <ip1_dns_für_ins.tor.net.eu.org>
ins    IN NS    <ip2_dns_für_ins.tor.net.eu.org>

Zone ins.tor.net.eu.org
ns1    IN A     <ip1_dns_für_ins.tor.net.eu.org>
```



- **Reverse Delegation <ip> → <name>**

```
Zone 171.193.in-addr.arpa
202    IN NS    <ip1_dns_reverse_193.171.202/24>
202    IN NS    <ip2_dns_reverse_193.171.202/24>

Zone 202.171.193.in-addr.arpa
55     IN PTR   193-171-202-55.provider.at
```



TOR-SERVER: UPSTREAM-PROVIDER & DNS [2v4]

IPv4-Reverse-Namensauflösung nach RFC 2317

```
Zone 202.171.193.in-addr.arpa
   55       IN PTR    193-171-202-55.provider.at.
   128/27   IN NS     <ip1 dns für 128/27.202.171.193.in-addr.arpa>
   128/27   IN NS     <ip1 dns für 128/27.202.171.193.in-addr.arpa>

   150      IN CNAME  150.128/27.202.171.193.in-addr.arpa.
   151      IN CNAME  151.128/27.202.171.193.in-addr.arpa.
   152      IN CNAME  152.128/27.202.171.193.in-addr.arpa.
   ...
```

```
Zone 128/27.202.171.193.in-addr.arpa
   150      IN PTR            tor2r.ins.tor.net.eu.org.
   151      IN PTR 193-171-202-151.ins.tor.net.eu.org.
```

TOR-SERVER: UPSTREAM-PROVIDER & DNS [3v4]

```
# nslookup

> 193.171.202.150
Server:    140.78.2.62
Address:   140.78.2.62#53

150.202.171.193.in-addr.arpa
   canonical name = 150.128/27.202.171.193.in-addr.arpa.

150.128/27.202.171.193.in-addr.arpa
   name = tor2r.ins.tor.net.eu.org.

> set type=any
> tor2r.ins.tor.net.eu.org.

