Praktische Netzwerksicherheit: (1) Firewalls

Prof. Dr. Klaus-Peter Kossakowski

Praktische Netzwerksicherheit: (1) Firewalls

M.Sc. Andrej Zieger

Prof. Dr. Klaus-Peter K[redacted]wski

Inhalte dieses Kapitels

- Elementare Komponenten von Netzen
- Rolle und Aufgabe von Firewalls
  - Elementarste Methode zur Separierung
  - Gezielte Beschränkung der Kommunikation
- Beispiel Firewall-Architektur
  - Schrittweise Entwicklung
  - kleines lokales Netzwerk

Ziele dieses Kapitels

Sie kennen/können erläutern:

- typische Komponenten der Netzwerksicherheit
- Konzept einer Firewall auf Ebene der Netzwerk-/Transportschicht
- => anhand IP, UDP und TCP
- Prinzip der geringsten Berechtigungen
- => anwenden auf Kommunikation im Netzwerk (lokal und Internet)
- => Ableitung einer Firewall-Architektur

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

Architektur Komponenten

Bausteine eines sicheren Netzwerkes

- Firewall
- IDS
- Network Monitoring
- Honeypot
- Log-Server

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**
  - Prinzip der geringsten Berechtigung
  - Zugriffskontrolle auf der Netzwerkschicht
    + evtl. Daten der Transportschicht
- **Eine Firewall**
  - Ersetzt keine Maßnahmen zur Vertraulichkeit der Übertragung oder Manipulationsfreiheit
  - Hat evtl. Schwierigkeiten mit Verschlüsselung

Definition: Network IDS

- **Ein Network IDS**
  - heißt Intrusion Detection System
  - ist eine Architekturkomponente
  - wichtig in Netzwerken mit höheren Sicherheitsanforderungen
  - kann unter Umständen sehr viele Ereignisse aufgezeichnen / eskalieren
  - => erfordert somit unbedingt Analyse und Tuning der Maßnahmen!
  - fokussiert meist auf Signaturen

Definition: Network IDS (2)

- **Ein NIDS**
  - als dedizierte Komponente
  - Implementiert das Prinzip der Verteidigung in der Tiefe
  - überwacht u.A. die Funktion einer Firewall
  - erkennt Angriffe Hilfe von diversen Daten
    - evtl. werden die sogar korreliert
- **Ein NIDS ersetzt keine Firewall!**
- **Verschlüsselung macht es der NIDS schwer**

Definition: Host IDS

- **Ein HIDS**
  - wirkt pro Host
  - implementiert Prinzip der Verteidigung in der Tiefe
  - überwacht u.A. die Funktion einer Anwendung
  - erkennt Angriffe Hilfe von diverser lokaler Daten
    - die auf Anwendungsebene nicht erst zusammengebaut werden müssen
- **Ein HIDS ersetzt keine Firewall**
  - ist aber effektiver als NIDS
- **Verschlüsselung ist kein Thema**

Definition: Network Monitoring

- **Network Monitoring**
  - ist meist eine Kombination verschiedener Tools
  - incl. NIDS, weniger konzentriert auf Signaturen
  - Benötigen ebenfalls Auswertung und Feintuning
  - ist häufig konsequenter und nachhaltiger, durch ganzheitliche Wirkung
- **Ein Network Monitoring ersetzt keine Firewall!**

Definition: Network Monitoring

- **Network Monitoring**
  - ist meist eine Kombination verschiedener Tools
  - incl. NIDS, weniger konzentriert auf Signaturen
  - Benötigen ebenfalls Auswertung und Feintuning
  - ist häufig konsequenter und nachhaltiger, durch ganzheitliche Wirkung
- **Ein Network Monitoring ersetzt keine Firewall!**

Definition: Honeypot

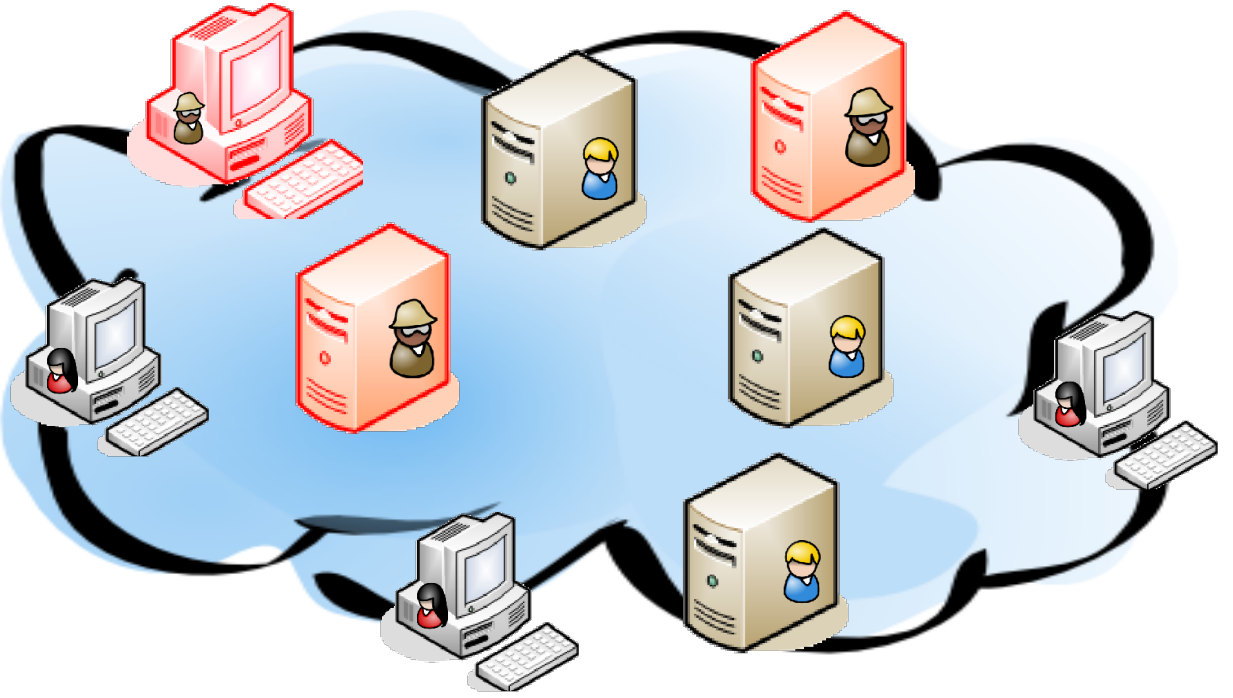
- **Ein Honeypot**
  - ist eine Architekturkomponente
  - explizit verwundbare Systeme
  - ist im Betrieb sehr aufwändig
    => es ist Vorsicht geboten, aber …
  - kann laterale Bewegungen von Angreifern im eigenen LAN aufdecken
  - … und außerdem Viren, Würmer und Trojaner
- **Ersetzt weder Firewall noch IDS!**

Definition: Log-Server

- **Ein Log-Server**
  - ist eine Architekturkomponente
  - ist quasi Pflicht
  - Sammelt Daten / Logs
    - Sinnfrei ohne Auswertung!
- **Ermöglicht Forensik!**
  - enthält Daten erfolgreicher Angriffe
  - enthält Spuren zu Herkunft
  - enthält Spuren durchgeführter Aktionen
  - Braucht seinerseits selbst Schutz

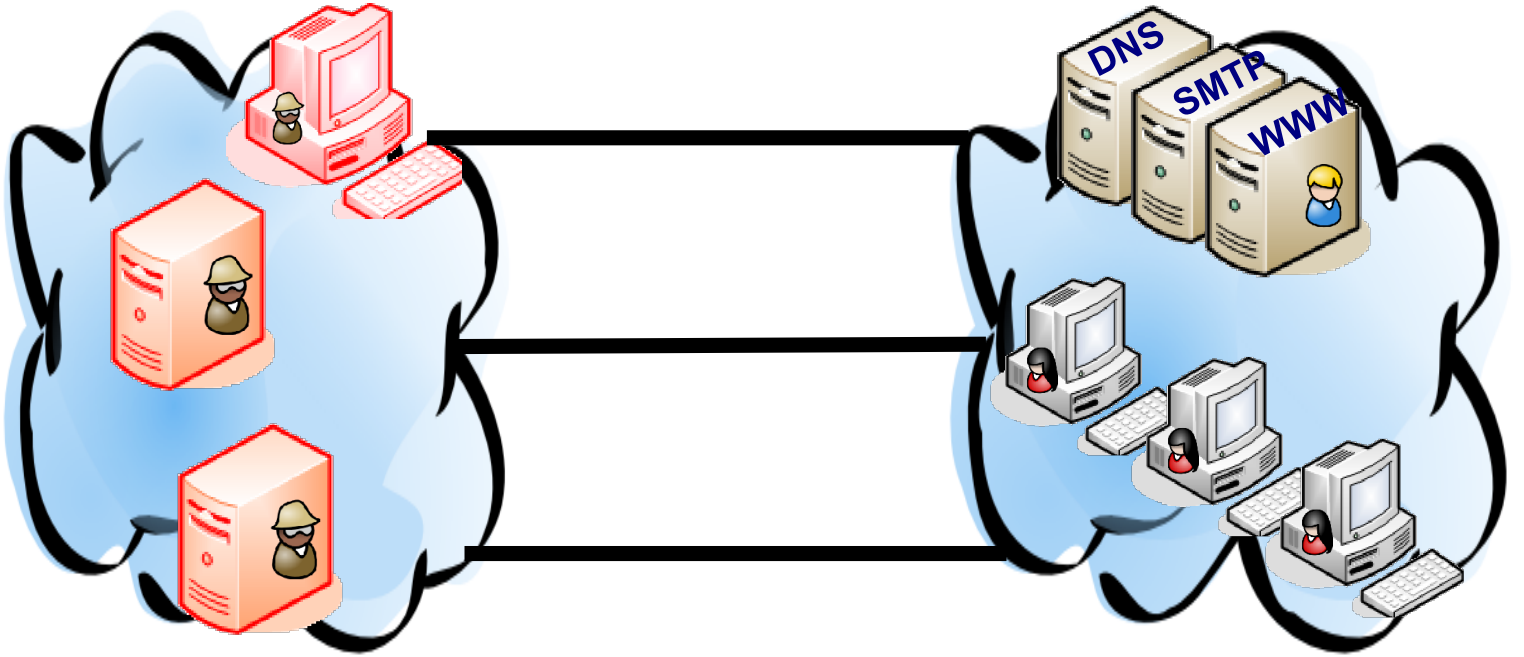
Am Anfang war ein Netz ...

Alles, jeder, überall ..., egal !



