Rechnernetze:
(8) Firewalls etc.

Prof. Dr. Klaus-Peter Kossakowski

Gliederung der Vorlesung

- Einführung und Historie des Internets
- Schichtenmodell, Netzwerk als Infrastruktur
- Layer 7: Anwendungsschicht
- Layer 7/4: Socket-Programmierung
- Layer 4: Transportschicht
- Layer 3: Netzwerkschicht
  - IPv4, ICMPv4, IPv6, Routing
  - Firewalls
  - Management
- Layer 2: Sicherungsschicht

Inhalte dieses Kapitels

In diesem Kapitel wird die Rolle und Aufgabe von Netzwerksicherheitskomponenten erklärt.

Besonders wird auf Firewalls eingegangen und erklärt, wie Eigenschaften des Netzwerk- sowie der Transportprotokolle genutzt werden, um eine Separierung von Rechnern mit unterschiedlichem Schutzbedarf durch Beschränkung der Kommunikation zu erreichen.

Die Firewall-Architektur eines kleinen, lokalen Netzwerkes wird schrittweise entwickelt.

Ziele dieses Kapitels

Sie kennen verschiedene typische Komponenten der Netzwerksicherheit und deren Funktion.

Sie können das Konzept einer Firewall auf Ebene der Netzwerk-/Transportschicht erläutern und dies anhand IP, UDP und TCP erklären.

Sie können das Prinzip der geringsten Berechtigung auf die Kommunikation zwischen einem lokalen Netz und dem Internet anwenden und eine Firewallarchitektur aus den Anforderungen ableiten.

Generell Empfehlung für mehr (IT-) Sicherheit!

Keep it stupid simple! a.k.a. K.I.S.S.

- **Kompartmentalisierung**
  - Principle of least privilege
  - Minimalisierte Vertrauensbeziehungen
- **Effektivität**
  - Principle of the weakest link
- **„Defense in Depth“**
  - Nicht nur eine Maßnahme

Definition: Firewall

- **Eine Firewall ist**
  - eine Architekturkomponente
  - mindestens ein System, aber oft mehrere Systeme
- **Eine Firewall wird**
  - zwischen Bereichen platziert, die
  - unterschiedliche Sicherheitsanforderungen haben, z.B.
    - zwischen LAN und Internet
    - zwischen kritischen Servern und LAN

Definition: Firewall (2)

- **Eine Firewall implementiert**
  - das Prinzip der geringsten Berechtigung und die
  - Zugriffskontrolle auf der Netzwerkschicht
    - evtl. mit Hilfe von Daten der Transportschicht
- **Eine Firewall ersetzt**
  - keine Maßnahmen zur Vertraulichkeit der Übertragung oder Manipulationsfreiheit
- **Verschlüsselung kann es der Firewall schwer machen**

Definition: Network IDS

- **Ein Network IDS (Intrusion Detection System) ist**
  - eine Architekturkomponente
  - in Netzwerken mit höheren Sicherheitsanforderungen
- **Abhängig von der Art des Systems können sehr viele Ereignisse aufgezeichnet / eskaliert werden**
  - Analyse und Tuning der Maßnahmen unbedingt erforderlich!

Definition: Network IDS (2)

- **Ein NIDS implementiert**
  - das Prinzip der Verteidigung in der Tiefe,
  - überwacht z.B. die Funktion einer Firewall, und
  - erkennt Angriffe Hilfe von allen Daten
    - evtl. werden die sogar zusammengebaut
- **Ein NIDS ersetzt**
  - keine Firewall
- **Verschlüsselung macht es der NIDS schwer**

Definition: Host IDS

- **Ein Host IDS implementiert**
  - das Prinzip der Verteidigung in der Tiefe,
  - überwacht z.B. die Funktion einer Anwendung, und
  - erkennt Angriffe Hilfe von allen Daten
    - die auf Anwendungsebene nicht erst zusammengebaut werden müssen
- **Ein HIDS ersetzt**
  - keine Firewall und ist effektiver als NIDS
- **Verschlüsselung ist kein Thema**

Definition: Network Monitoring

- **Network Monitoring ist meistens eine Anwendung von verschiedenen Tools incl. eines NIDS, konzentriert sich aber weniger auf Signaturen**
  - das sind Muster von Angriffen
- **Benötigen ebenfalls Auswertung und Feintuning**
  - Ist aber meistens konsequenter und nachhaltiger, weil ganzheitlicher, in der Wirkung

Definition: Honeypot

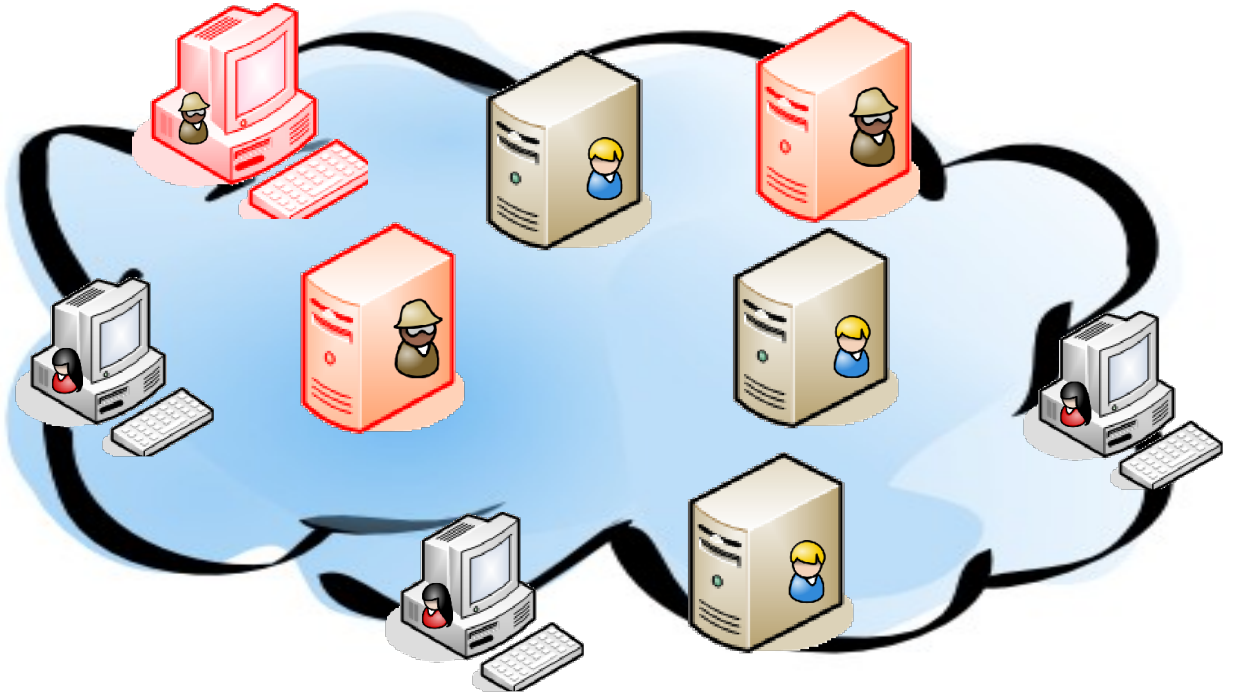
- **Ein Honeypot ist**
  - eine Architekturkomponente
  - in besonderen Umgebungen
- **Da es im Betrieb recht aufwändig sein kann, ist Vorsicht geboten, aber …**
- **Wenn es richtig platziert wird, dann kann man recht einfach laterale Bewegungen von Angreifern im eigenen LAN aufdecken**
  - … und außerdem Viren, Würmer und Trojaner

Definition: Log-Server

- **Ein Log-Server ist**
  - eine Architekturkomponente
  - und Pflicht in quasi allen Umgebungen
- **Dient vor allem zum Sammeln von Daten**
  - die natürlich ausgewertet werden müssen
- **Braucht seinerseits Schutz vor Angriffen, da die Daten erfolgreiche Angriffe, deren Herkunft und evtl. auch durchgeführte Aktionen der Angreifer aufzeigen können**

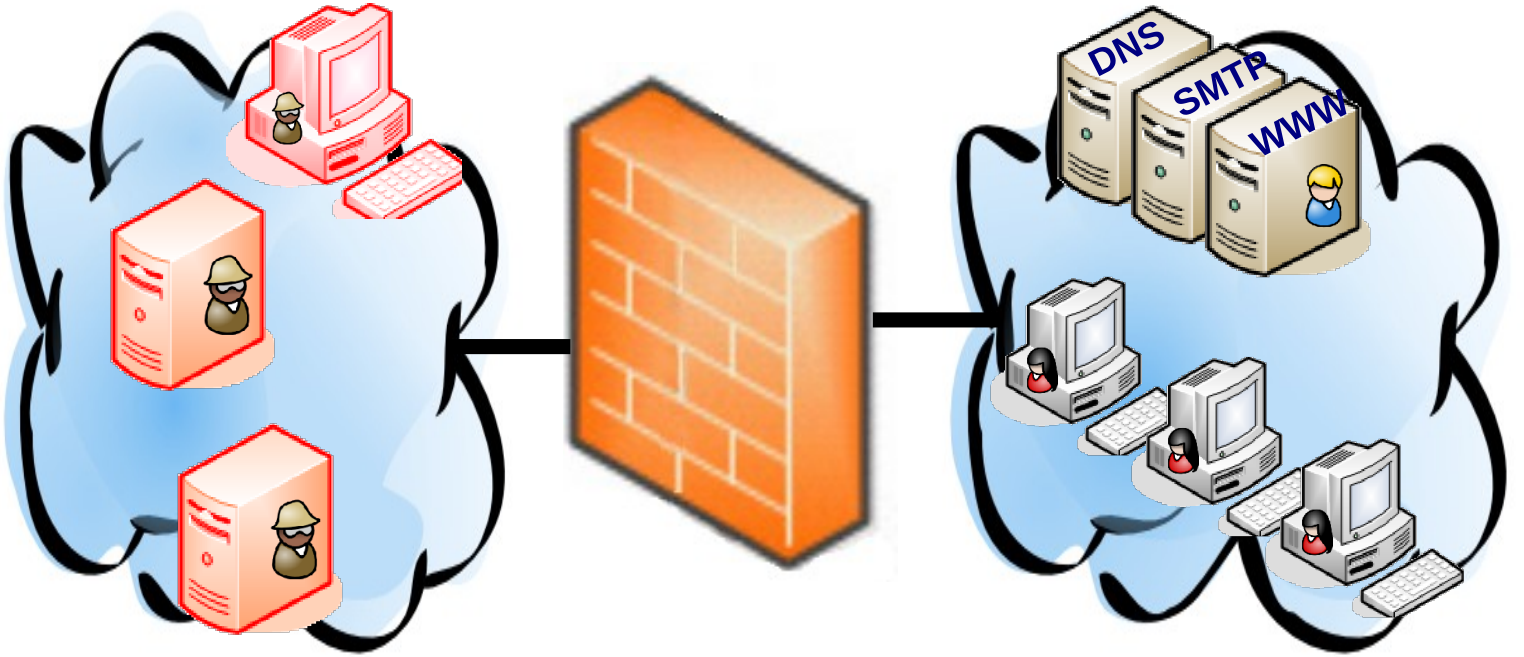
Am Anfang war ein Netz ...

Alles, jeder, überall ..., egal !