tor2r.ins.tor.net.eu.org  text = "TOR-Server; abuse@tor.jku.at“
Name:    tor2r.ins.TOR.net.eu.org
Address: 193.171.202.150
```

Anmerkung: Output stark gekürzt. Statt “dig” wurde “nslookup” wegen der “Kompatibilität” zu Windows gewählt.

TOR-SERVER: UPSTREAM-PROVIDER & DNS [4v4]

Konsequenzen:

- Eigene DNS-Zone(n)
- Eigene(r) DNS-Server
- Frage Secondary DNS
- Delegation generell

\+ Zusatzaufwand für IPv4-Reverse-Einträge

TOR-SERVER: UPSTREAM-PROVIDER & WHOIS [1v4]

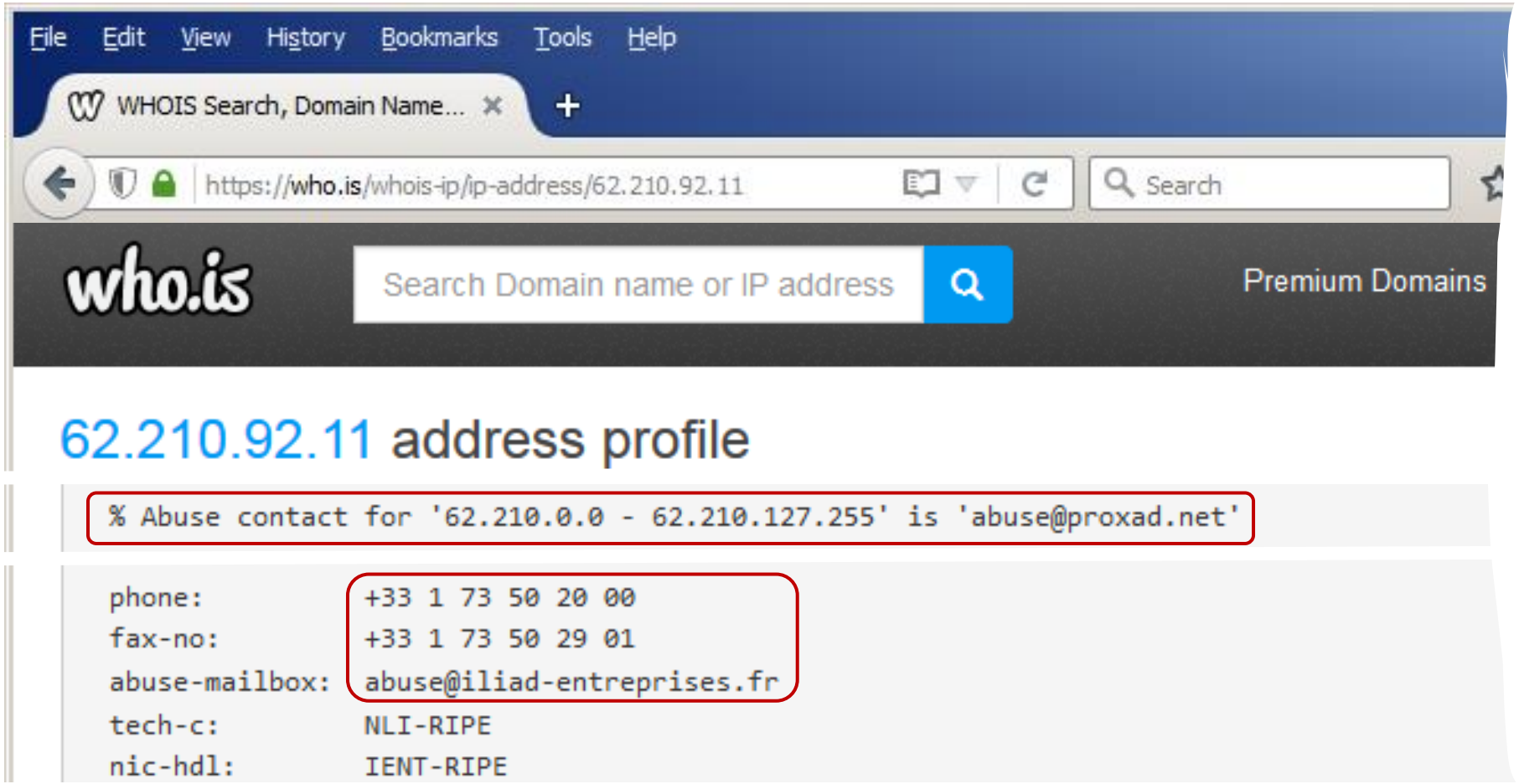
- Tor-Exit-Server wird für Attacken gegen andere Systeme missbraucht.
- IPS / Firewall erkennt diese Attacke.
- Admin händisch / System automatisch sucht sich **per WHOIS** den Besitzer der Source-IP der Attacke

… und schreibt an die zugehörige Abuse-Email-Adresse eine „böse“ Email

oder

… macht einen höflichen / unhöflichen Telefonanruf.

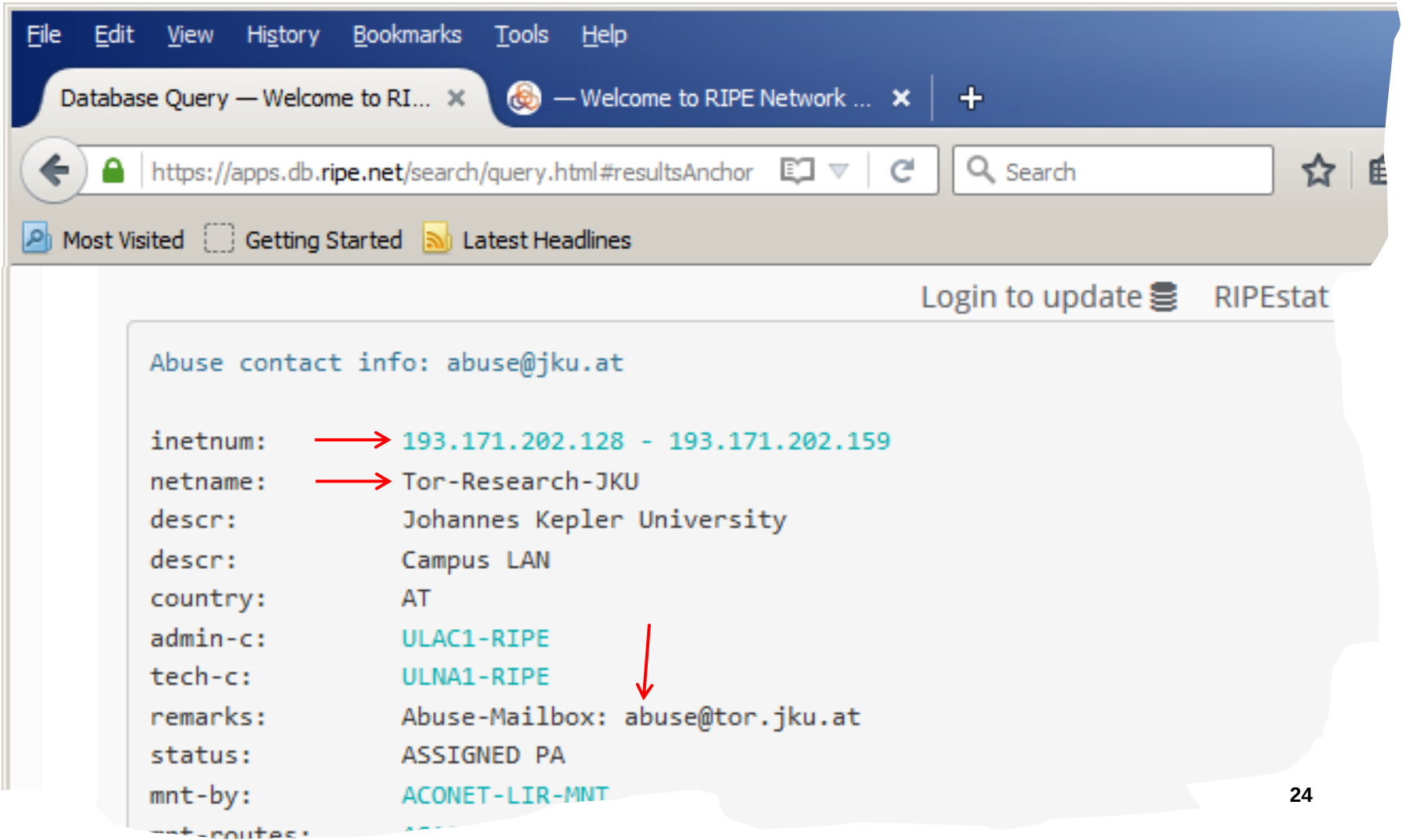
TOR-SERVER: UPSTREAM-PROVIDER & WHOIS [2v4]



TOR-SERVER: UPSTREAM-PROVIDER & WHOIS [3v4]

- Upstream-Provider erhält Mails (Tickets) an seine Abuse-Adresse, telefonische Anfragen usw.
- Reaktion darauf?
  - ☹ Alle „unsere“ IPs sperren
  - ☹ „Unsere“ Tor-IP sperren
  - 😐 Ignorieren
  - ☺ Selbst reagieren
  - ☺ Mails an „uns“ weiterleiten
  - = Irgendwann verliert der Upstream-Provider aber die Geduld
- Eigener WHOIS-Eintrag
  - ☐ Mit Information über den Tor-Server
  - ☐ Mit eigener Abuse-Email-Adresse
  - ☐ …