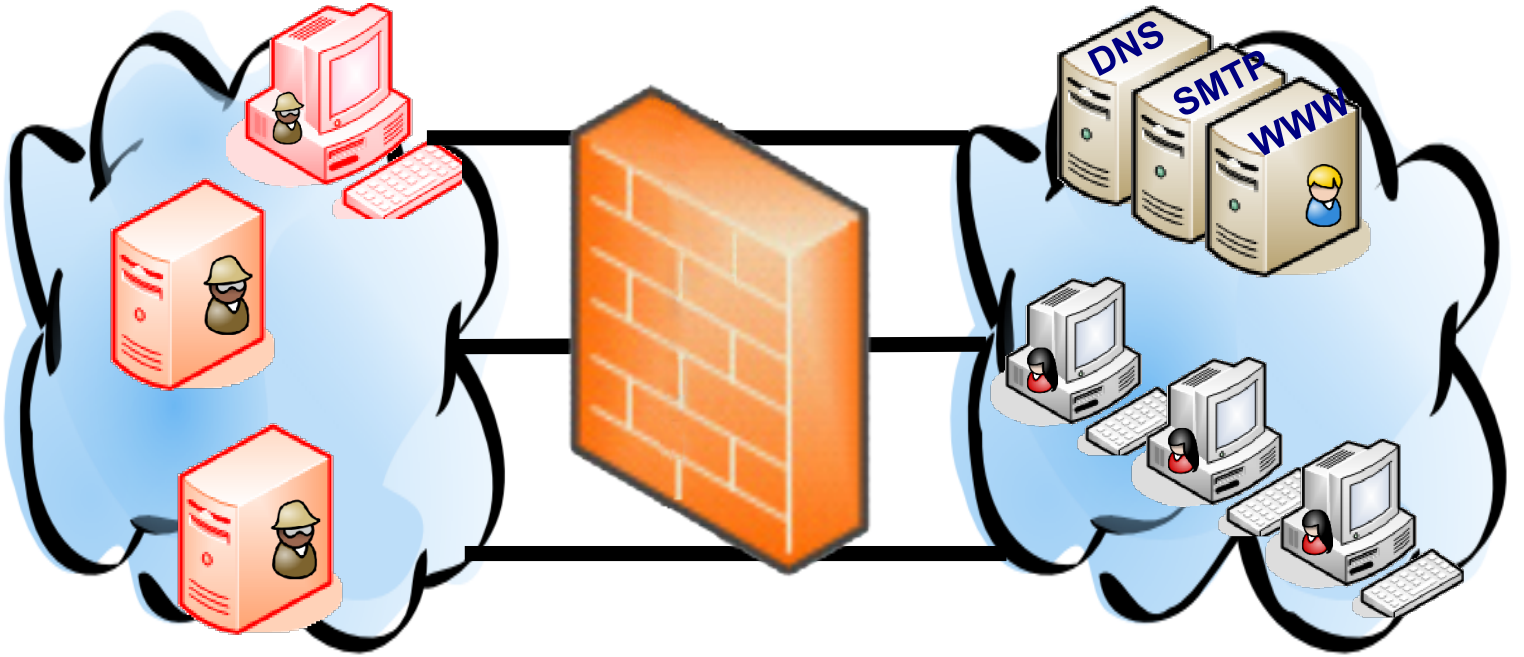
Aufteilung von Netzen

„Separation of Concerns“



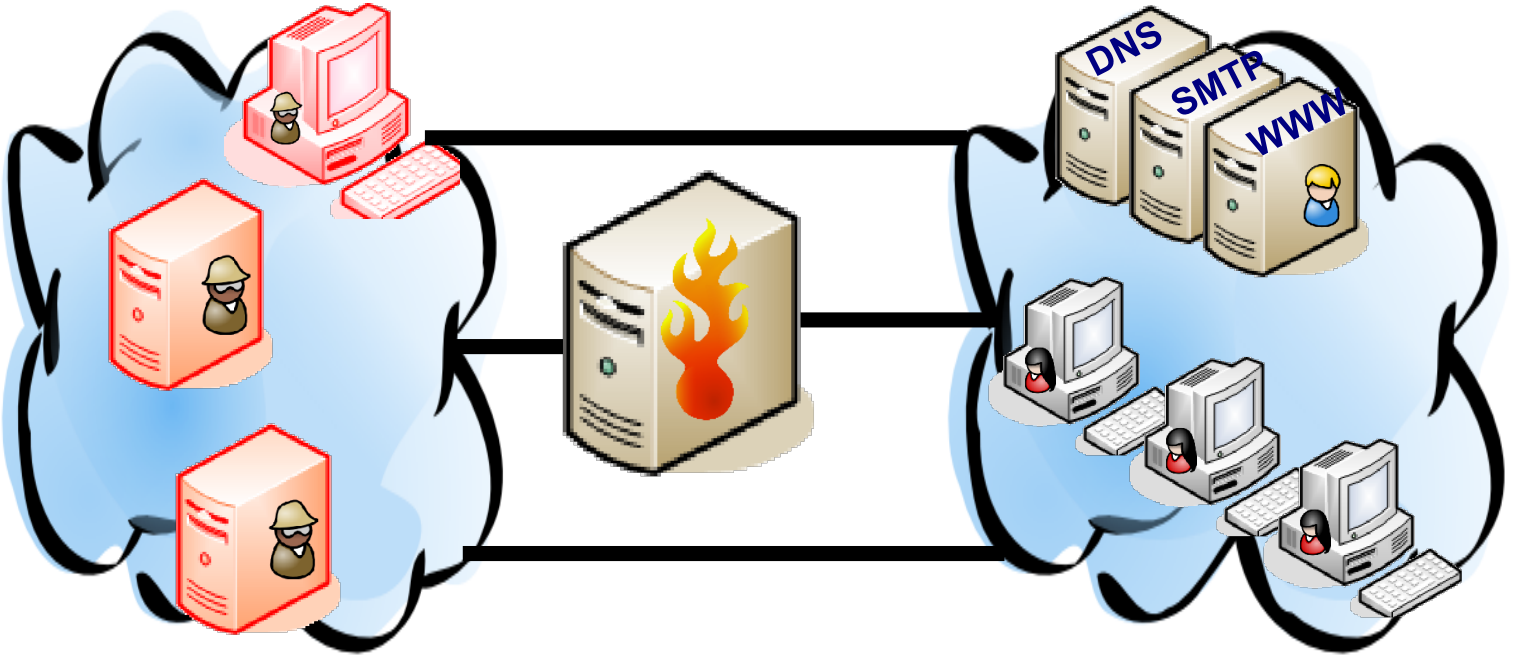
Aufteilung von Netzen (2)

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



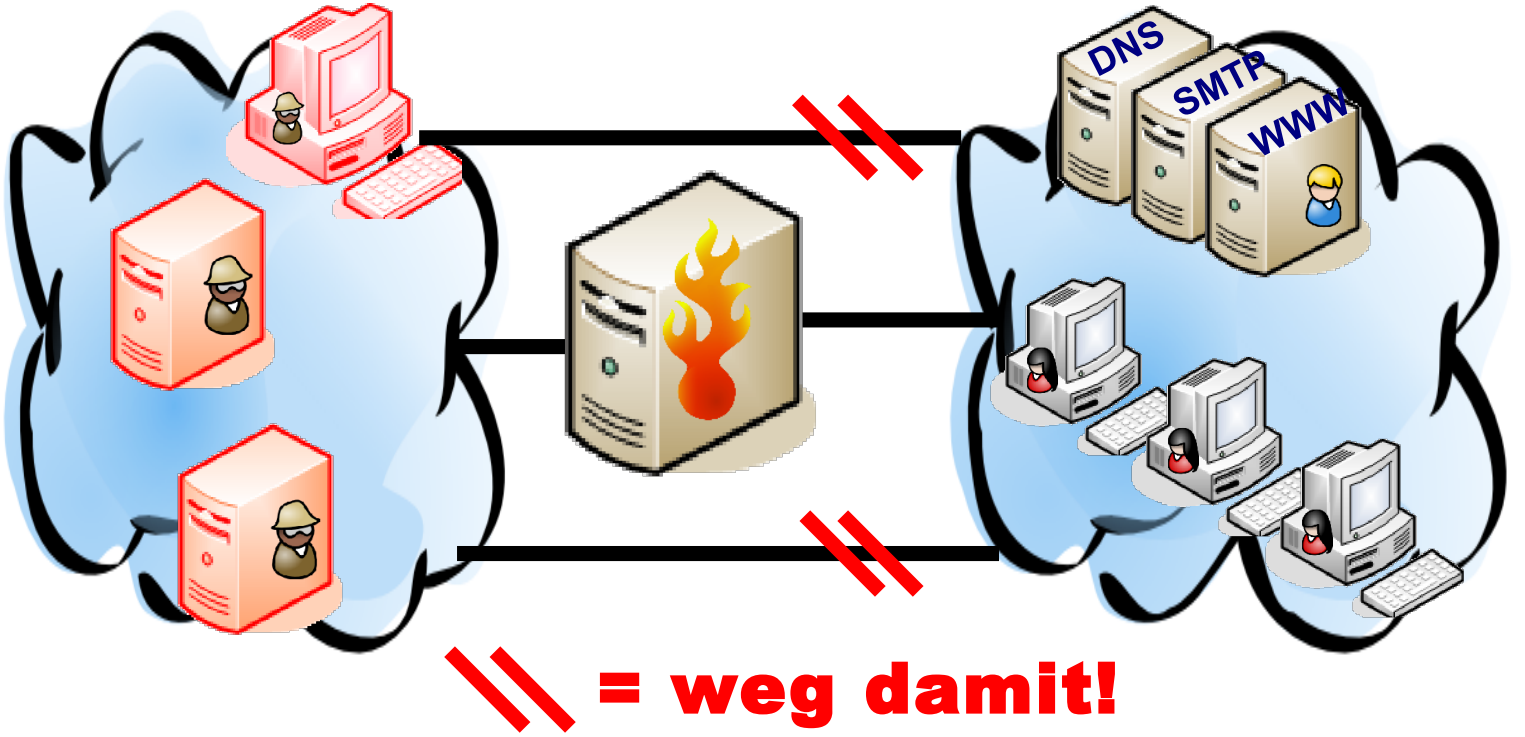
Aufteilung von Netzen (3)

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



Aufteilung von Netzen (4)

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



Separieren von Netzen

- **Aufteilung von Netzen**
  == Filterung von Paketen
- **Firewalls arbeiten üblicherweise auf**
  - Layer 3: Netzwerkschicht, d.h. IP / ICMP
  - Layer 4: Transportschicht, d.h. UDP / TCP
  - was nicht verstanden, wird verworfen!
- **Selbst mögliche Quelle für**
  - Verzögerung
  - zusätzliche Fehler

Die älteste Form: Packet Screens

- **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)