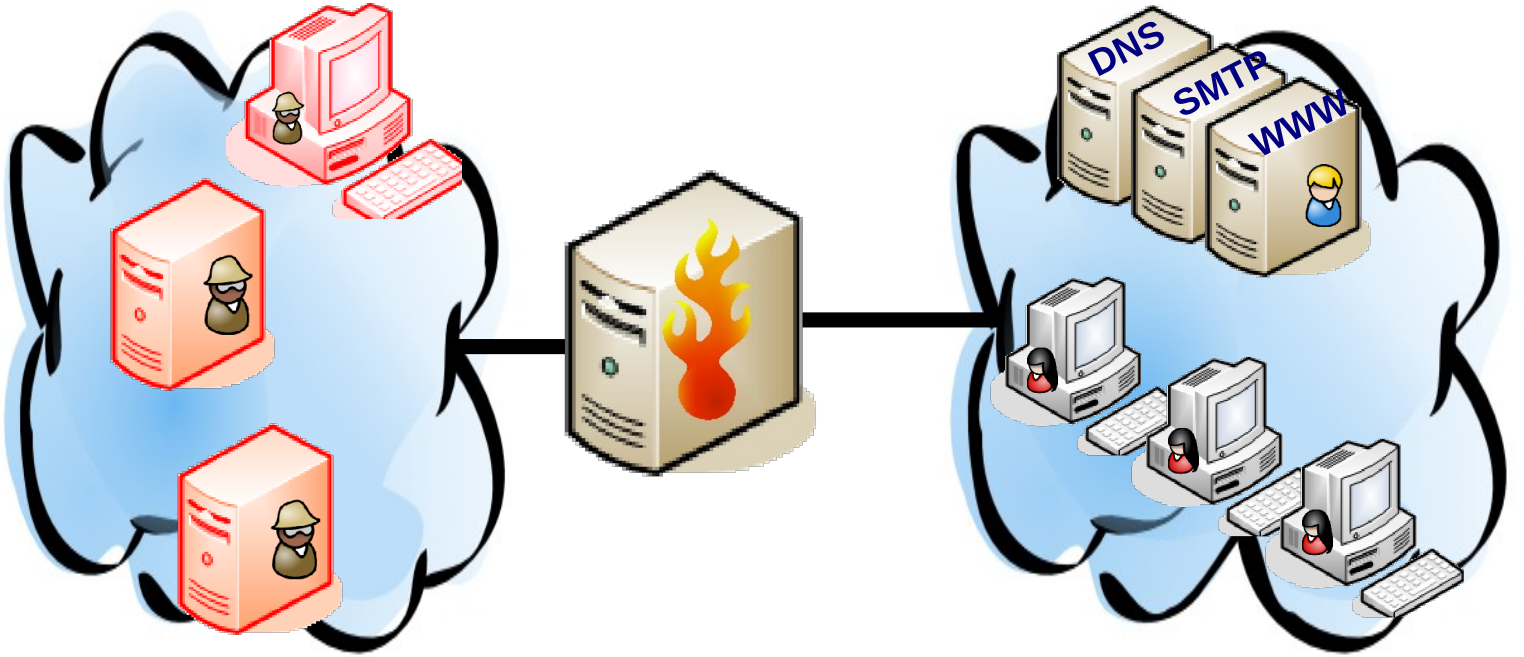
Aufteilung von Netzen

„Principle of least privilege“ erfordert eine Minimierung der Konnektivität!



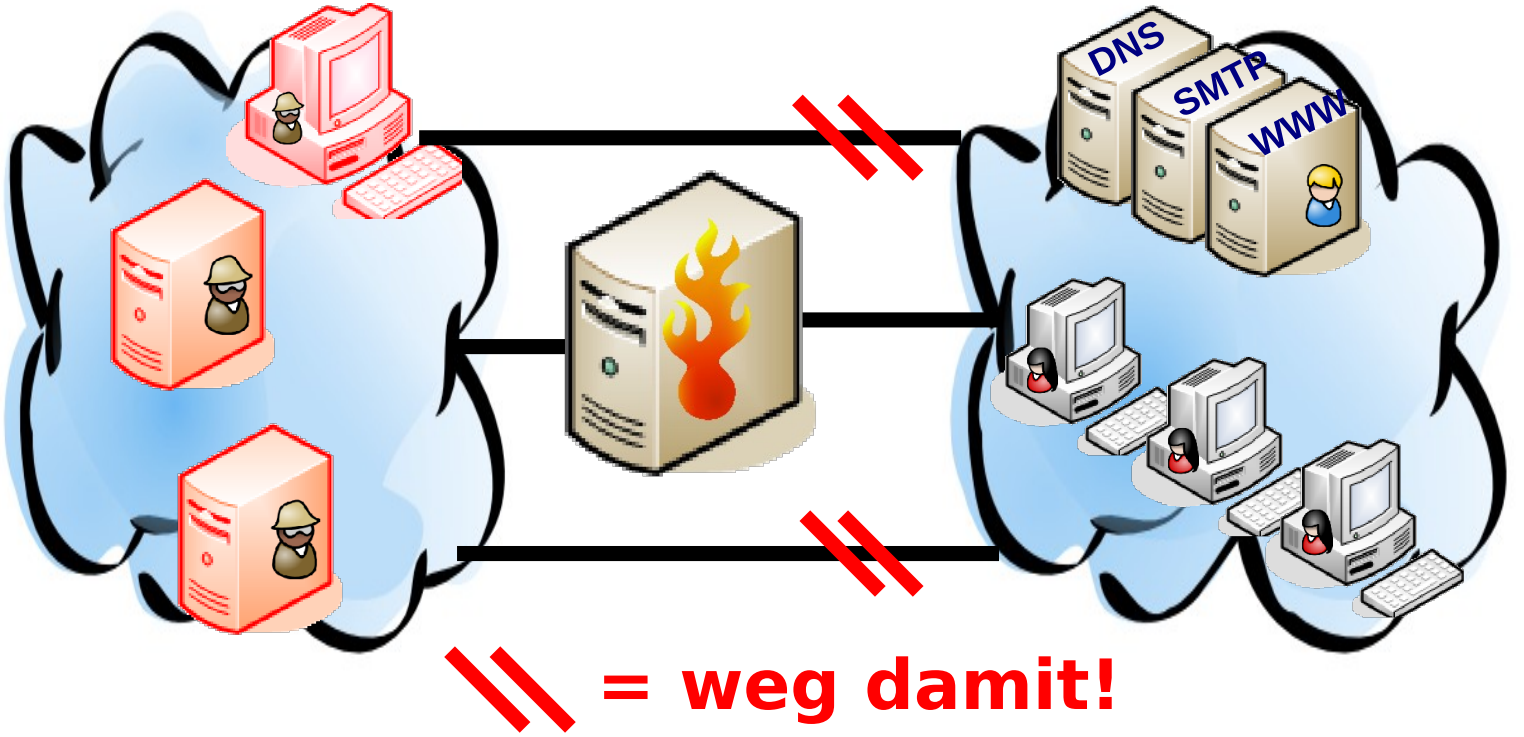
Aufteilung von Netzen (2)

„Principle of least privilege“ erfordert eine Minimierung der Konnektivität!



Aufteilung von Netzen (3)

„Principle of least privilege“ erfordert eine Minimierung der Konnektivität!



Aufteilung von Netzen == Filterung von Paketen

Alle in den Paketen vorliegende Daten können verwendet werden um zu entscheiden, ob das Paket „durchkommen“ darf.

- **Firewalls arbeiten üblicherweise auf**
  - Layer 4: Transportschicht, d.h. UDP / TCP
  - Layer 3: Netzwerkschicht, d.h. IP / ICMP
- **Was Firewalls nicht verstehen, wird verworfen!**
- **In jedem Fall zusätzliche Verzögerung und auch mögliche Fehlerquelle**

Die älteste Form: Packet Screens (kann jeder Router)

- **Statische Paketfilterung anhand**
  - Senderadresse (IP)
  - Empfängeradresse (IP)
  - Protokoll (TCP, UDP, ICMP)
- **Für UDP und TCP zusätzlich**
  - Senderport (TCP)
  - Empfängerport (TCP)
- **TCP-Flags, insbesondere SYN-Flag**
- **ICMP-Nachrichtentypen**
- **Router-Interface, auf dem das Paket ankam**

Packet Screens (2)

No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
1	LAN	*	TCP	>1023	21	any	ACCEPT
2	LAN	*	TCP	>1023	25	any	ACCEPT
3	LAN	*	TCP	>1023	53	any	ACCEPT
4	LAN	*	TCP	>1023	80	any	ACCEPT
5	LAN	*	TCP	>1023	443	any	ACCEPT
6	LAN	*	TCP	>1023	>1023	any	ACCEPT
7	*	LAN	TCP	21	>1023	!syn	ACCEPT
8	*	LAN	TCP	25	>1023	!syn	ACCEPT
9	*	LAN	TCP	53	>1023	!syn	ACCEPT
10	*	LAN	TCP	80	>1023	!syn	ACCEPT
11	*	LAN	TCP	443	>1023	!syn	ACCEPT
12	*	LAN	TCP	>1023	>1023	!syn	ACCEPT
13	LAN	*	UDP	>1023	53	any	ACCEPT
14	*	LAN	UDP	53	>1023	any	ACCEPT
15	*	*	any	any	any	any	DROP

Packet Screens: Relevante Probleme

Bestimmte Protokolle wie „Passive FTP“ brauchen sehr viele mögliche Verbindungen!

No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
...							
6	LAN	*	TCP	>1023	>1023	any	ACCEPT
...							
12	*	LAN	TCP	>1023	>1023	!syn	ACCEPT

Programme von Angreifern (Hintertüren) und Malware (Bots) nutzen genau solche Lücken ...

Packet Screens: Relevante Probleme (2)

Alle Endgeräte im LAN werden gleich behandelt

No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
1	LAN	*	TCP	>1023	21	any	ACCEPT
2	LAN	*	TCP	>1023	25	any	ACCEPT
3	LAN	*	TCP	>1023	53	any	ACCEPT
4	LAN	*	TCP	>1023	80	any	ACCEPT
5	LAN	*	TCP	>1023	443	any	ACCEPT
6	LAN	*	TCP	>1023	>1023	any	ACCEPT

Daneben gibt es die (zentralen) Server wie

SMTP server (25/tcp)

FTP server (21/tcp)

DNS server (53/udp+tcp)

WWW (80+443/tcp)

Packet Screens (3)

Beschränkungen für SMTP und DNS!

No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
1	LAN	*	TCP	>1023	21	any	ACCEPT
2	smtp srv	*	TCP	>1023	25	any	ACCEPT
3	dns srv	*	TCP	>1023	53	any	ACCEPT
4	LAN	*	TCP	>1023	80	any	ACCEPT
5	LAN	*	TCP	>1023	443	any	ACCEPT
6	LAN	*	TCP	>1023	>1023	any	ACCEPT
7	*	LAN	TCP	21	>1023	!syn	ACCEPT
8	*	smtp srv	TCP	25	>1023	!syn	ACCEPT
9	*	dns srv	TCP	53	>1023	!syn	ACCEPT
10	*	LAN	TCP	80	>1023	!syn	ACCEPT
11	*	LAN	TCP	443	>1023	!syn	ACCEPT
12	*	LAN	TCP	>1023	>1023	!syn	ACCEPT
13	dns srv	*	UDP	>1023	53	any	ACCEPT
14	*	dns srv	UDP	53	>1023	any	ACCEPT
15	*	*	any	any	any	any	DROP

Verbesserungen: Stateful Inspection

- **Dynamische Paketfilterung basiert auf**
  - traditionellen Packet Screens und
  - Dem Wissen über den Zustand der Verbindung (FSM einer TCP-Verbindung)

Wie soll denn das funktionieren?

Verbesserungen: Stateful Inspection (2)

Einfache Grundregeln:

- Solange ein Client keine Verbindung (SYN) aufgebaut hat, gibt es auch keine „Antwort“-Pakete aus dem Internet
- Solange ein Server nicht den Wunsch nach einer Verbindung (SYN/ACK) bestätigt hat, gibt es auch keine anderen Pakete
- Solange der Client nicht den Handshake beendet hat, gibt es auch keine andere Kommunikation!