TOR-SERVER: UPSTREAM-PROVIDER & WHOIS [4v4]



TOR-SERVER: BESCHWERDE→BEISPIEL-REAKTION

- Beschwerde
  - Attacke war von der IP des Tor-Servers
  - Automatisierte Email, ausgehend z.B. von einem IPS
  - Benennt eine Attacke und einen Destination-Bereich /24
  - Erklärt, dass die Source-IP ein Tor-System ist, das aber „egal“ ist
- Reaktion z.B.:
  - Rückfrage, ob der Sender wirklich für den gesamten genannten IP-Adressbereich “zeichnungsberechtigt” ist
  - Blocken des IP-Bereiches in der Exit-Policy für einen bestimmten Zeitraum (z.B. 1 Monat); insb. wenn sonst der Upstream-Provider die IP sperren würde https://lists.torproject.org/pipermail/tor-relays/2015-November/008163.html

TOR-SERVER: SPERREN NETZE / PROTOKOLLE

- Korrekt und öffentlich sichtbar in der ExitPolicy
  `ExitPolicy reject <ip>[/<mask>]`
  `ExitPolicy reject <ip>[/<mask>]:<portnr>`
- Gegen (!!) die Tor-Policy:
  - Einfach irgendwo in einer (am Tor-Server oder extern) vorgeschalteten Firewall
  - Falls das der Upstream-Provider macht, hat man hier wenig Möglichkeiten
- Sperre ganzer Protokolle:
  - Einfügen von: `ExitPolicy reject *:<portnr>`
  - Löschen Eintrag: `ExitPolicy accept *:<portnr>`

TOR-SERVER SICHERHEIT VIA FIREWALL [1v5]

- ☺ Tor-Port ist in der Konfiguration des Tor-Servers frei wählbar (siehe Konfiguration ORPort bzw. auch DirPort)
- ☹ Das „Port-Problem“