- **Logischer Zusammenhang analysiert**
  - Ohne Verbindung (SYN), keine „Antwort“
  - Ohne Bestätigung (SYN/ACK) nichts anderes
  - Ohne Client-Handshake, keine Kommunikation!
- **Filterregeln auf „Lebenszyklus“ erweitert**
  - Nach Handshake werden alle Daten erlaubt
  - TCP-Sequence-Numbers werden überprüft
- **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

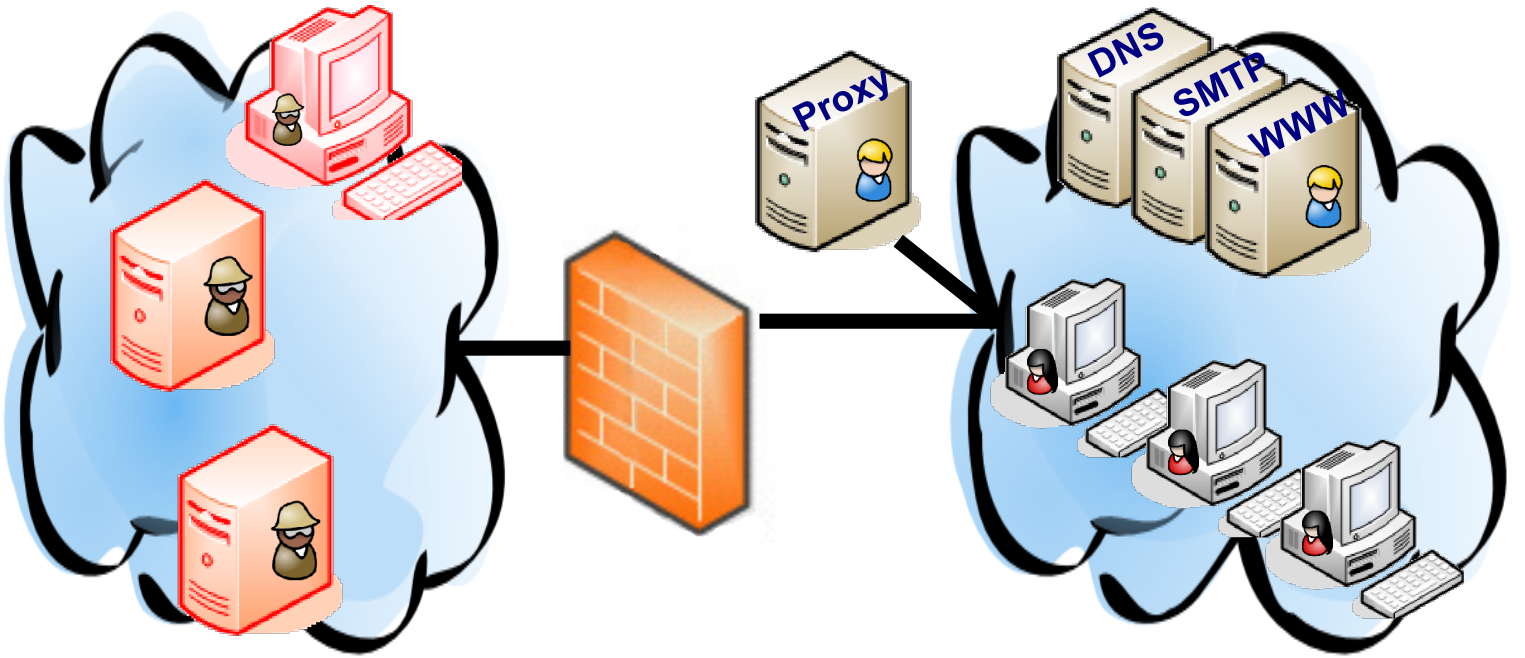
- **Extern erreichbare Systeme**

Bestimmte Probleme bleiben:

- **Server extern erreichbar**
  - Angreifer mit einem Streich „drinnen“
- **Endgeräte direkt ins – unsichere – Internet**
  - Clients als unbewusste „Türöffner“
- **intern und extern Dienste auf einem Server**
  - erschwert Absicherung

Prinzip der geringsten Berechtigung!

Einführung von Proxy-Servern



Einführung von Proxy-Servern(2)

- **Ein Proxy**
  - leitet Anfragen & Antworten weiter
  - muss Formate & Protokolle beherrschen
  - analysiert Verkehr in Echtzeit
  - reglementiert auf Anwendungsebene
- **Proxies nicht auf Routern realisieren**
  - Da evtl. Schwachstellen vorhanden
  - Routing wichtiger als Proxy-Verkehr
  - Proxy-DoS einfacher als Router-DoS

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, Flash, Silverlight….
- **Filterung von Cookies**
- **Sehr aufwändig,**
  - alle Aspekte des Protokolls implementiert
  - Wenn das Protokoll zu komplex/mächtig ist, gibt es meist Probleme ...

Proxy-Server für Firewalls / Virus Filter

- **„Scannen“ erfordert Vorarbeiten**
  - Entpacken, Typ-Erkennung, PreLoaders?
- **Übliche Probleme:**
  - Kodierungs-Zoo: 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

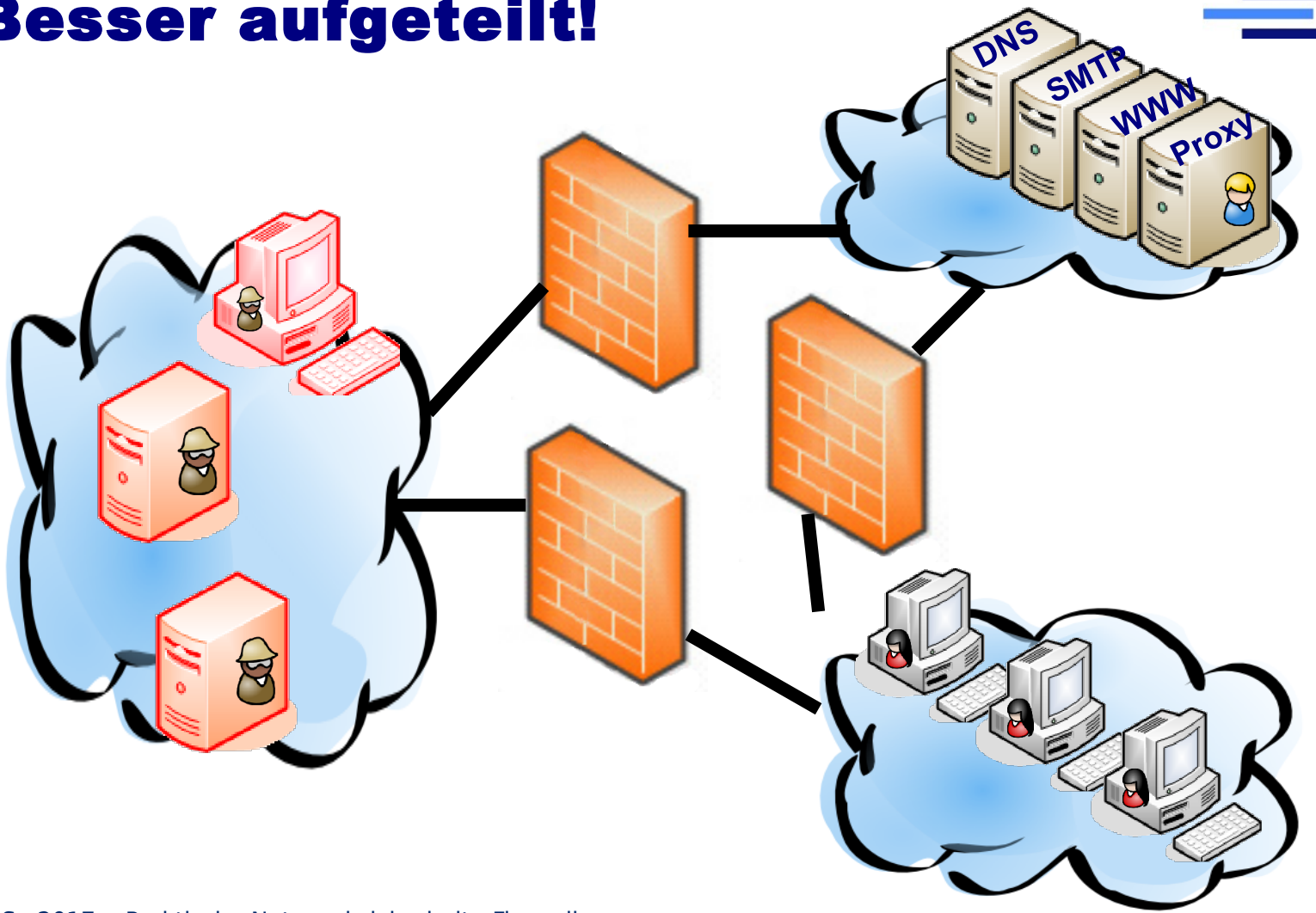
- **Kommerzielle URL-Checker verwenden oft eine herstellerspezifische Datenbank**
- **Übliche Probleme:**
  - URLs sind extrem flexibel
  - Pflege eigener Datenbanken ist zu aufwendig und teuer, außerdem fehleranfällig bzw. nicht vollständig
  - Was qualifiziert eine URL dafür, in die „schwarze Liste“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

Bestimmte Probleme bleiben:

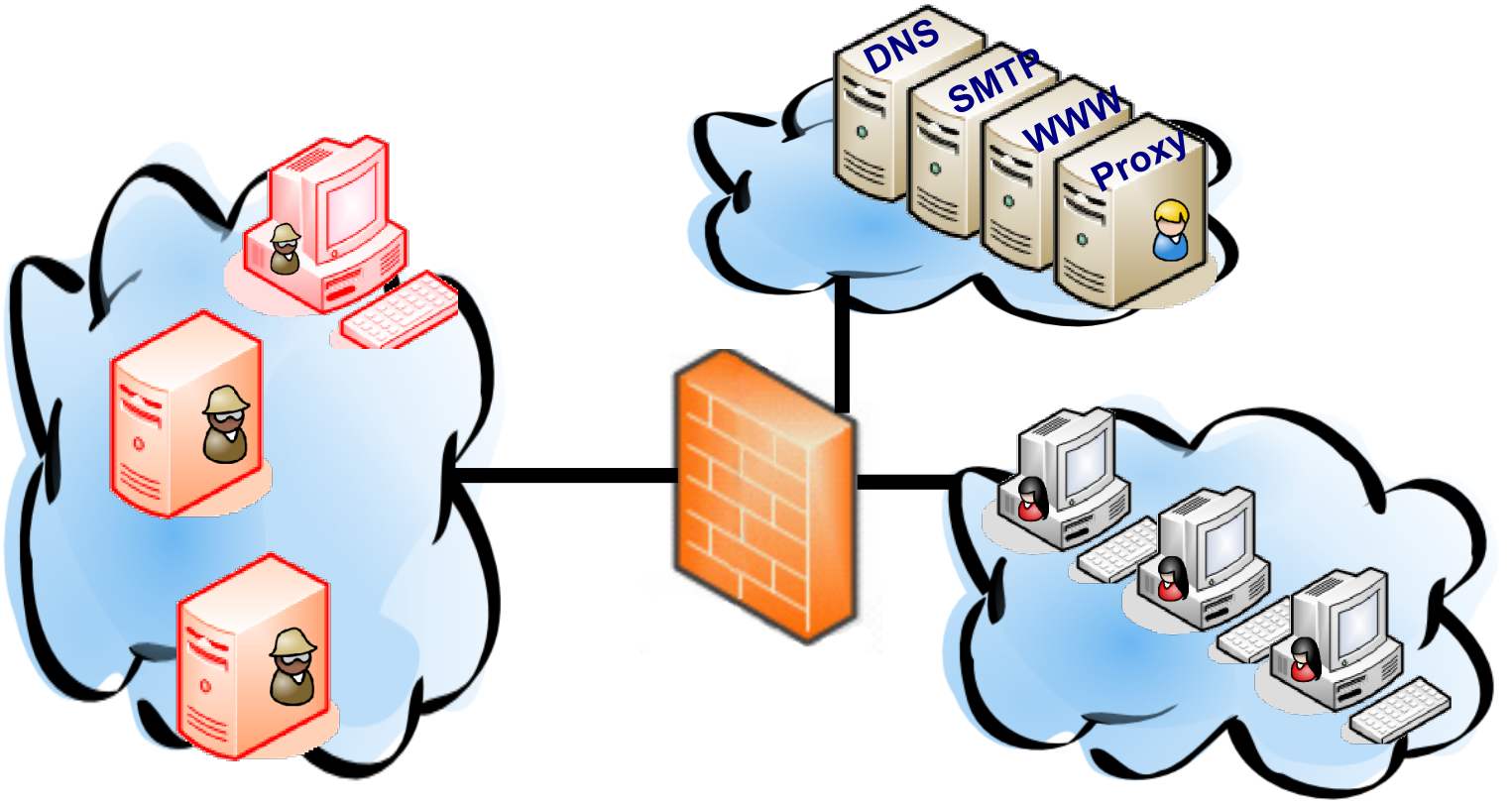
- **Server extern erreichbar**
  - Angreifer mit einem Streich „drinnen“
- ~~**Endgeräte direkt ins – unsichere – Internet**~~
  - ~~Clients als unbewusste „Türöffner“~~
  - Proxies sind „drin“ und gehen „raus“
- **intern und extern Dienste auf einem Server**
  - erschwert Absicherung

Prinzip der geringsten Berechtigung!

Besser aufgeteilt!

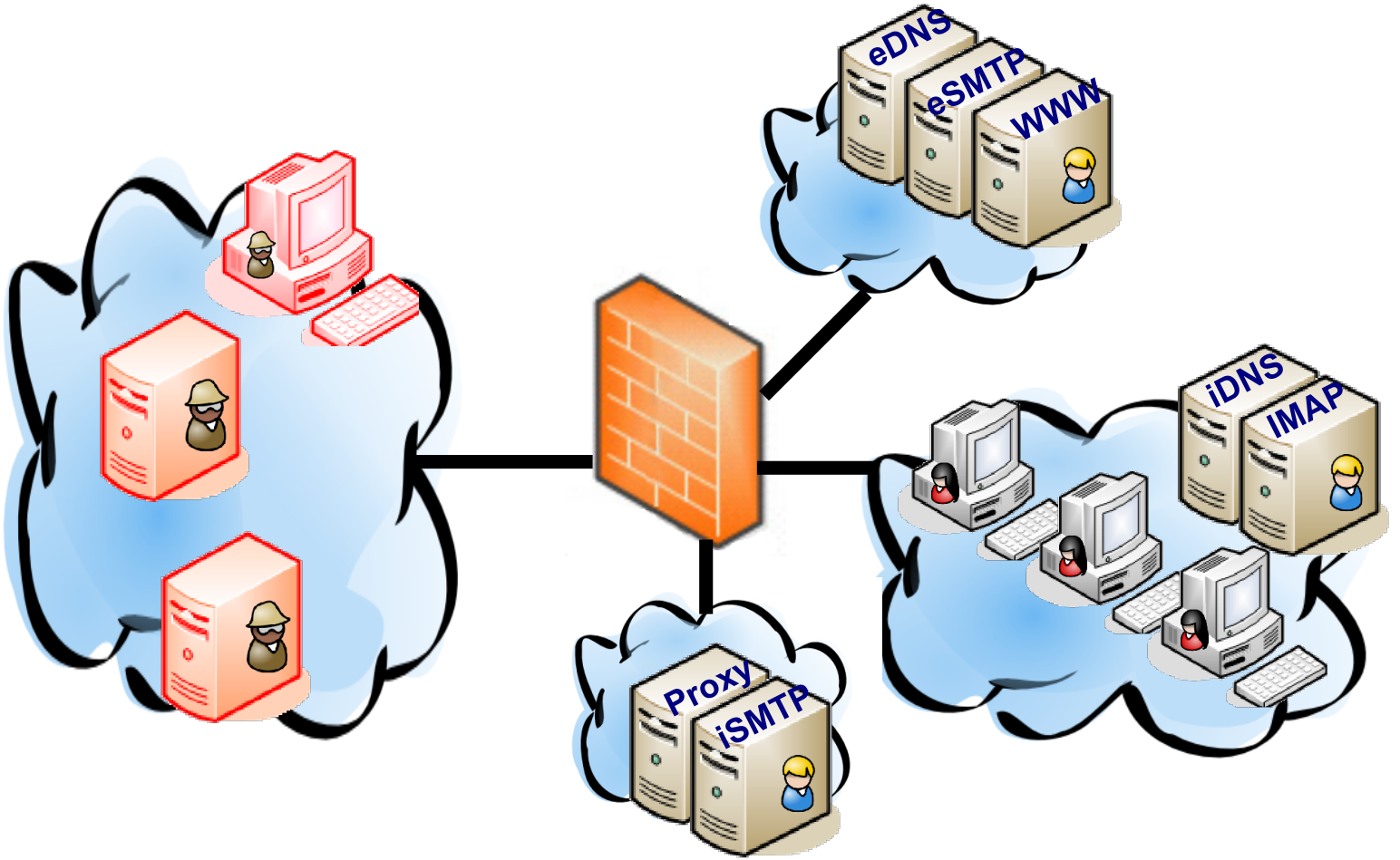


Übliche Option: Schaffung einer DMZ



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?

- SSH-Tunnel in die DMZ
- Proxy Port 443 in DMZ erlauben & CMS

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!

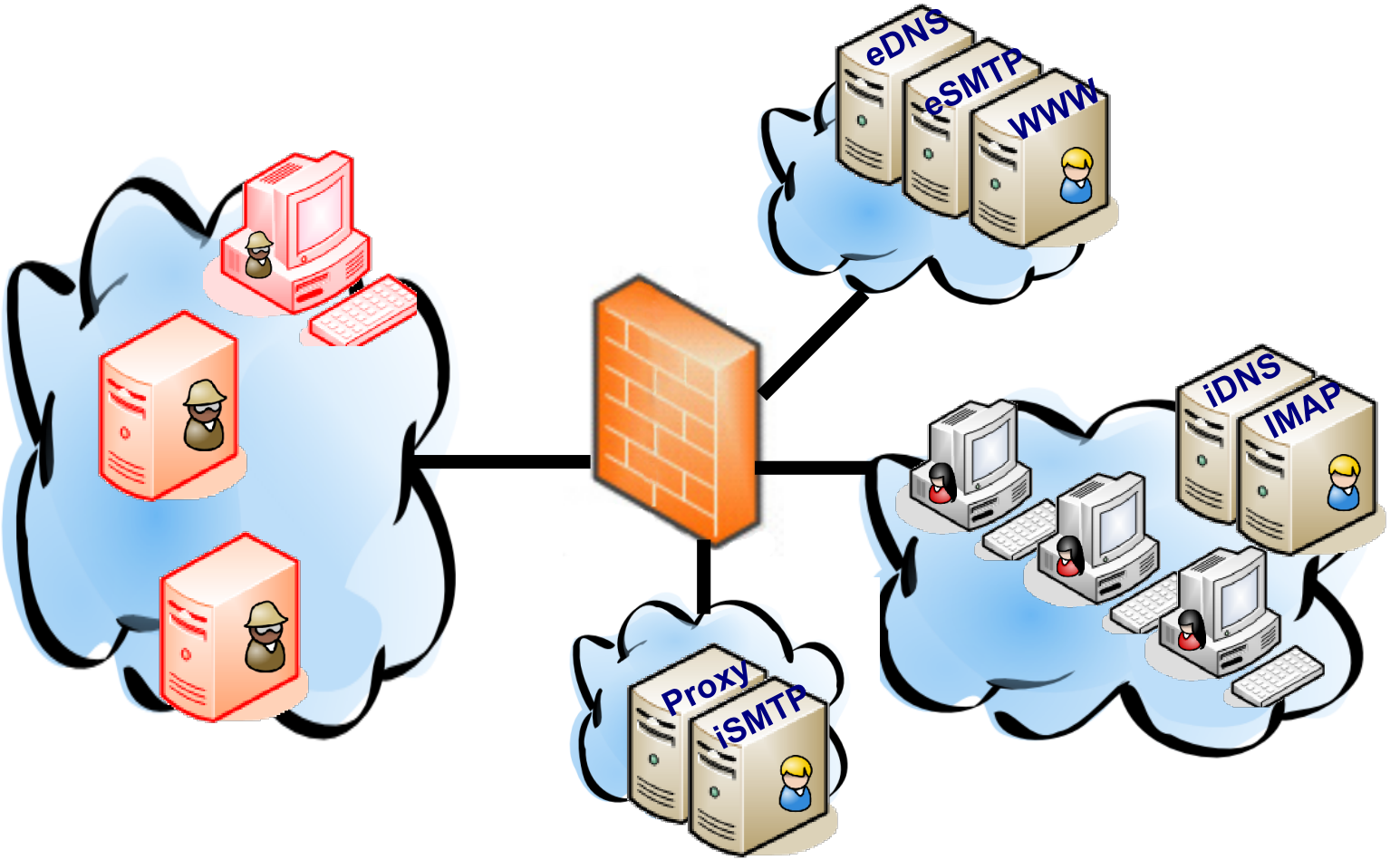
FAQ zur DMZ-Konfiguration (3)