Verbesserungen: Stateful Inspection (3)

- Logischer Zusammenhang zwischen den Paketen, die der gleichen Verbindung zuzuordnen sind, wird analysiert
- Filter-Regeln werden für die Lebenszeit einer Verbindung so erweitert, dass die „passenden“ Pakete erlaubt werden
- Sobald der TCP-Handshake erfolgreich beendet ist, können Daten fließen
- TCP-Sequence-Numbers werden überprüft, was das Fälschen schwieriger macht
- Weniger Regeln → weniger Fehler

Packet Screens (3)

No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
1	LAN	*	TCP	> 1023	21	any	ACCEPT
2	smtp srv	*	TCP	> 1023	25	any	ACCEPT
3	dns srv	*	TCP	> 1023	53	any	ACCEPT
4	LAN	*	TCP	> 1023	80	any	ACCEPT
5	LAN	*	TCP	> 1023	443	any	ACCEPT
6	LAN	*	TCP	> 1023	> 1023	any	ACCEPT
7	*	LAN	TCP	21	> 1023	!syn	ACCEPT
8	*	smtp srv	TCP	25	> 1023	!syn	ACCEPT
9	*	dns srv	TCP	53	> 1023	!syn	ACCEPT
10	*	LAN	TCP	80	> 1023	!syn	ACCEPT
11	*	LAN	TCP	443	> 1023	!syn	ACCEPT
12	*	LAN	TCP	> 1023	> 1023	!syn	ACCEPT
13	dns srv	*	UDP	> 1023	53	any	ACCEPT
14	*	dns srv	UDP	53	> 1023	any	ACCEPT
15	*	*	any	any	any	any	DROP

Regelsatz für Stateful Inspection

No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
1	LAN	*	TCP	>1023	21	syn	ACCEPT
2	smtp srv	*	TCP	>1023	25	syn	ACCEPT
3	dns srv	*	TCP	>1023	53	syn	ACCEPT
4	LAN	*	TCP	>1023	80	syn	ACCEPT
5	LAN	*	TCP	>1023	443	syn	ACCEPT
6	LAN	*	TCP	>1023	>1023	syn	ACCEPT
13	dns srv	*	UDP	>1023	53	any	ACCEPT
15	*	*	any	any	any	any	DROP

Ein bisschen muss noch konfiguriert werden ...

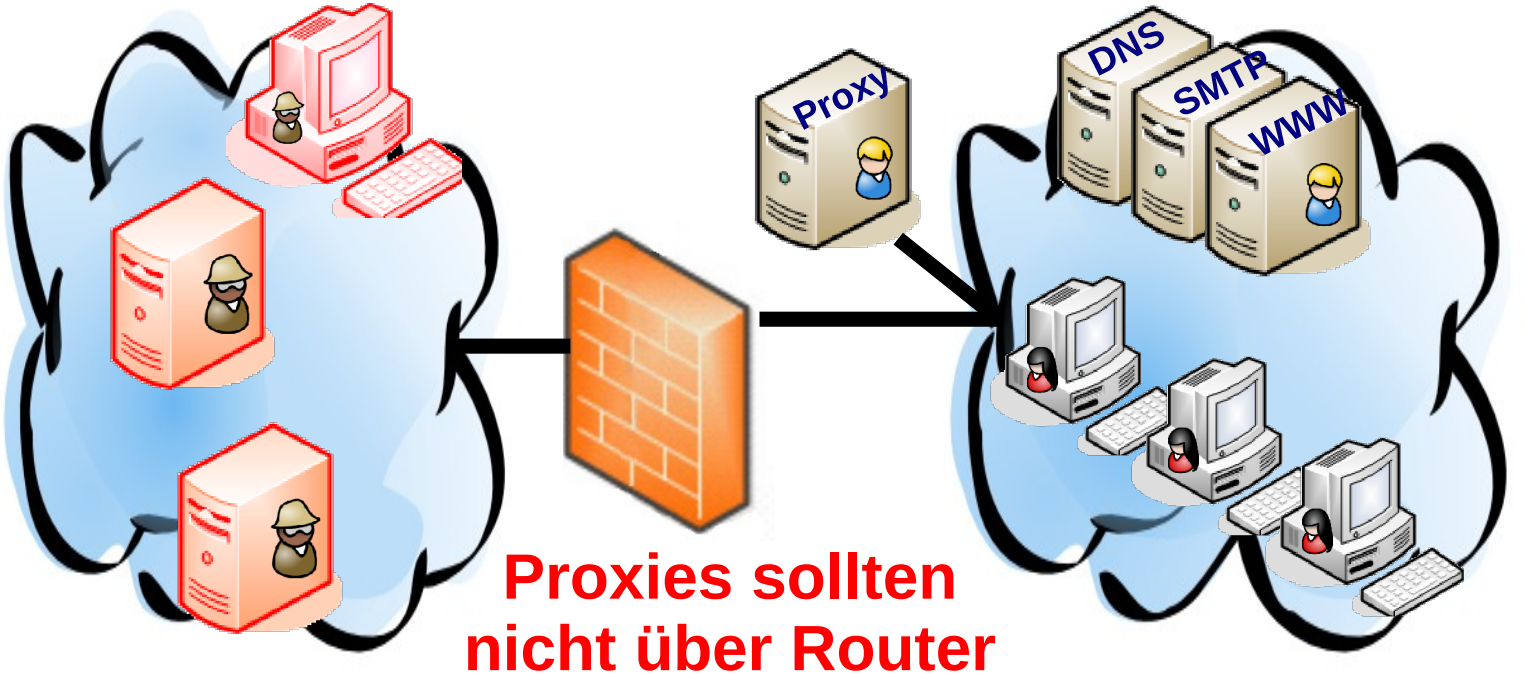
No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
1	LAN	*	TCP	>1023	21	syn	ACCEPT
2	smtp srv	*	TCP	>1023	25	syn	ACCEPT
3	dns srv	*	TCP	>1023	53	syn	ACCEPT
4	dns srv	*	UDP	>1023	53	any	ACCEPT
5	LAN	*	TCP	>1023	80	syn	ACCEPT
6	LAN	*	TCP	>1023	443	syn	ACCEPT
7	*	smtp srv	TCP	>1023	25	syn	ACCEPT
8	*	dns srv	TCP	>1023	53	syn	ACCEPT
9	*	dns srv	UDP	>1023	53	any	ACCEPT
10	*	www srv	TCP	>1023	80	syn	ACCEPT
11	*	www srv	TCP	>1023	443	syn	ACCEPT
12	*	*	any	any	any	any	DROP

Bestimmte Probleme bleiben: Prinzip der geringsten Berechtigung

- Solange Server extern erreichbar sind, kann der Angreifer mit einem Streich „drinnen“ sein
- Solange Endgeräte direkt ins – unsichere – Internet dürfen, sind diese auch direkt betroffen
- Solange intern und extern angebotene Dienste den gleichen Server benutzen, ist eine Absicherung schwieriger

Einführung von Proxy-Servern

Hierfür müssen die entsprechenden Formate und Protokolle verarbeitet werden können!



Proxies sollten nicht über Router realisiert werden!

Integration der Proxies für FTP und WWW

No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
1	proxy	*	TCP	>1023	21	syn	ACCEPT
2	smtp srv	*	TCP	>1023	25	syn	ACCEPT
3	dns srv	*	TCP	>1023	53	syn	ACCEPT
4	dns srv	*	UDP	>1023	53	any	ACCEPT
5	proxy	*	TCP	>1023	80	syn	ACCEPT
6	proxy	*	TCP	>1023	443	syn	ACCEPT
7	*	smtp srv	TCP	>1023	25	syn	ACCEPT
8	*	dns srv	TCP	>1023	53	syn	ACCEPT
9	*	dns srv	UDP	>1023	53	any	ACCEPT
10	*	www srv	TCP	>1023	80	syn	ACCEPT
11	*	www srv	TCP	>1023	443	syn	ACCEPT
12	*	*	any	any	any	any	DROP

Statt LAN werden jetzt die Proxies direkt angegeben – das ist schon alles!

z.B. Content-Filter

- **Filterung von Applets (ActiveX, JavaScript, Java), die im HTML-Text eingebunden sind**
- **Filterung von Cookies**
- **Üblicherweise sehr aufwändig, weil alle Aspekte eines Protokolls implementiert sein müssen**
  - Wenn das Protokoll zu komplex (mächtig) ist, gibt es aber auch Probleme ...

Proxy-Server für Firewalls / Virus Filter

- **Das „Scannen“ erfordert eine ganze Menge an Vorarbeiten, z.B. Entpacken**
- **Übliche Probleme:**
  - Zu viele unterschiedliche Kodierungen: tar, ar, uuencode, base64, zip, lha, arj, gzip, bzip, compress, ...
  - Rekursive Archive
  - Sehr viele Unterverzeichnisse
  - Verschlüsselte Dateien
  - Virus-Signaturen sind veraltet

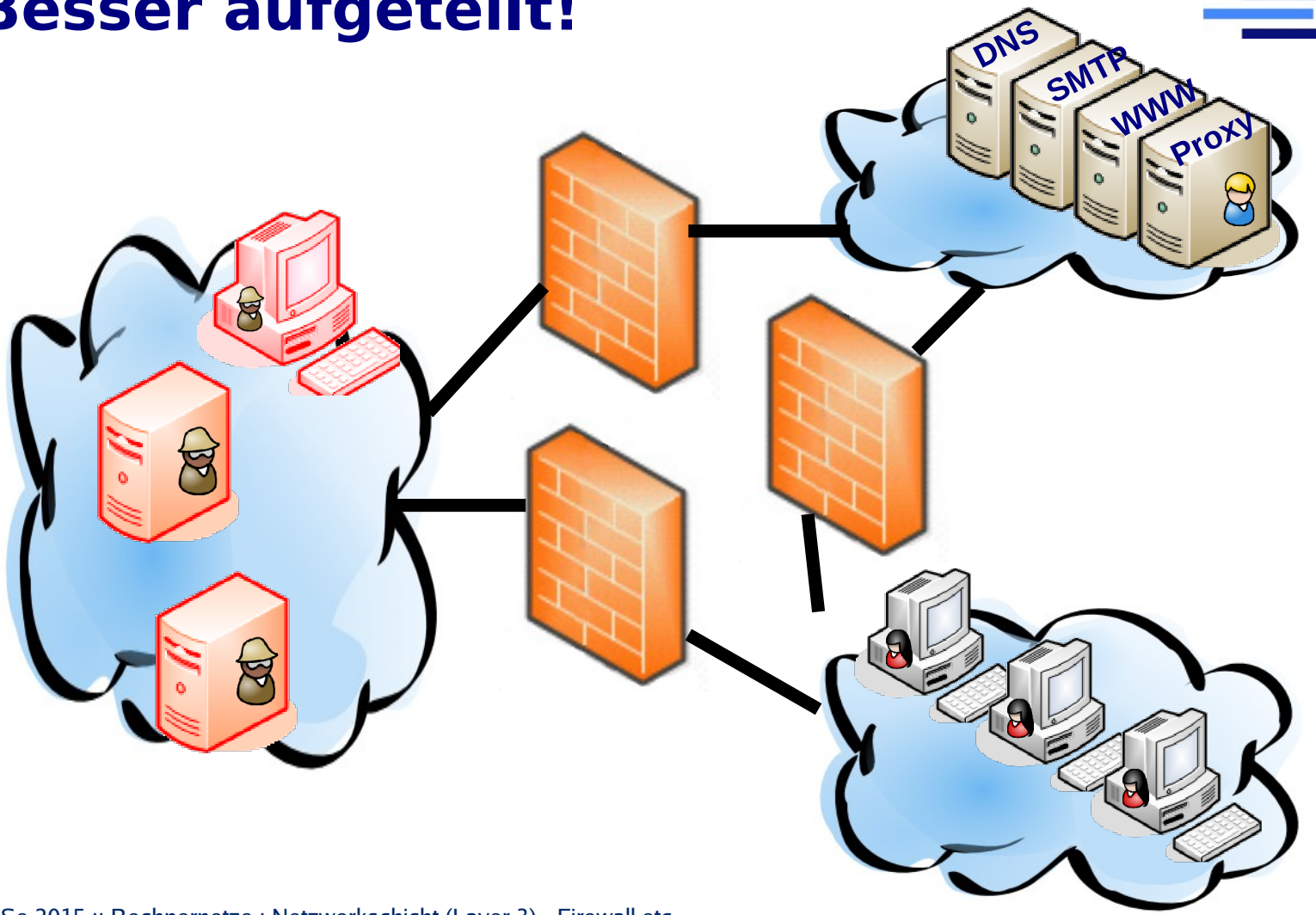
Proxy-Server für Firewalls / URL Checker

- **Kommerzielle URL-Checker verwenden oft eine herstellerspezifische Datenbank**
- **Übliche Probleme:**
  - URLs sind extrem flexibel
  - Pflege eigener Datenbanken ist zu aufwendig und teuer, außerdem fehleranfällig bzw. nicht vollständig
  - Was qualifiziert eine URL dafür, in die „schwarze Liste“ aufgenommen zu werden?