  - Kurzer Blick auf die Ports der Tor-Server z.B. via https://torstatus.blutmagie.de/index.php?SR=ORPort&SO=Asc
  - Gebräuchliche Ports sind u.a./insb. 9001, 443 (8443), 80 (8080), …
  - Aber: Auch viele andere Ports kommen vor; Beispiele: 20-25, 39, 43, 47, 53, 90,110,143, 219, 220, 389, 425, 427, 440-448, 8443, 9002-9010, …, … 65530, …
- In der Firewall:

Source	to	Destination	Action
outside_world:*	→	ip_tor_server:ORPort	allow
ip_tor_server:*	→	outside_world:*	allow

TOR-SERVER SICHERHEIT VIA FIREWALL [2v5]

Sicht FW-Admins: Protokollieren (Logging) ist wesentlich

- Was passiert(e)
- Woher/wie werden „wir“ angegriffen
- Welcher Traffic wird irrtümlich geblockt
- Reaktionen darauf

Bei Tor-Einsatz ist Ziel aber: Nichts protokollieren

- Angriffe gegen IPs der Firewall
- Tor-Server „dahinter“

Konsequenz: Irgendwie im „Blindflug“ unterwegs

TOR-SERVER SICHERHEIT VIA FIREWALL [3v5]

Sicht FW-Admins: L7 Content-Analyse

- Devices: Proxy, IPS
- Beispiele:
  - Unverschlüsselt „sowieso“: HTTP, FTP, …
  - HTTPS (wer wirklich möchte muss zuerst das Firmen-Root-Zertifikat der FW akzeptieren)
  - …

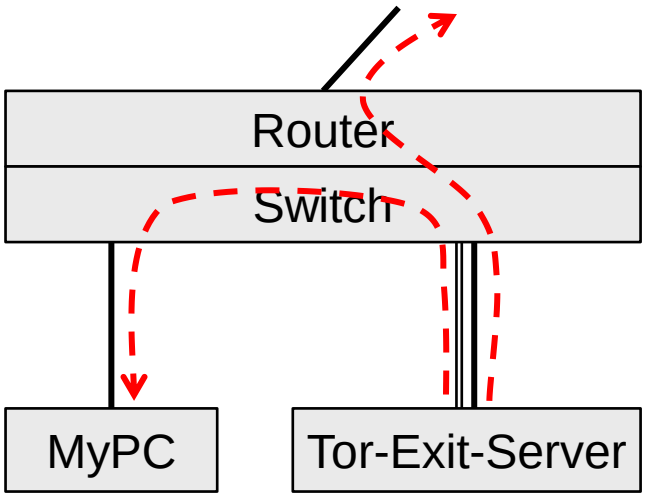
Tor-Einsatz

- Keine Content-Analyse gewünscht (Logs, ..) und
- Großteils auch nicht möglich (End-to-End Security)

Konsequenz: Irgendwie im „Blindflug“ unterwegs

TOR-SERVER SICHERHEIT VIA FIREWALL [4v5]

Über einen Tor-Exit-Server kann „konzeptionell“ auch das eigene direkte Umfeld attackiert werden.