5. Kann ich noch mehr Angriffe abwehren?

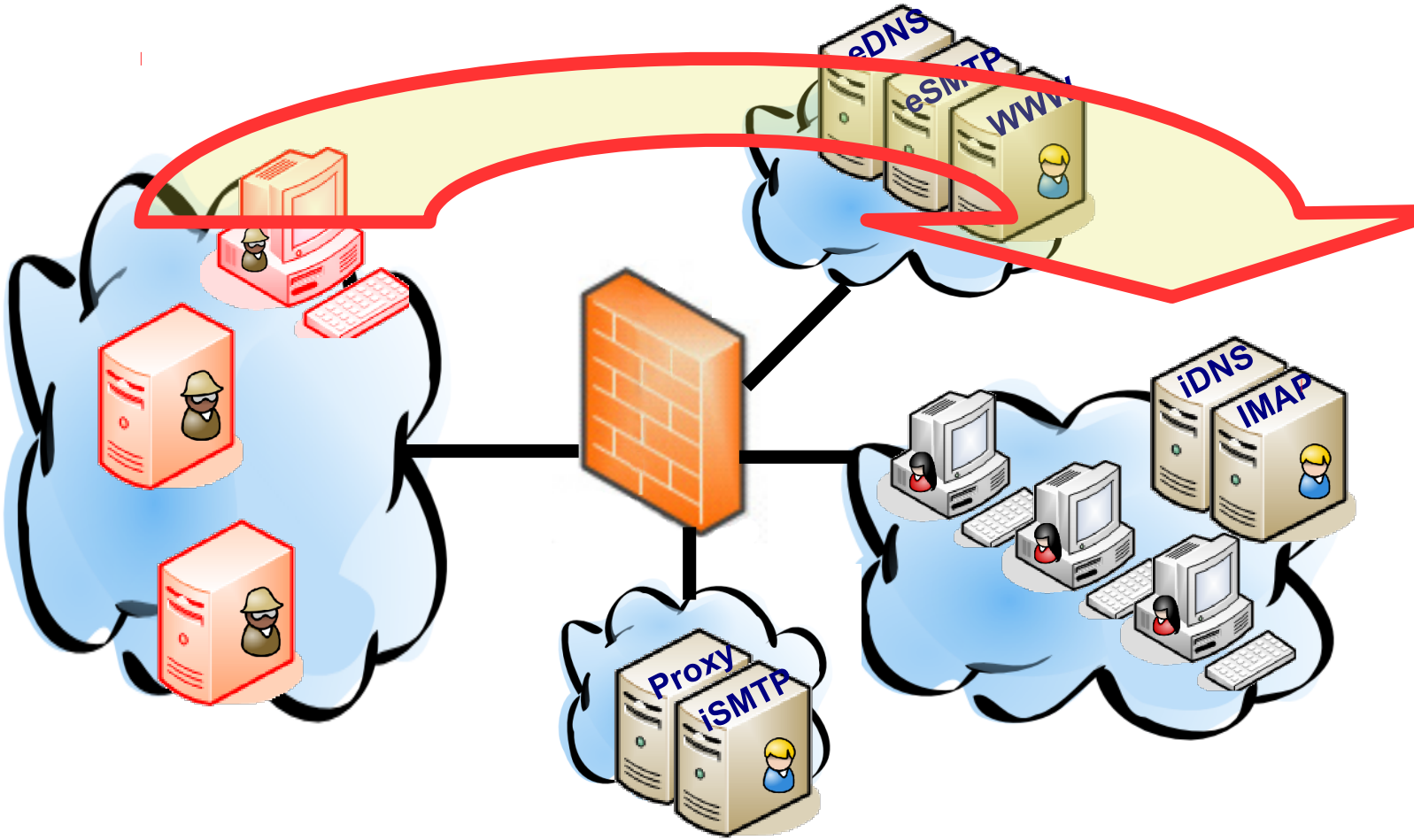
- Immer! Gefälschte Pakete mit internen IP-Adressen könnten gesondert behandelt werden
  (Anti-Spoofing-Filter)
- Unbekannte bzw. nicht verwendete Protokolle gesondert behandeln

Im Moment reicht die DROP-Regel!

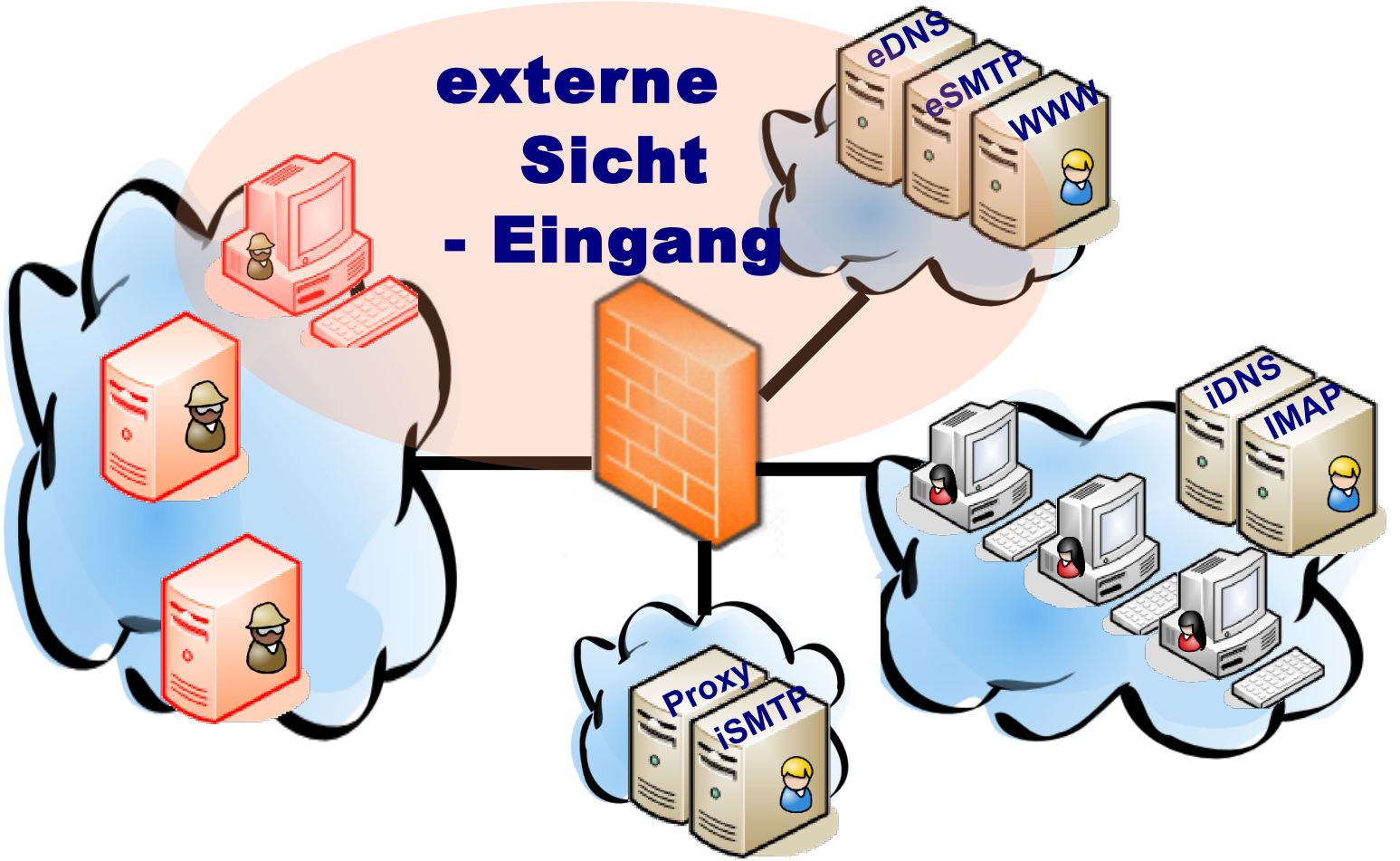
Warum zwei SMTP-Server? Verkehrsflüsse auftrennen



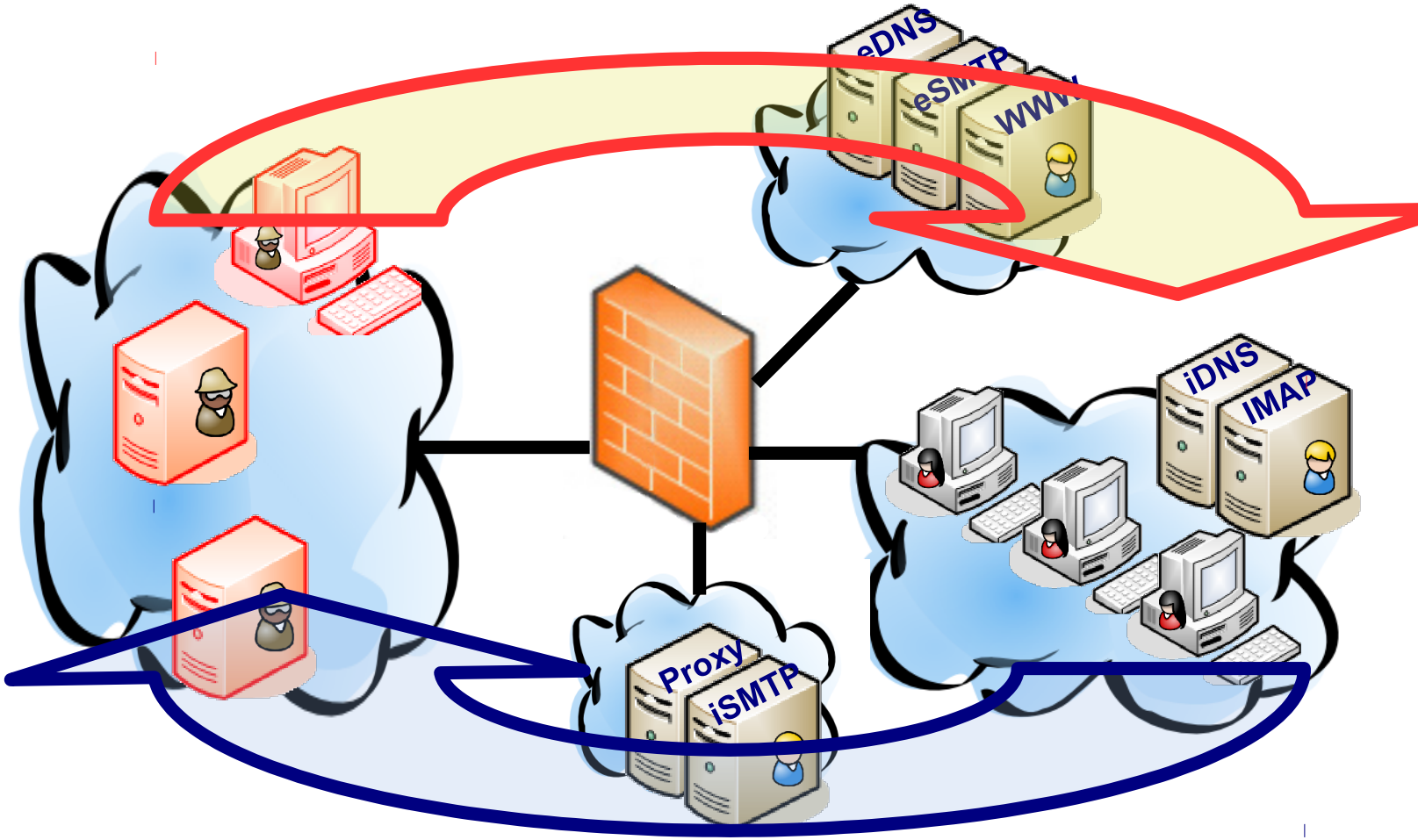
Warum zwei SMTP-Server? Verkehrsflüsse auftrennen