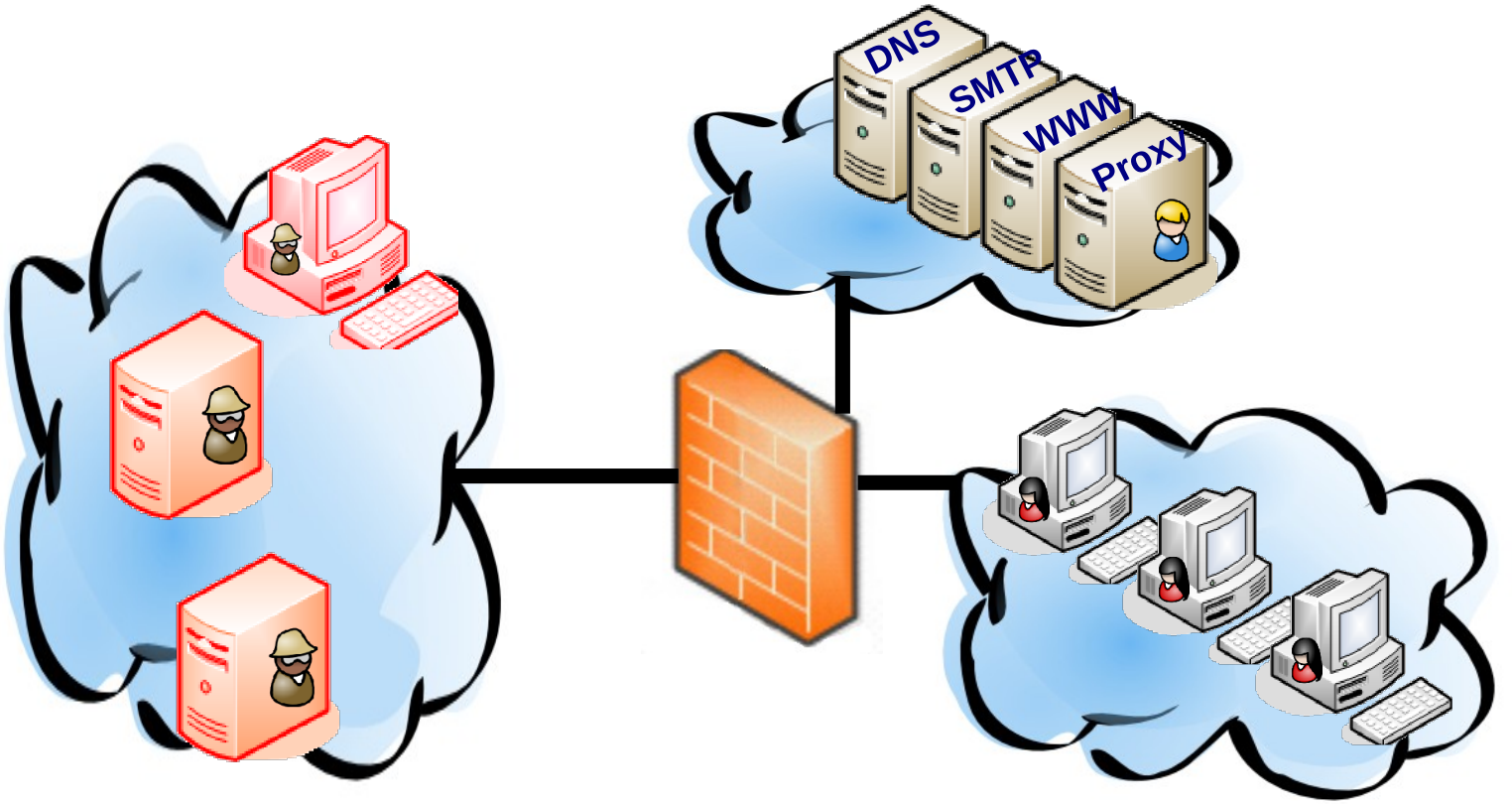
Bestimmte Probleme bleiben: Prinzip der geringsten Berechtigung

- Solange Server extern erreichbar sind, kann der Angreifer mit einem Streich „drinnen“ sein
- ~~Solange Endgeräte direkt ins – unsichere – Internet dürfen, sind diese auch direkt betroffen~~
- Proxies stehen immer noch im internen Netz und kommunizieren mit „extern“
- Solange intern und extern angebotene Dienste den gleichen Server benutzen, ist eine Absicherung schwieriger

Besser aufgeteilt!

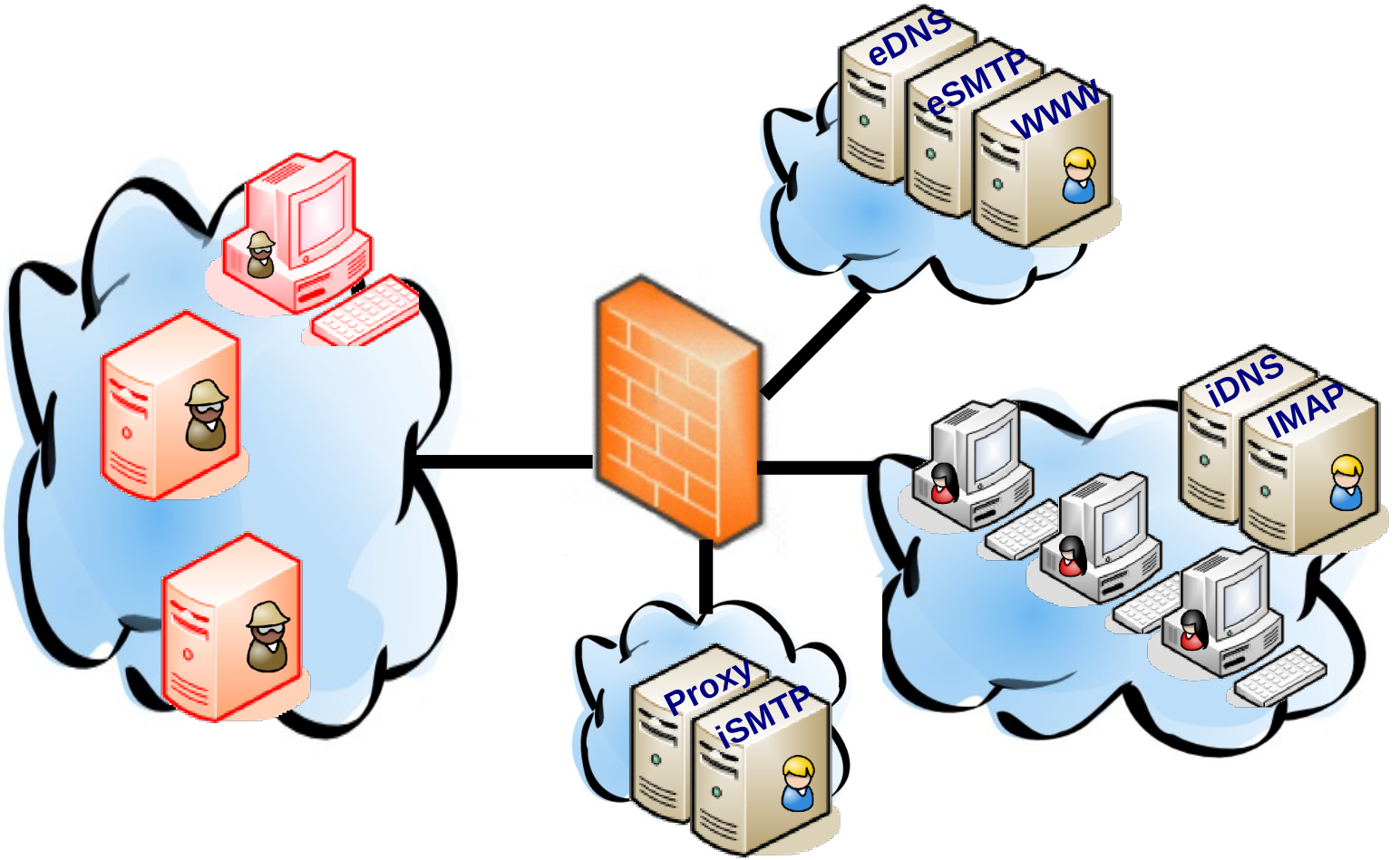


Übliche Option: Schaffung einer DMZ



Hat nichts mit Militär zu tun, ist aber nun mal der Begriff: De-Militarisierte Zone

Es geht noch besser: Verkehrsflüsse auftrennen



Schaffung der DMZ

… zunächst einmal der Proxy und ausgehende SMTP-Verbindungen – incl. Admin (22/tcp=ssh)

No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
1	proxy	OUT	TCP	> 1023	21	syn	ACCEPT
2	proxy	OUT	TCP	> 1023	80	syn	ACCEPT
3	proxy	OUT	TCP	> 1023	443	syn	ACCEPT
4	proxy	OUT	UDP	> 1023	53	any	ACCEPT
5	LAN	proxy	TCP	> 1023	21	syn	ACCEPT
6	LAN	proxy	TCP	> 1023	80	syn	ACCEPT
7	LAN	proxy	TCP	> 1023	443	syn	ACCEPT
8	iSMTP	OUT	TCP	> 1023	25	syn	ACCEPT
9	LAN	iSMTP	TCP	> 1023	25	syn	ACCEPT
10	LAN	proxy	TCP	> 1023	22	syn	ACCEPT
11	LAN	iSMTP	TCP	> 1023	22	syn	ACCEPT

Schaffung der DMZ (2)

… und jetzt die von außen zugänglichen Servern – aus dem LAN nur Admin (22/tcp=ssh)

No	Source	Dest	Prot	SrcPort	DstPort	Flags	Action
12	OUT	eSMTP	TCP	>1023	25	syn	ACCEPT
13	OUT	eDNS	TCP	>1023	53	syn	ACCEPT
14	OUT	eDNS	UDP	>1023	53	any	ACCEPT
15	OUT	www srv	TCP	>1023	80	syn	ACCEPT
16	OUT	www srv	TCP	>1023	443	syn	ACCEPT
17	eSMTP	OUT	UDP	>1023	53	any	ACCEPT
18	www srv	OUT	UDP	>1023	53	any	ACCEPT
19	eSMTP	imap srv	TCP	>1023	25	syn	ACCEPT
20	LAN	eDNS	TCP	>1023	22	syn	ACCEPT
21	LAN	eSMTP	TCP	>1023	22	syn	ACCEPT
22	LAN	www srv	TCP	>1023	22	syn	ACCEPT
23	*	*	any	any	any	any	DROP

FAQ zur DMZ-Konfiguration

1. Warum braucht der iDNS keine externen Verbindungen?

- Alle internen Rechnernamen und IP-Adressen werden ohne externe Referenzen gepflegt bzw. konfiguriert
- Alle Systeme der DMZ, die nach außen kommunizieren, erhalten DNS-Informationen vom ISP

2. Warum gibt es aus dem LAN erlaubte Verbindungen via 22/tcp?

- Sicherer Zugang für Administratoren

FAQ zur DMZ-Konfiguration (2)

3. Wie werden Web-Seiten in der DMZ gepflegt?

- Man betreibt z.B. ein CMS und überträgt die erzeugten Seiten per SSH in die DMZ
  - … oder öffnet einen designierten Port ...

4. Was fehlt noch in der Konfiguration?

- Interne Meldungen werden üblicherweise per SMTP aus der DMZ gesendet
- DMZ-Systeme müssen Systemmeldungen weitergeben, z.B. mit syslog (601/udp)
  - … aber vorsicht, weil verbindungslos!