Varianten zur Absicherung:

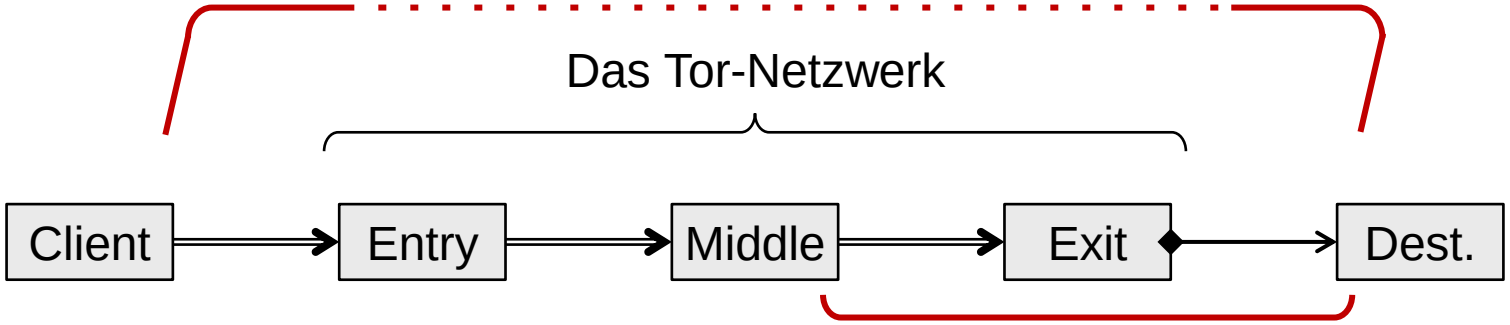
- In der Tor-Server-Software selbst durch **`ExitPolicy reject <eigene_kritische_IPs>`**
- \+ In der Firewall direkt am/im OS auf der Tor-Server-HW (z.B. IPtables)
- \+ Auf einer externen Firewall, welche auf diesem Segment nur den Tor-Server angeschlossen hat

TOR-SERVER SICHERHEIT VIA FIREWALL [5v5]

- Server soll beispielsweise Emails mit Logging-Informationen an bzw. über einen „nahen / eigenen“ Mailserver senden.
  - ☐ Dieser Mailserver muss von der TorIP aus erreichbar sein.
  - ☐ SMTP nach aussen soll frei sein (TorIP:* → Internet:25).
    Es gibt derzeit >= 2 Tor-Server, welche über Port 25 erreichbar sind)
  - ☺ TCP-Port 25 (SMTP) in meist in der Tor-Exit-Policy geblockt
- Was aber wäre, wenn es um andere Ports ginge?
  - ☐ Erreichbarkeit von der TorIP aus erforderlich
  - ☐ Erreichbarkeit via TorExit-Policy erwünscht

  } `TorIP:* → MyServer:pXYZ ?`
- Mögliche Konsequenzen
  - ☐ Tor-Server mit mehreren IPs
  - ☐ Service of andere Portnummer umlegen
  - ☐ L7-Analyse integrieren (??)
  - ☐ …

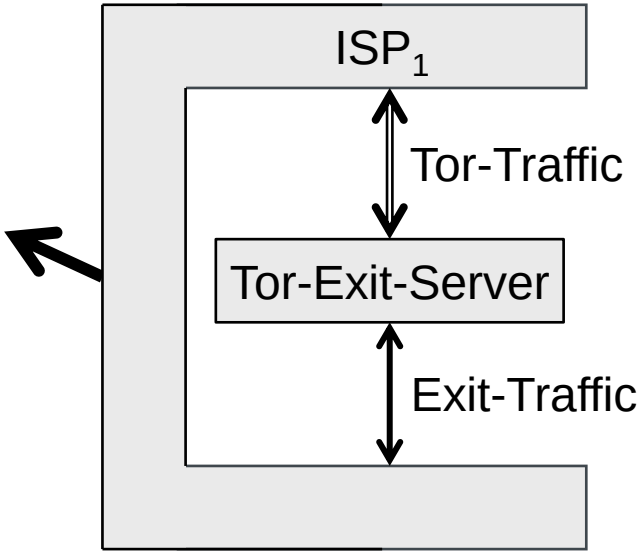
TOR-SERVER PROJEKT: „SICHERHEITSANALYSE“ [1v2]



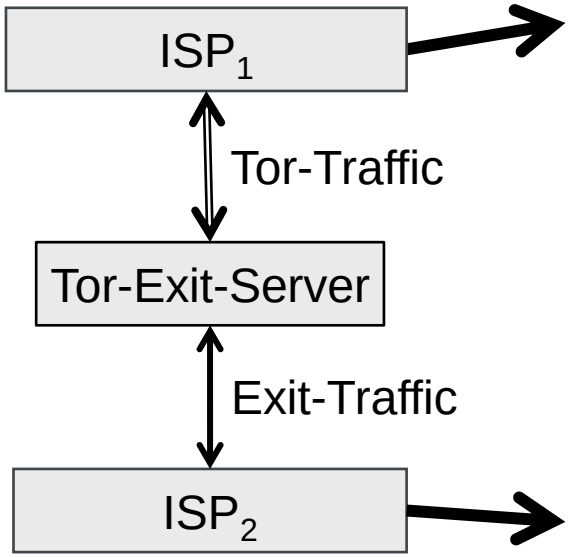
- Tor hat eine implizite “Schwachstelle” wegen Low Latency
- Was wäre der schlimmste Fall bei Daten auf/von einem Knoten?