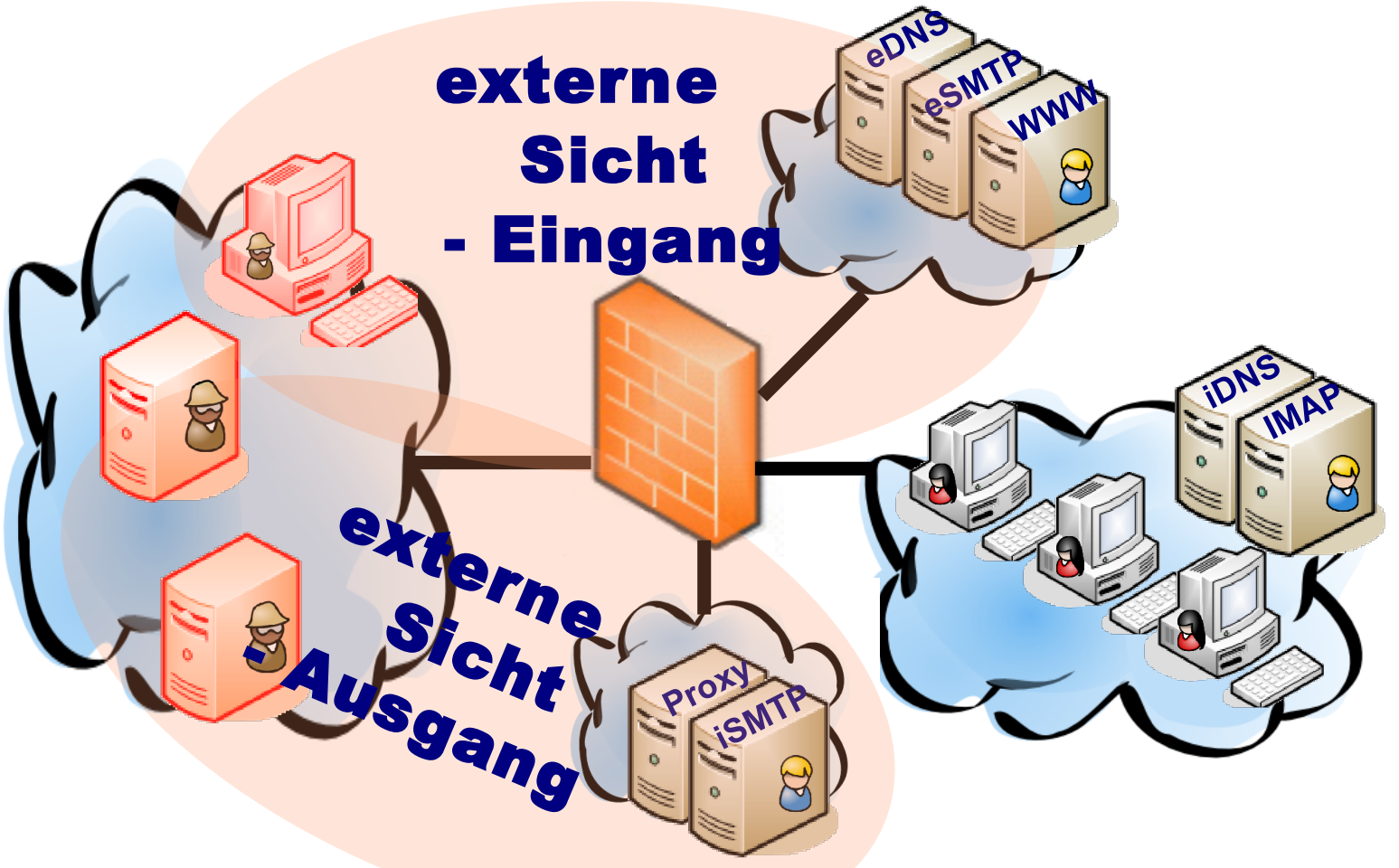
Warum zwei DNS-Server?
Sichtweisen auftrennen



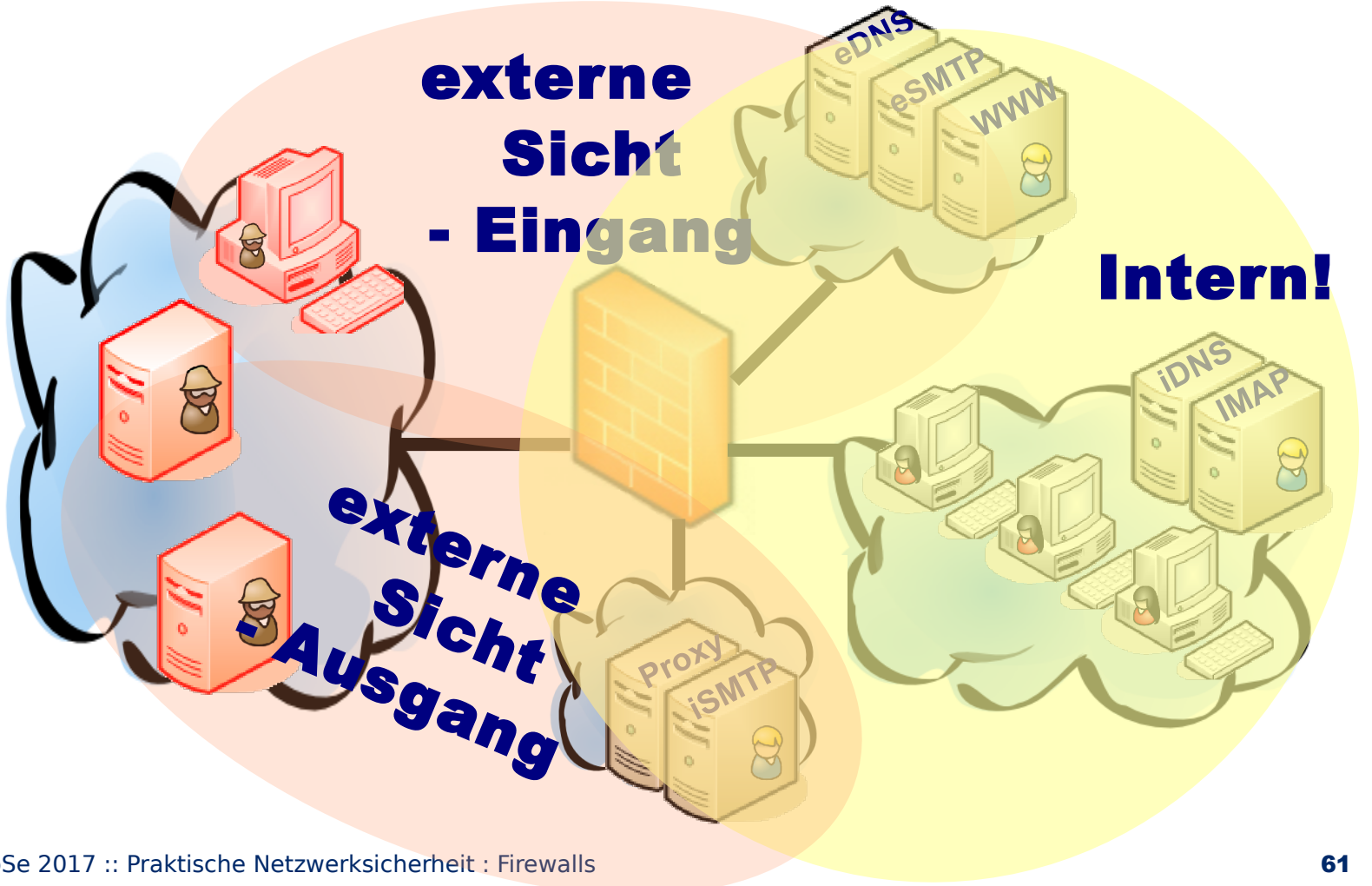
Warum zwei SMTP-Server?
Verkehrsflüsse auftrennen



Warum zwei DNS-Server?
Sichtweisen auftrennen



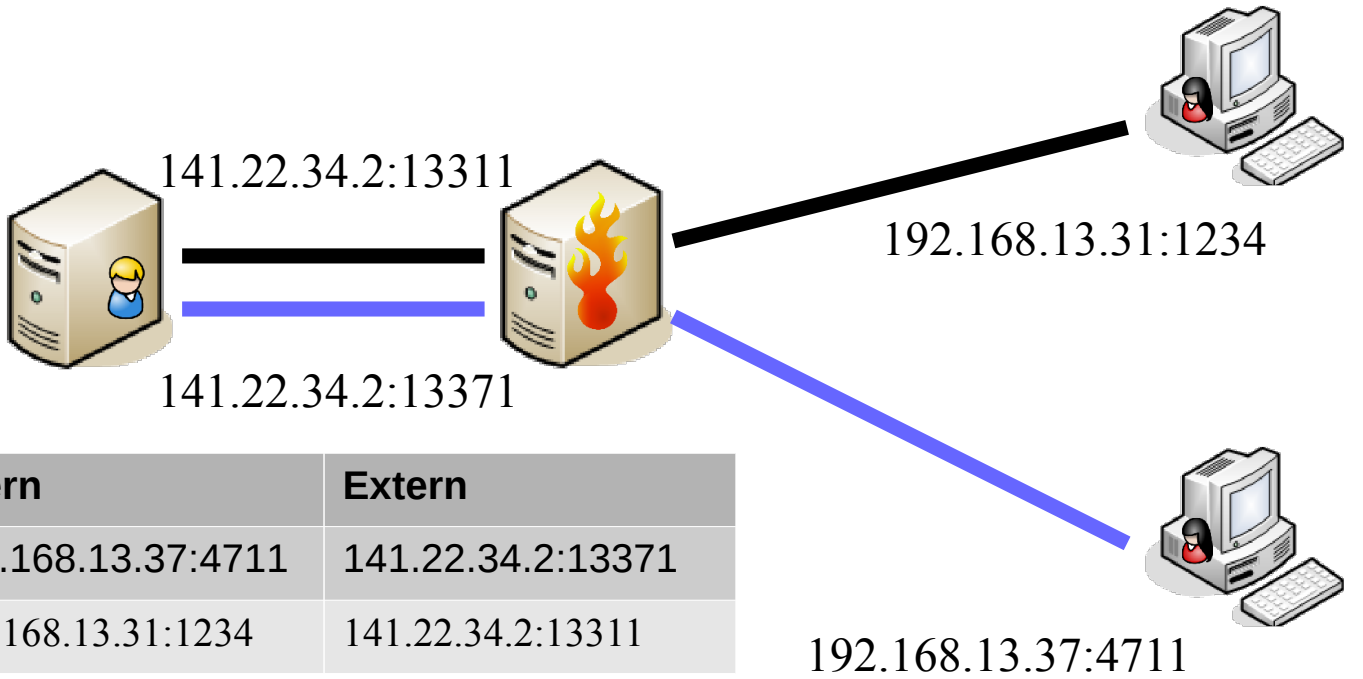
Warum zwei DNS-Server?
Sichtweisen auftrennen



Interne Adressen gut versteckt!