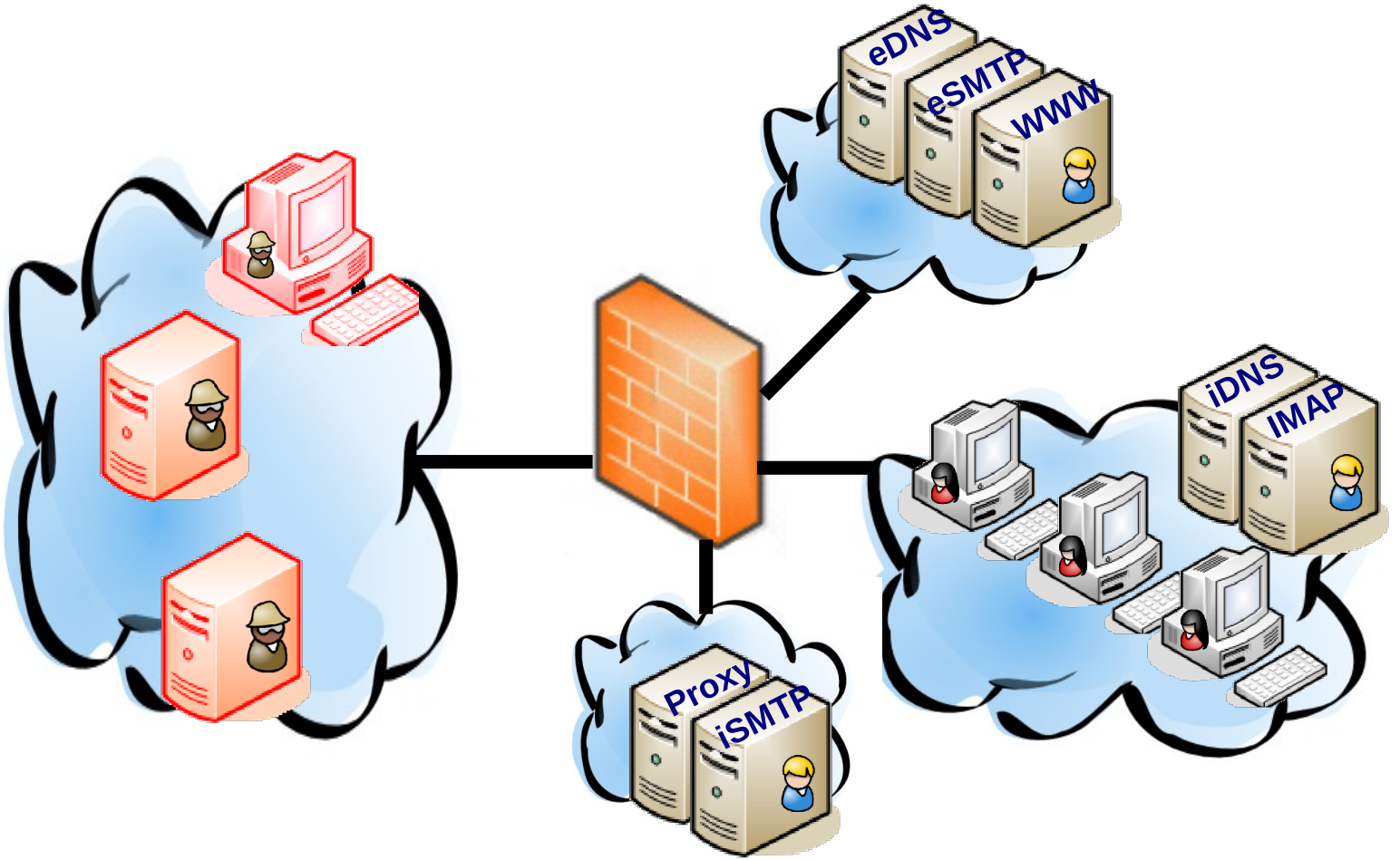
FAQ zur DMZ-Konfiguration (3)

5. Kann ich noch mehr Angriffe abwehren?

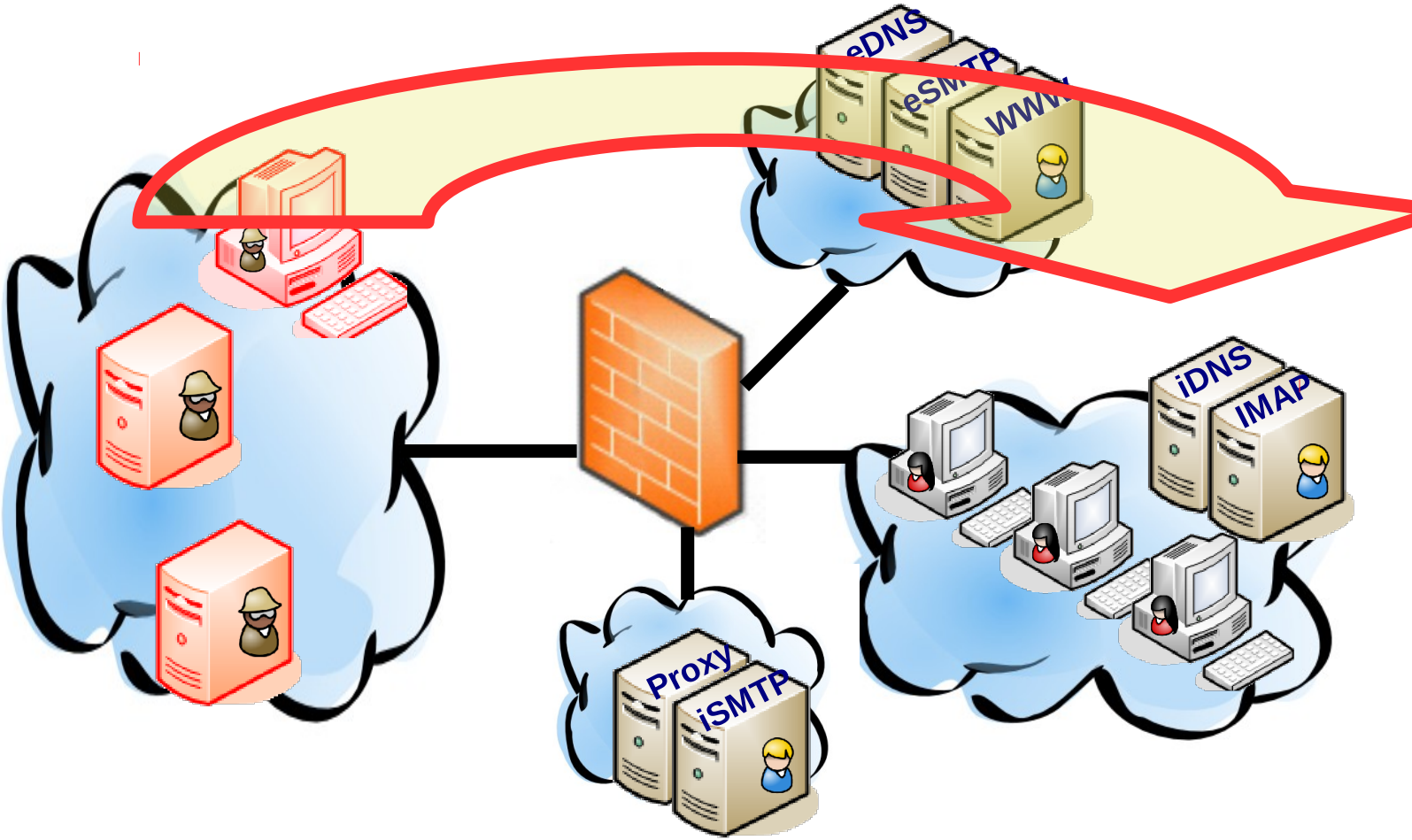
- Immer! Gefälschte Pakete mit internen IP-Adressen könnten gesondert behandelt werden
  (Anti-Spoofing-Filter)
- Unbekannte bzw. nicht verwendete Protokolle gesondert behandeln

Im Moment reicht die DROP-Regel!

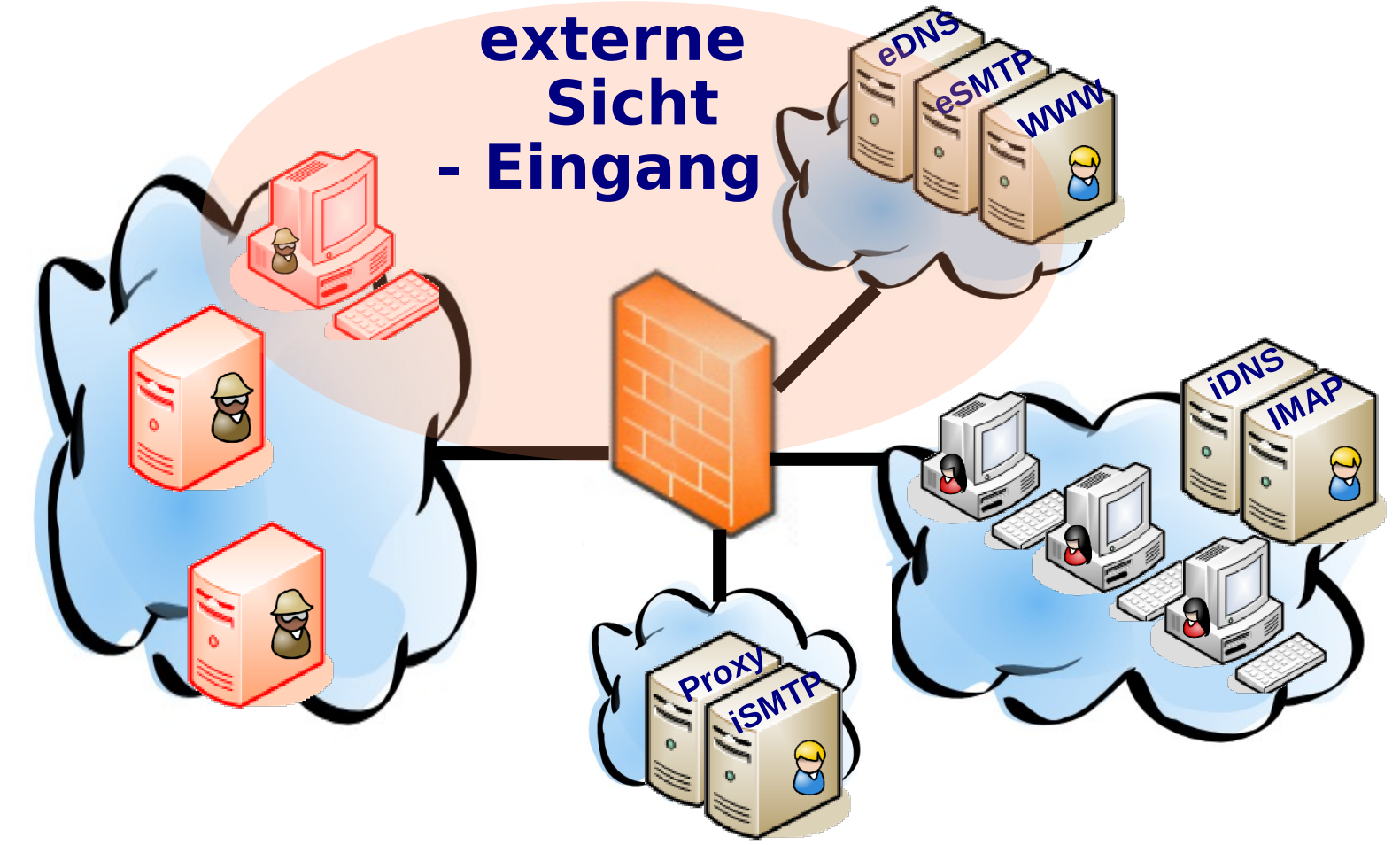
Warum zwei SMTP-Server? Verkehrsflüsse auftrennen