  - ☐ Beide Seiten (incoming connections & outgoing connections inkl. zeitlicher Abfolge liegen vor.
  - ☐ Kombination insb. durch zeitliche Abfolge, Paketgrößen usw.
- Konsequenzen: Nur Exit-Traffic kommt überhaupt in Frage; keine Zeitinformationen bei allen Auswertungen → Simple Counting

TOR-SERVER PROJEKT: „SICHERHEITSANALYSE“ [2v2]

- ISP ist Upstream-Provider und Downstream-Provider in einem.
- ISP kann damit (technisch!) den gesamten Traffic protokollieren, wird ev. IPS einsetzen, …
- Typischer Ist-Status (1 ISP)

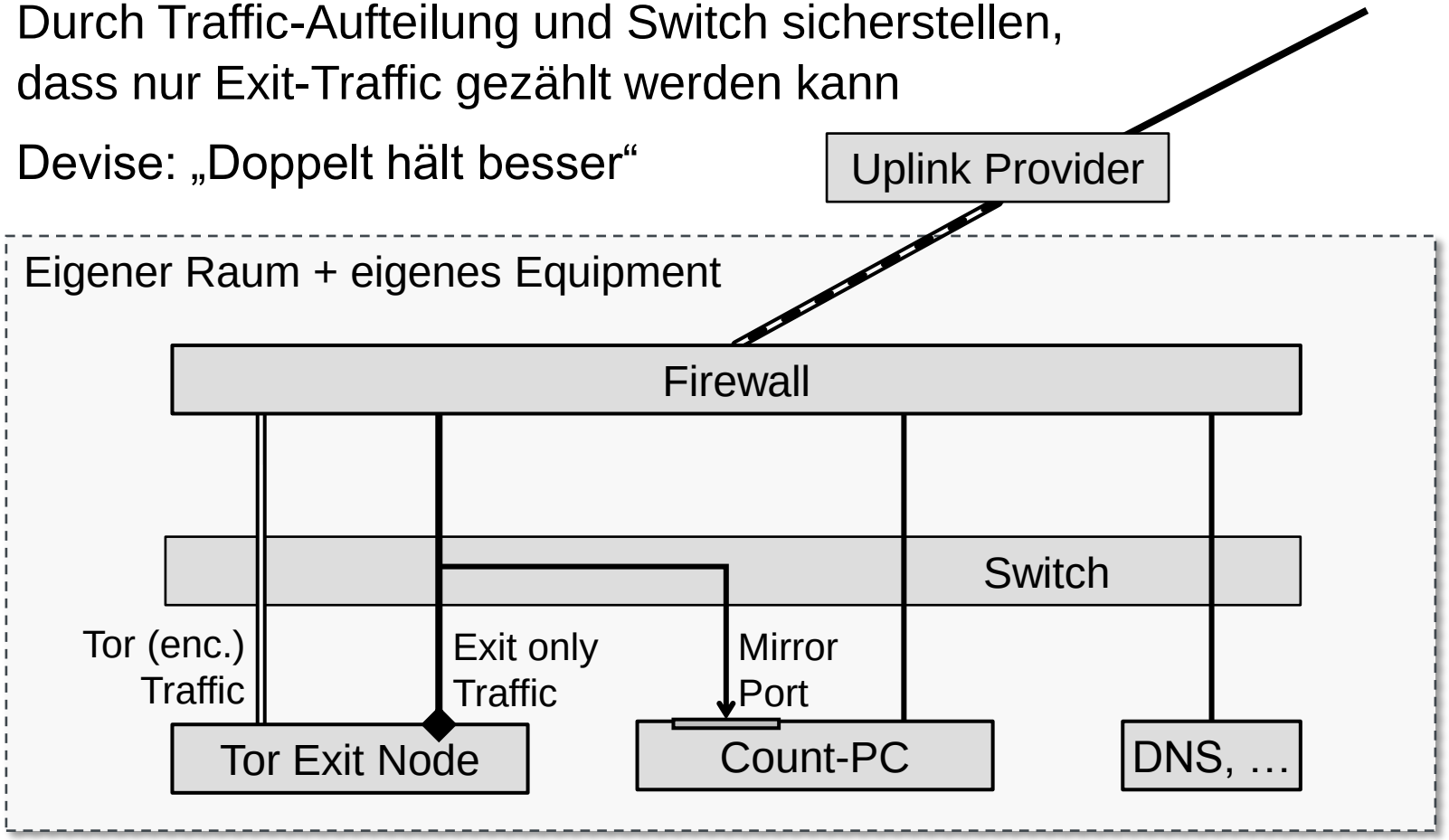


- 2 ISPs für Tor-Entry und Exit

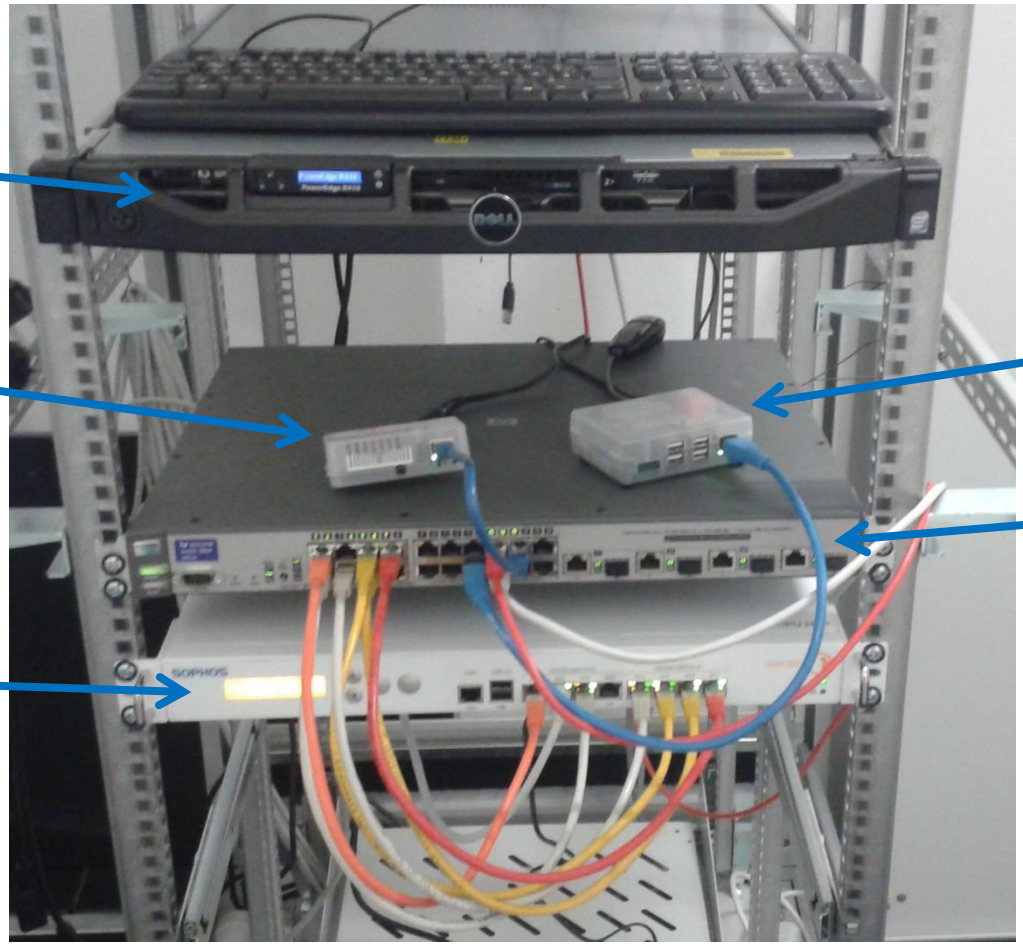


TOR-SERVER PROJEKT: TOPOLOGIE

- Durch Traffic-Aufteilung und Switch sicherstellen, dass nur Exit-Traffic gezählt werden kann
- Devise: „Doppelt hält besser“



Tor-Server Projekt: Basis-Infrastruktur



JOHANNES KEPLER
UNIVERSITÄT LINZ

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

… und ich freue mich auf Ihre Anregungen, Fragen, …

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
www.jku.at