Network Address Translation (NAT)

- viele Private IP abgebildet auf eine öffenltiche
- Umschreiben der Antwort-Adresse



Intern	Extern
192.168.13.37:4711	141.22.34.2:13371
192.168.13.31:1234	141.22.34.2:13311

Interne Adressen gut versteckt!

Network Address Translation (NAT)

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

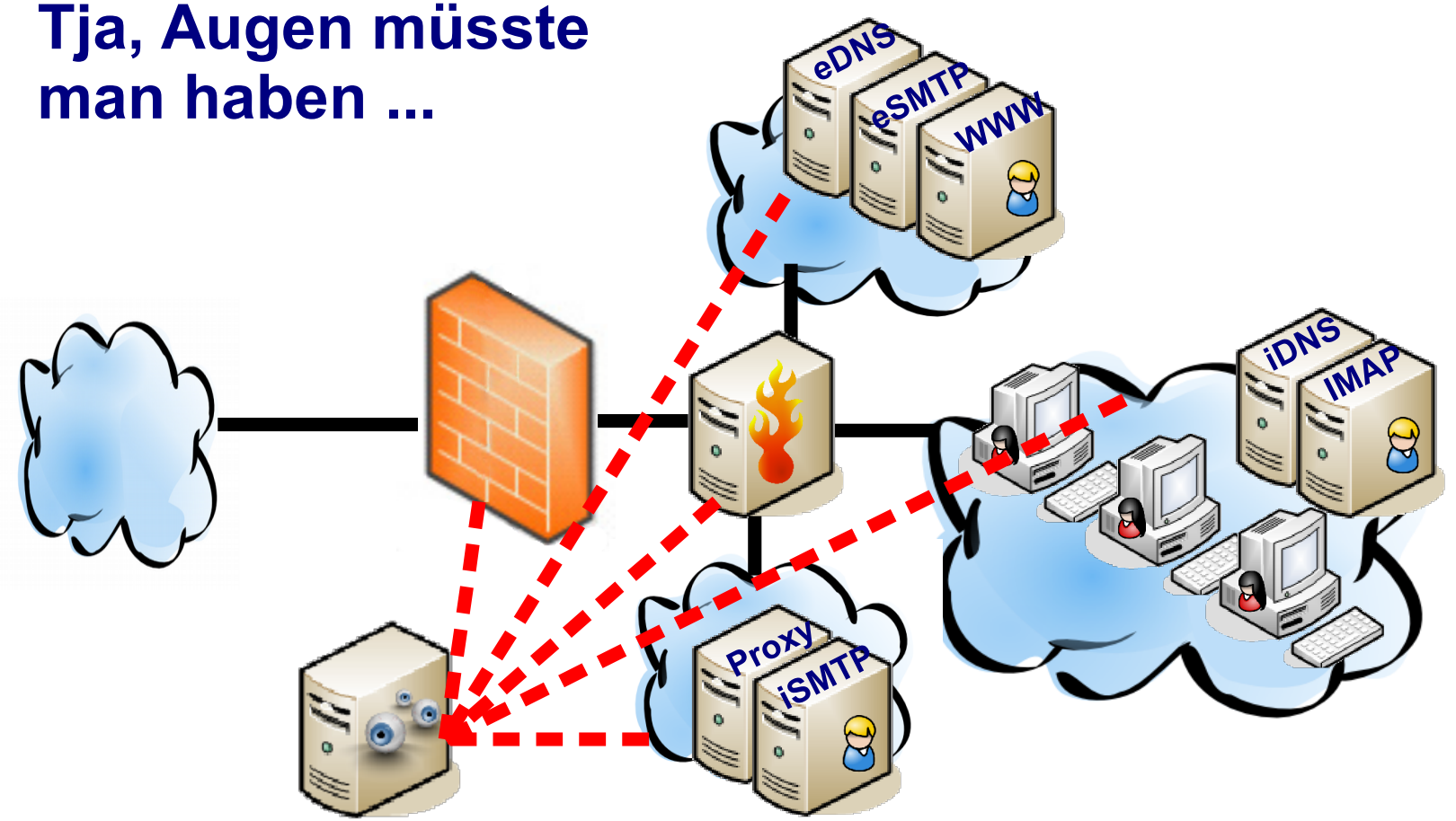
Interne Adressen zu gut versteckt!

- 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?

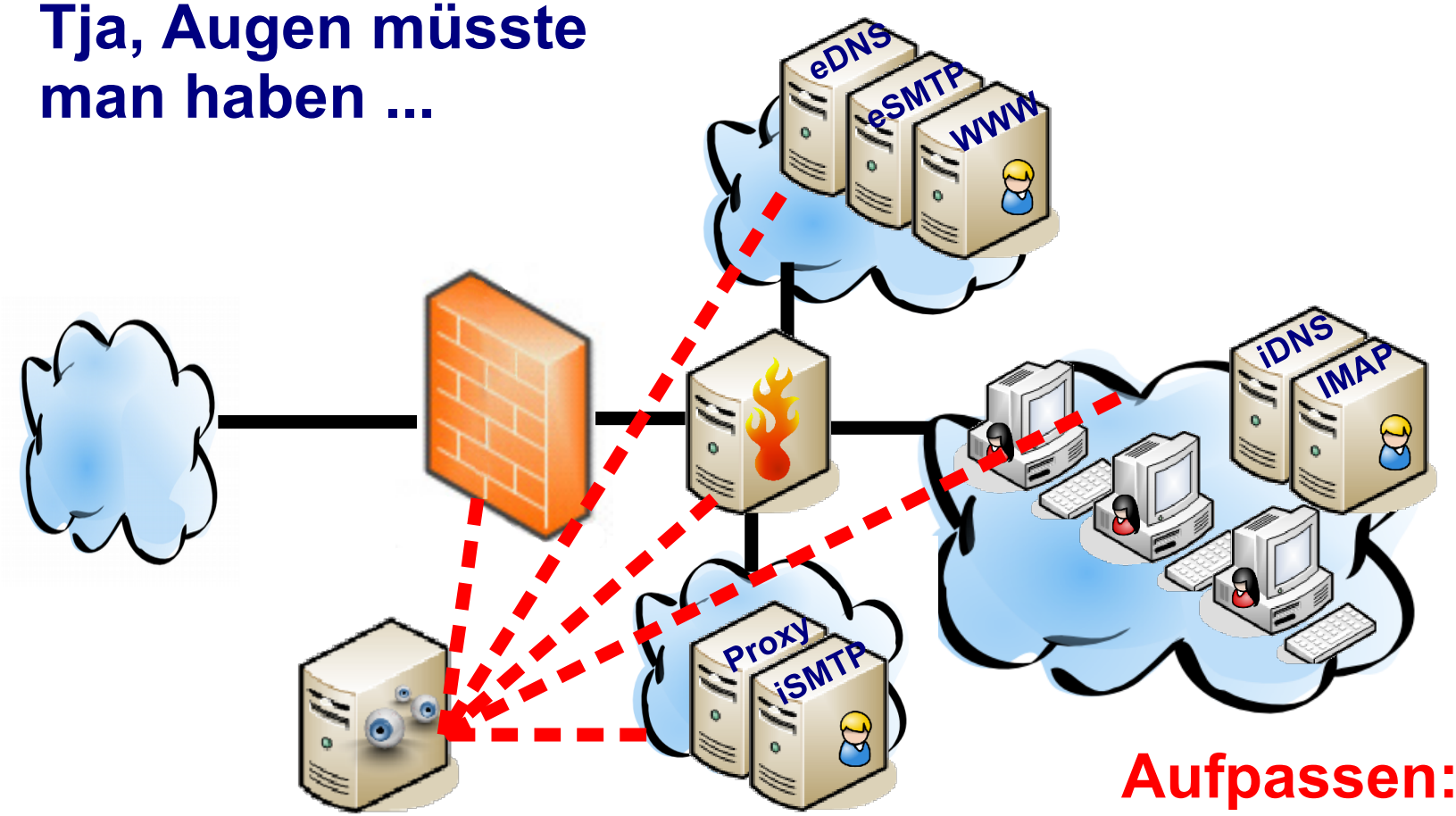
Wie kontrollieren wir die Firewall?

Tja, Augen müsste man haben ...



Wie kontrollieren wir die Firewall?