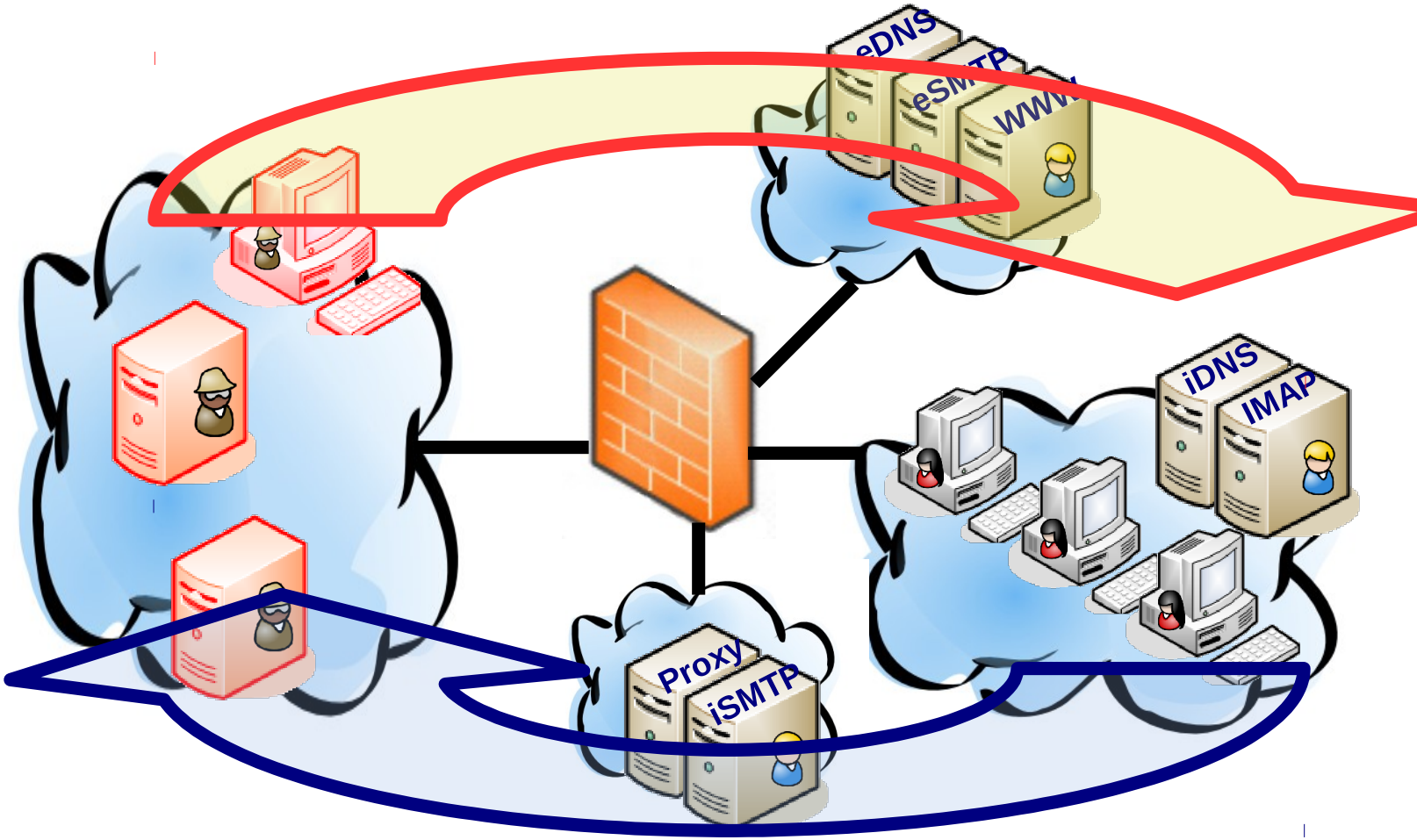
Warum zwei SMTP-Server? Verkehrsflüsse auftrennen



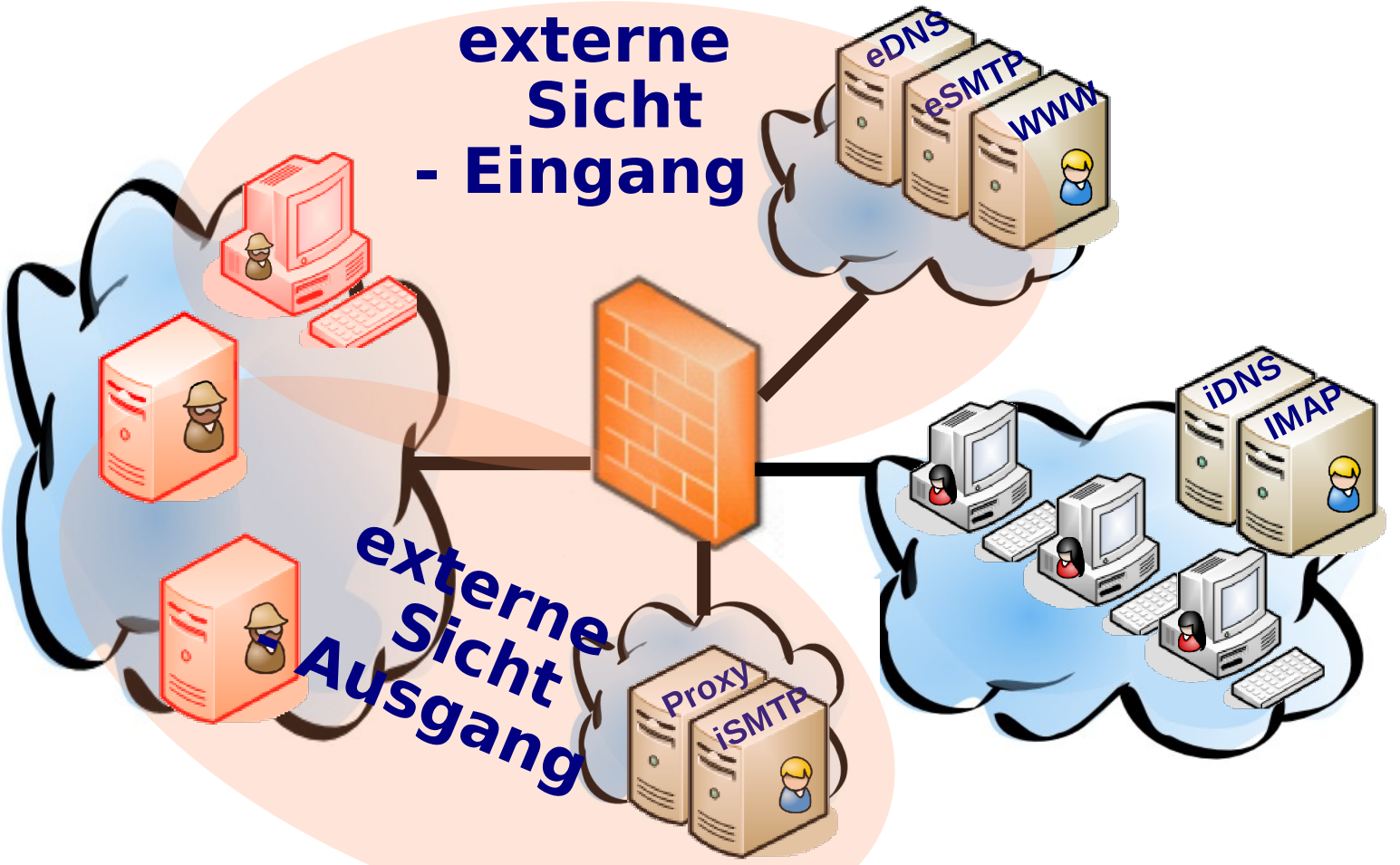
Warum zwei DNS-Server? Sichtweisen auftrennen



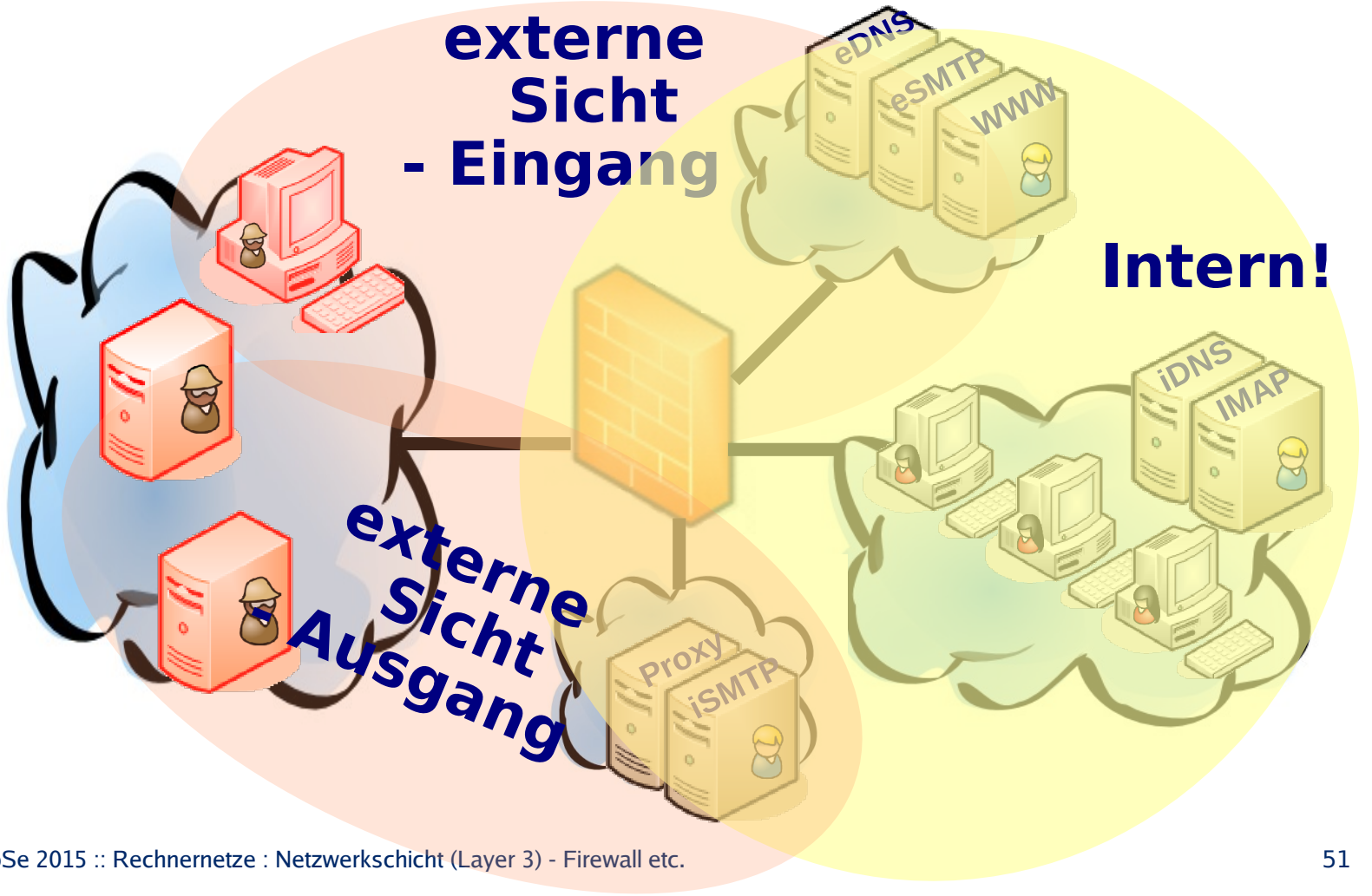
Warum zwei SMTP-Server? Verkehrsflüsse auftrennen



Warum zwei DNS-Server? Sichtweisen auftrennen



Warum zwei DNS-Server?
Sichtweisen auftrennen



Interne Adressen gut versteckt!

Network Address Translation (NAT) war ja eine Möglichkeit

- **Lokale IP-Adressen werden durch zugewiesene IP-Adresse des ISPs abgebildet**
- **Eingehende Verbindungen direkt an Endgeräte ist nicht möglich**
  - jedenfalls nicht bei korrekter Konfiguration
- **Alle ausgehenden Pakete werden umgeschrieben:**
  - Sender-IP, Sender-Port, Checksum, ...

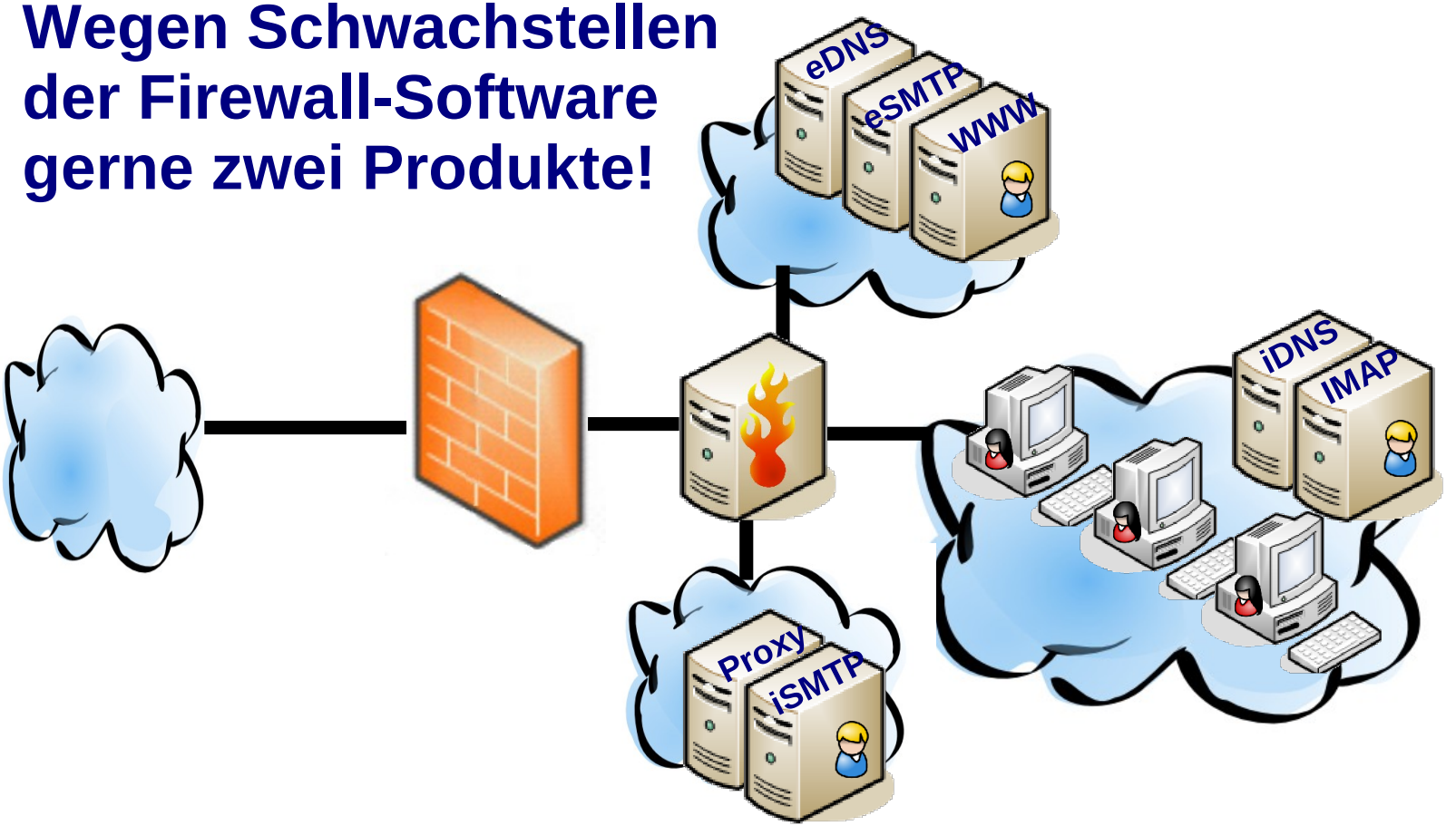
Interne Adressen zu gut versteckt!

Stellen Sie sich vor, in Ihrem LAN hinter Network Address Translation (NAT) ist eine Malware aktiv

- **Sie bekommen von vielen CERTs sinnvolle Hinweise, dass Ihr Netz kompromittiert ist**
- **Nur, die IP-Adresse hilft Ihnen nicht weiter**
- **Jedenfalls nicht, wenn Sie nicht die ganzen Umschreibungen mitprotokolliert haben**
  - Zeitstempel allein reicht nicht, unbedingt die Portangaben mitloggen!

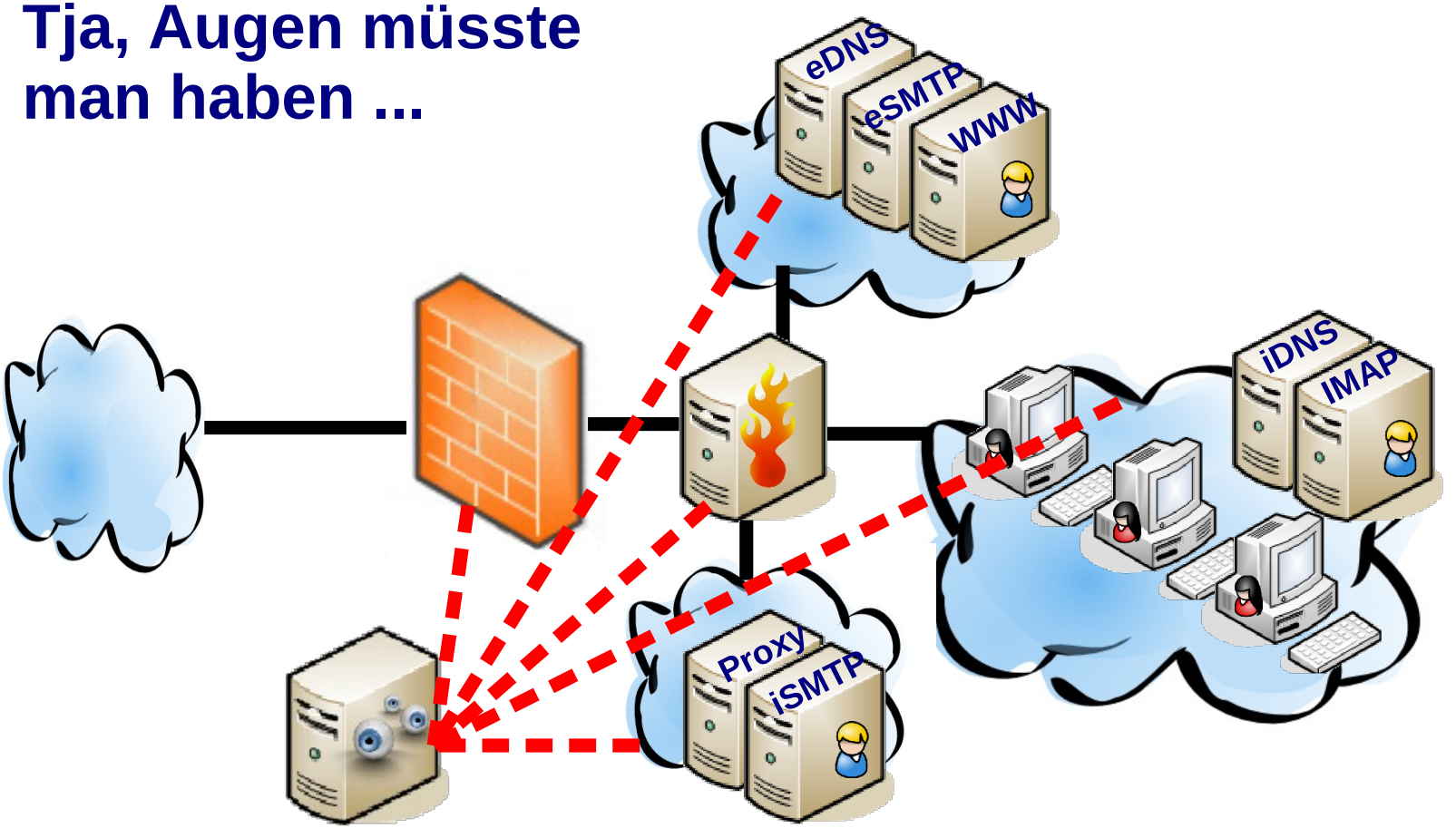
Bekommen wir das noch sicherer?

Wegen Schwachstellen der Firewall-Software gerne zwei Produkte!



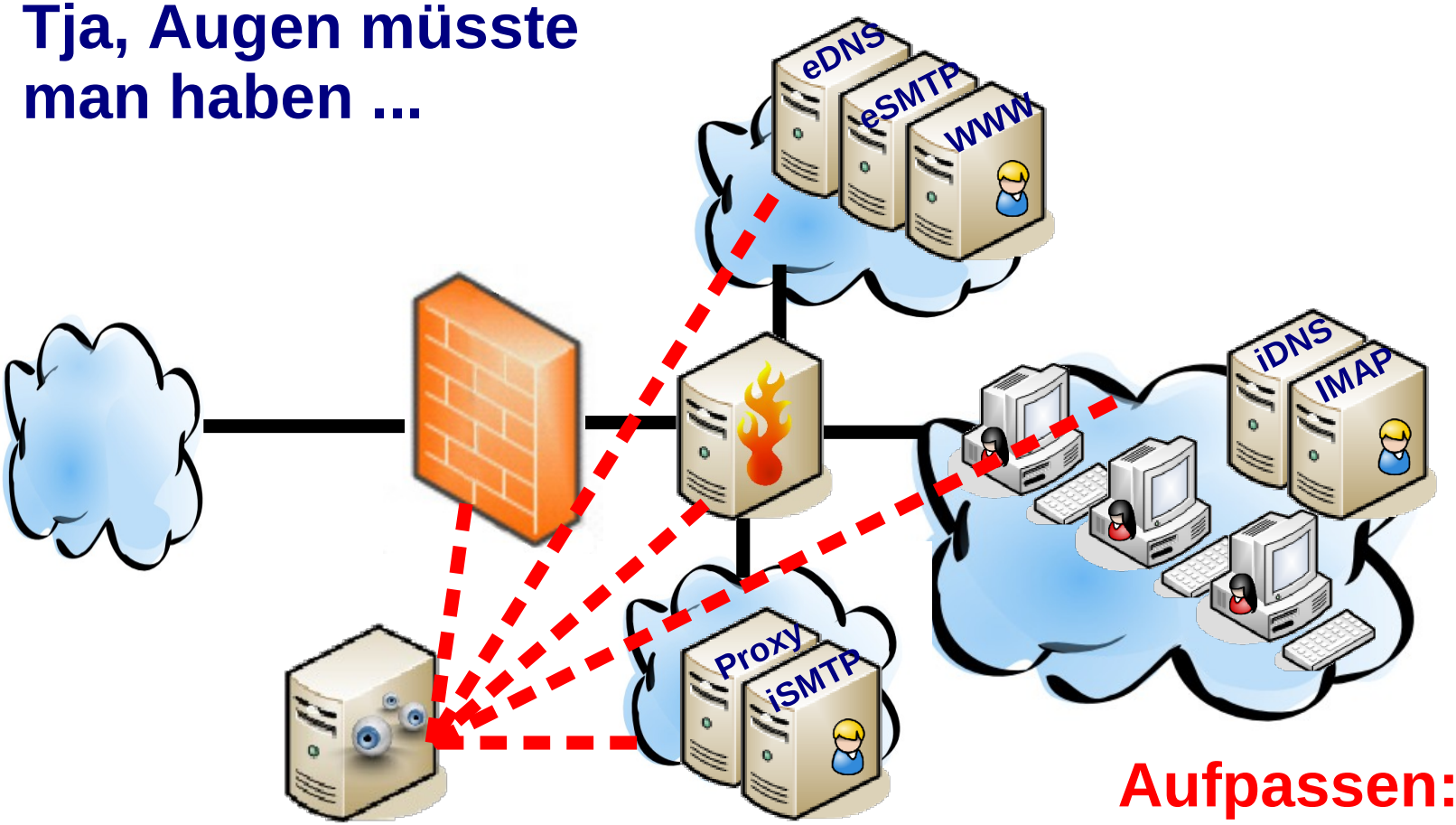
Wie kontrollieren wir die Firewall?

Tja, Augen müsste man haben ...



Wie kontrollieren wir die Firewall?