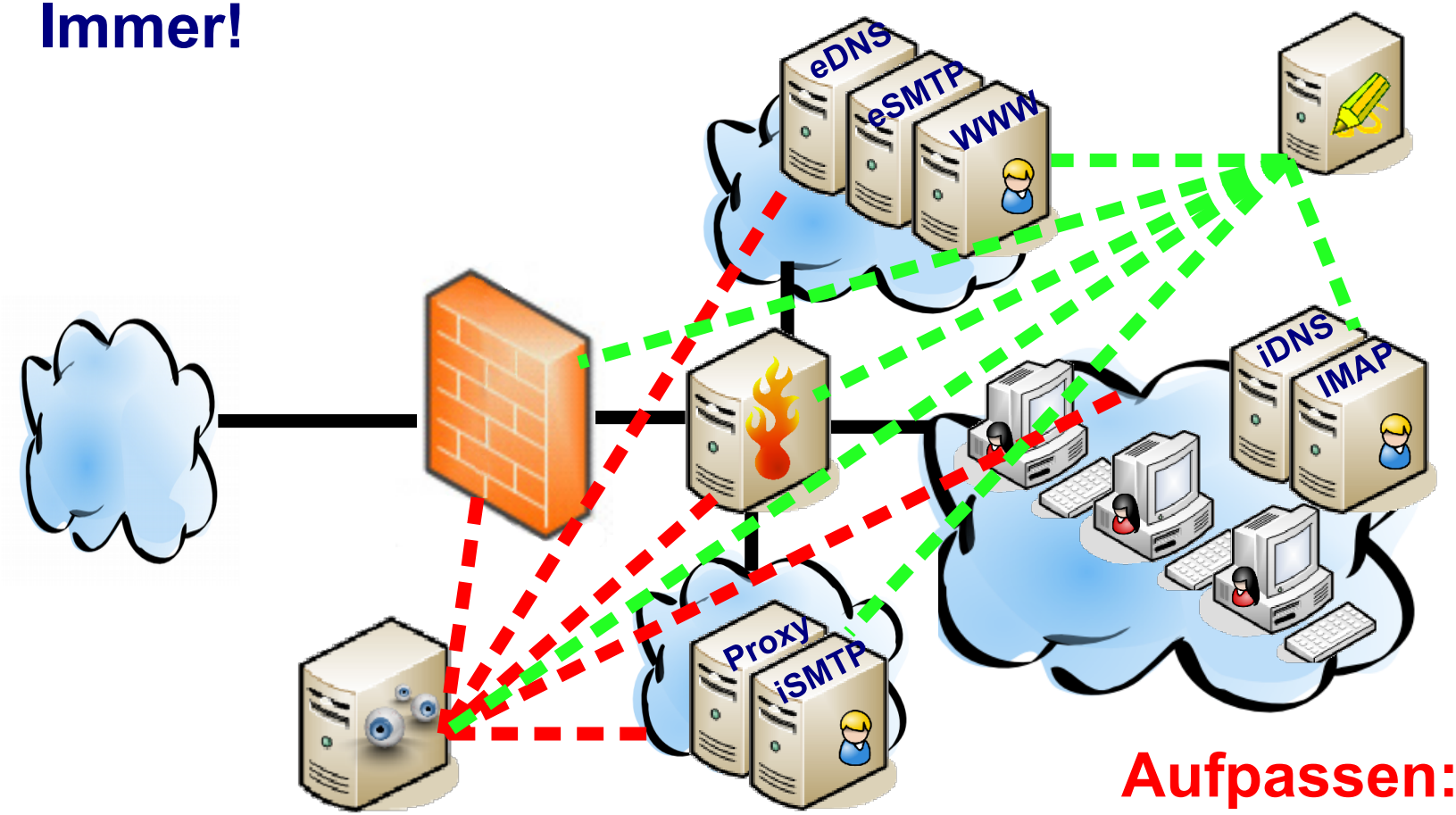
Tja, Augen müsste man haben ...



Aufpassen: Schafft neue Probleme!

Geht noch mehr?

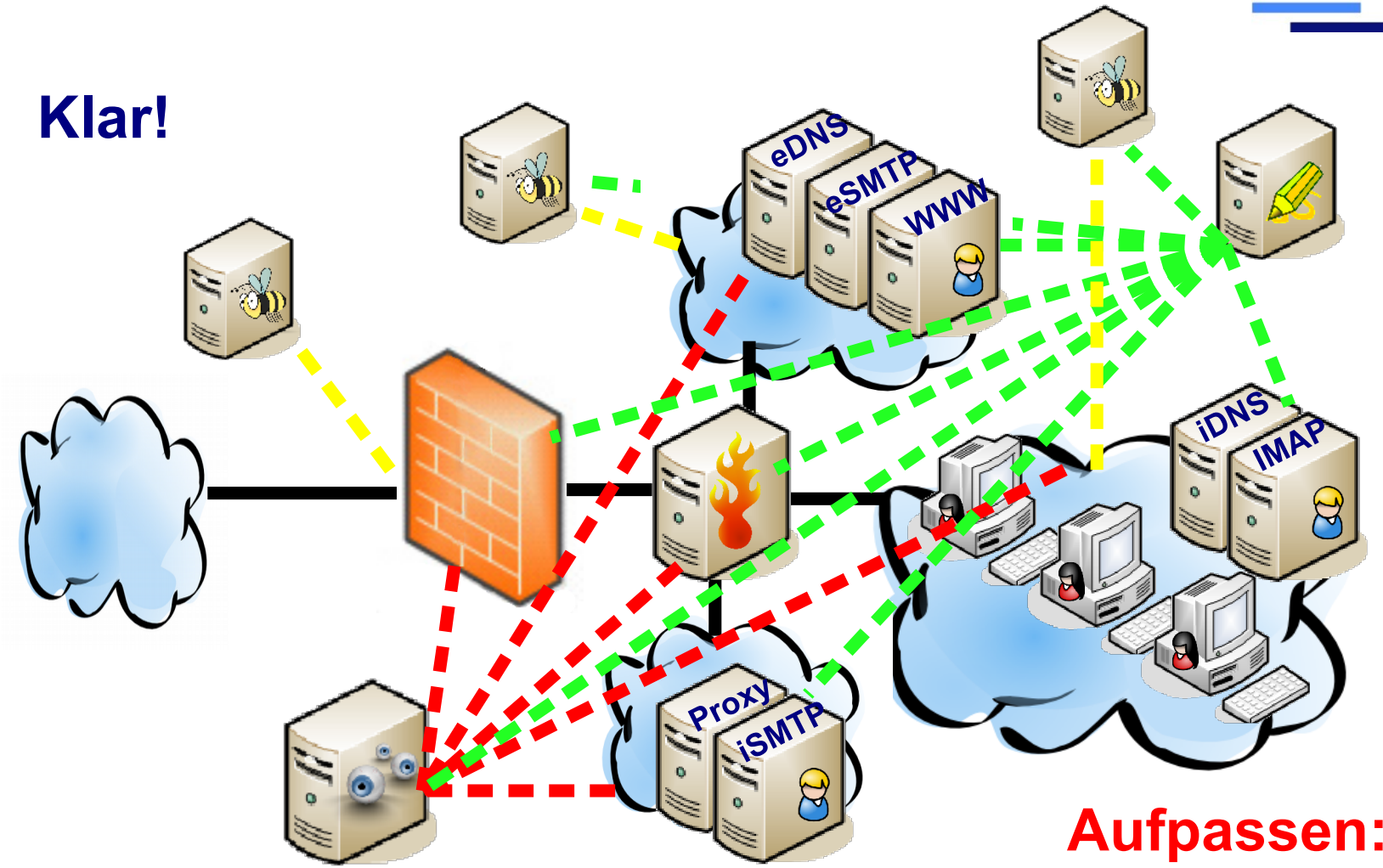
Immer!



Aufpassen: Schafft neue Probleme!

Noch mehr?

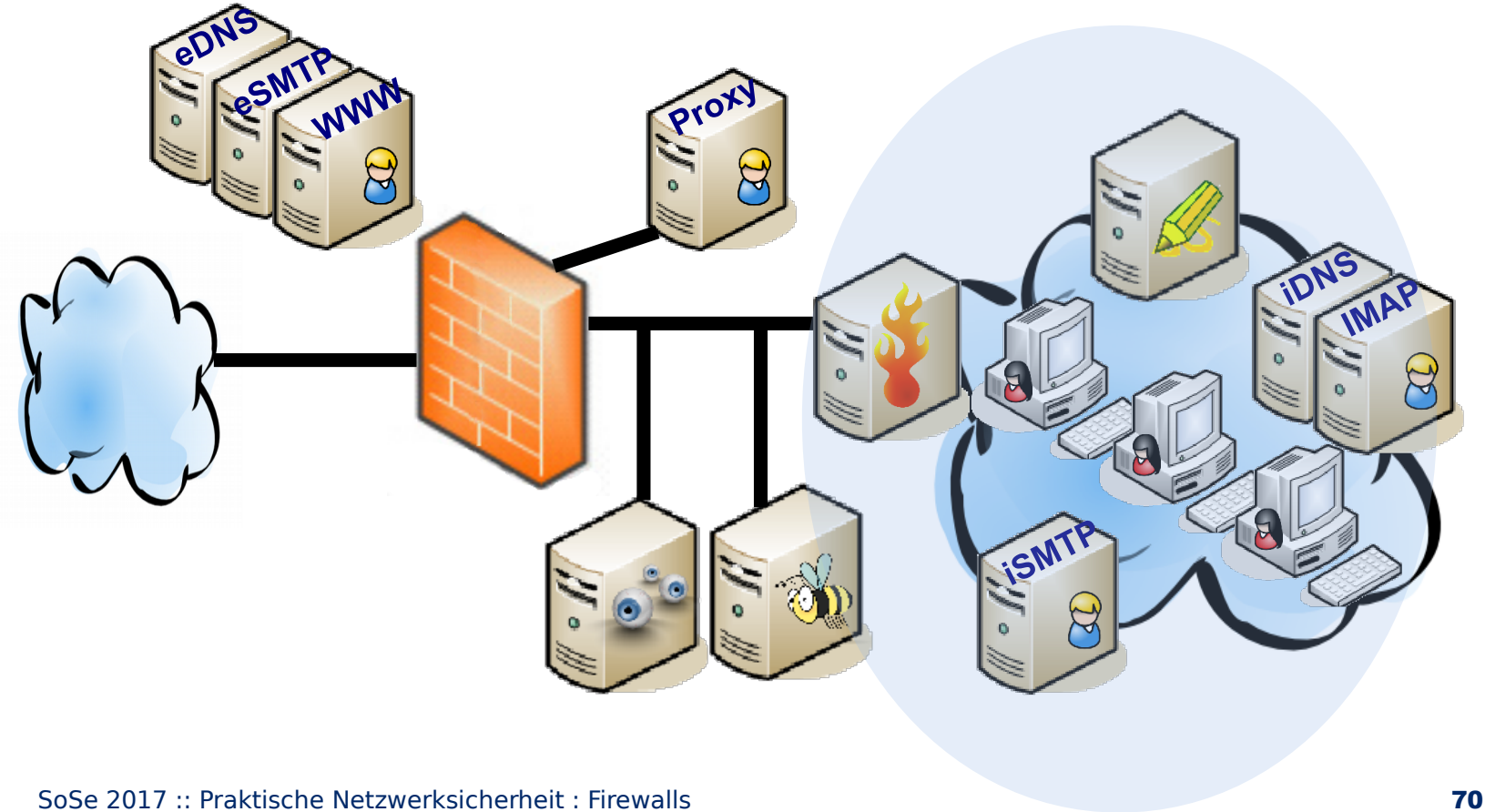
Klar!



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/