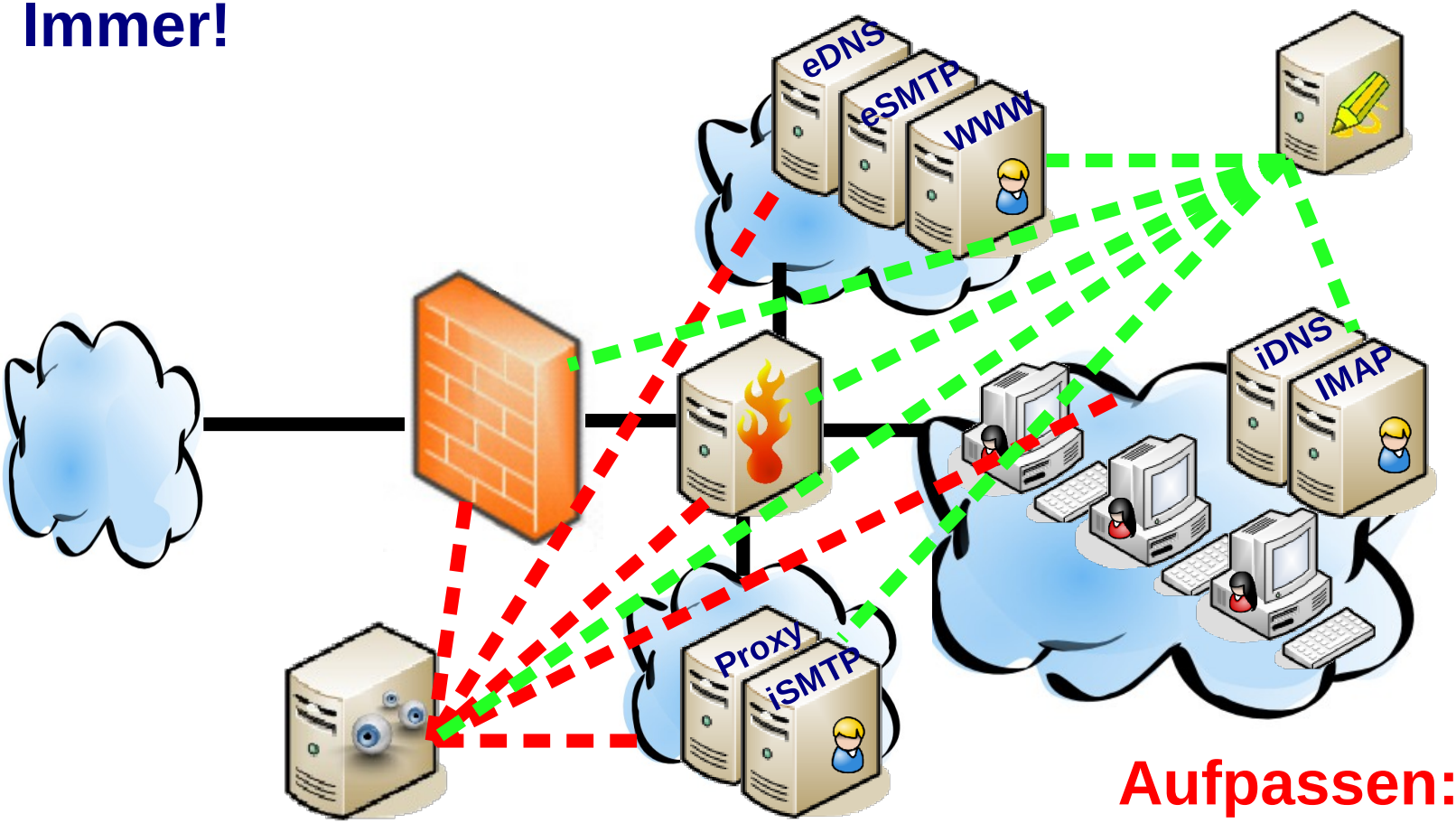
Tja, Augen müsste man haben ...



Aufpassen: Schafft neue Probleme!

Geht noch mehr?

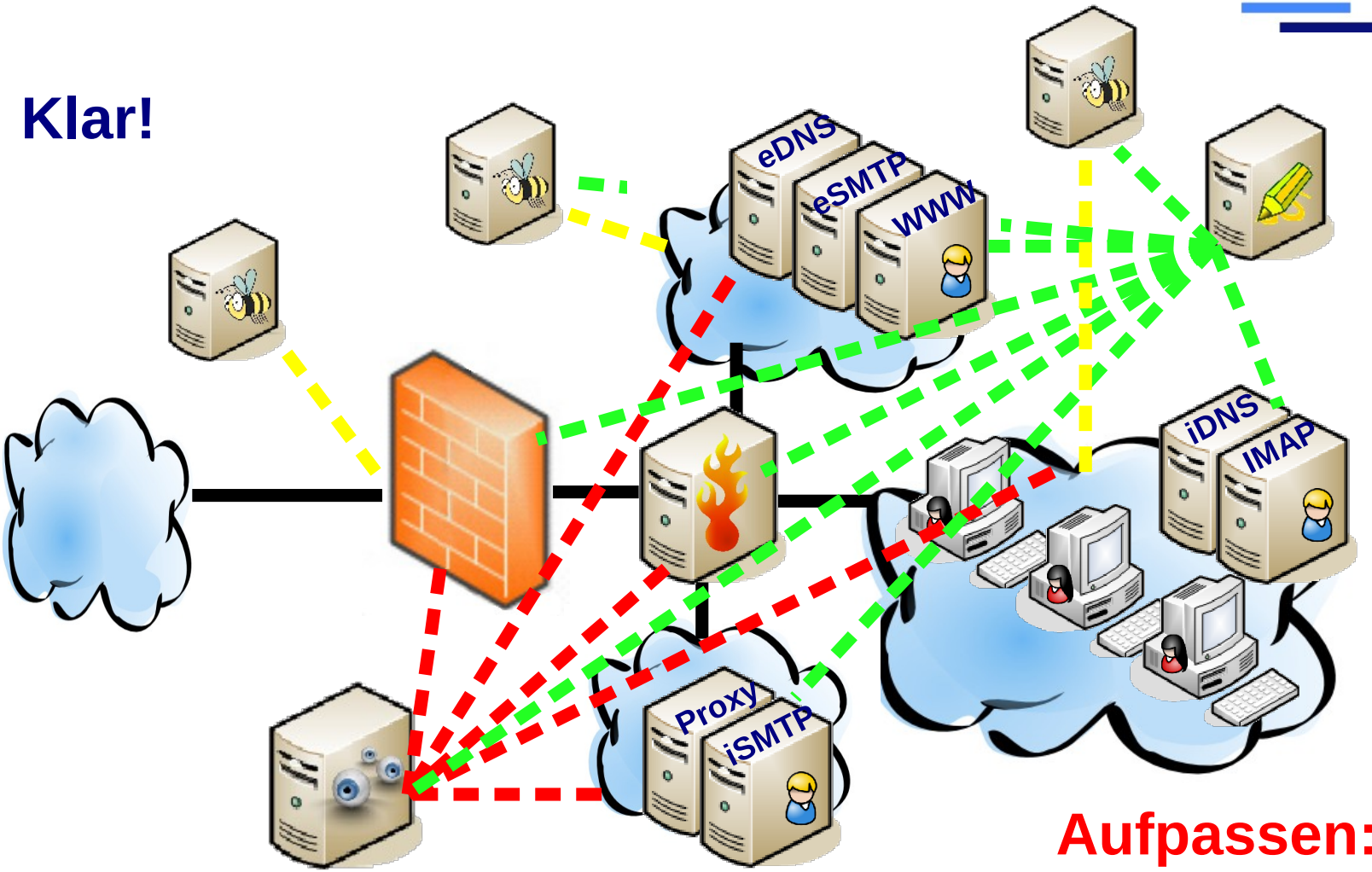
Immer!



Aufpassen: Schafft neue Probleme!

Noch mehr?

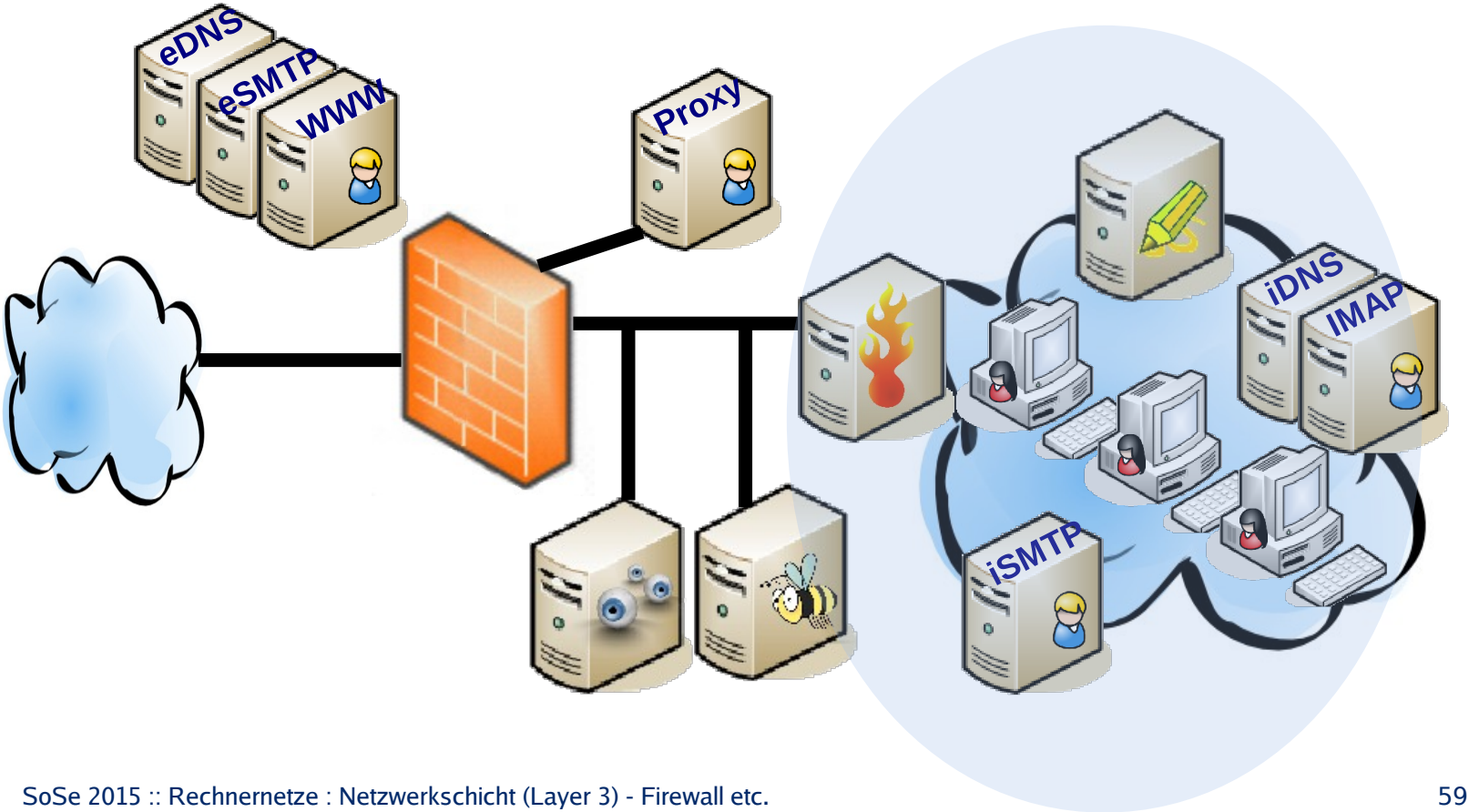
Klar!



Aufpassen:
Schafft neue Probleme!

Aber es ging doch um K.I.S.S.?

Einige Systeme kann prima der ISP betreiben!



Offene Probleme trotz Firewall?

- **Erlaubte Kommunikation ist immer noch**
  - Unverschlüsselt
  - Fälschbar
- **DNS- und Routing-Informationen sind immer angreifbar**
- **Denial-of-Service-Angriffe sind immer möglich**
  - Viele kleine Pakete → TCP SYN Flood
  - Viele große Pakete → UDP Flood
  - Viele große Pakete von „guten“ Servern → Reflecting amplification DoS Attacks

Kontakt

Prof. Dr. Klaus-Peter Kossakowski

Email: klaus-peter.kossakowski@haw-hamburg.de

Mobil: +49 171 5767010

https://users.informatik.haw-hamburg.de/~kpk/