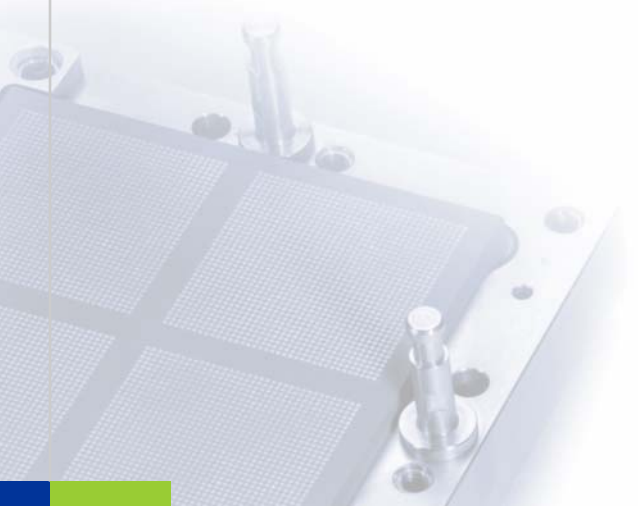
R|R|Z|N

Sicherheitstage SS 2006

Firewallschutz für Institute

Christine Peter

14. Juni 2006



Eigenschaften einer Firewall

R|R|Z|N

Einsatz von Firewall-Technik ist eine mögliche Sicherheitmaßnahme zum Schutz vor Angriffen.

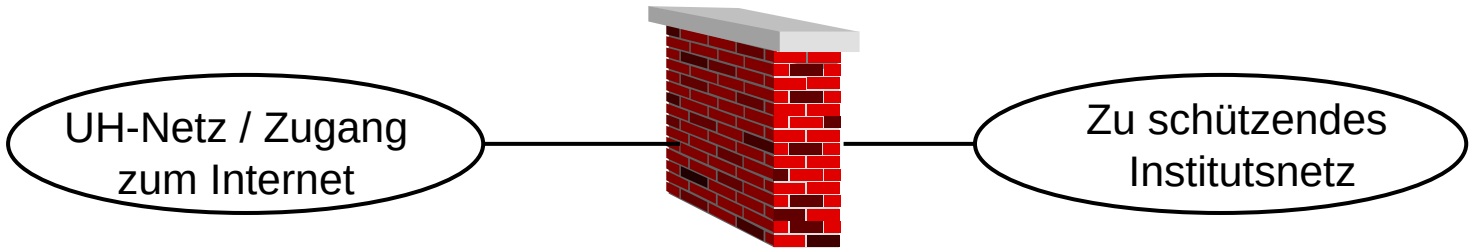
Eine Firewall

- **schützt eine Gruppe organisatorisch zusammengehörender Rechner vor**
  - Angreifern aus dem Internet
  - Angreifern aus dem restlichen Intranet.
- **Ebenso:**
  - Die Firewall begrenzt schädliche Zugriffe und die Verbreitung von Viren, Würmern usw. aus dem geschützten Abschnitt heraus.
  - Ein bestehendes Sicherheitsproblem bleibt „eingekesselt“ und greift nicht auf andere Bereiche über.

Eigenschaften einer Firewall

R|R|Z|N

- Eine Firewall trennt das Netzwerk mit den zu schützenden Systemen von der Außenwelt.



- **Jeglicher Datenverkehr**
  - alle Zugriffe der geschützten Systeme nach außen
  - alle Zugriffe von außen auf eines der geschützten Systeme

  läuft durch die Firewall.

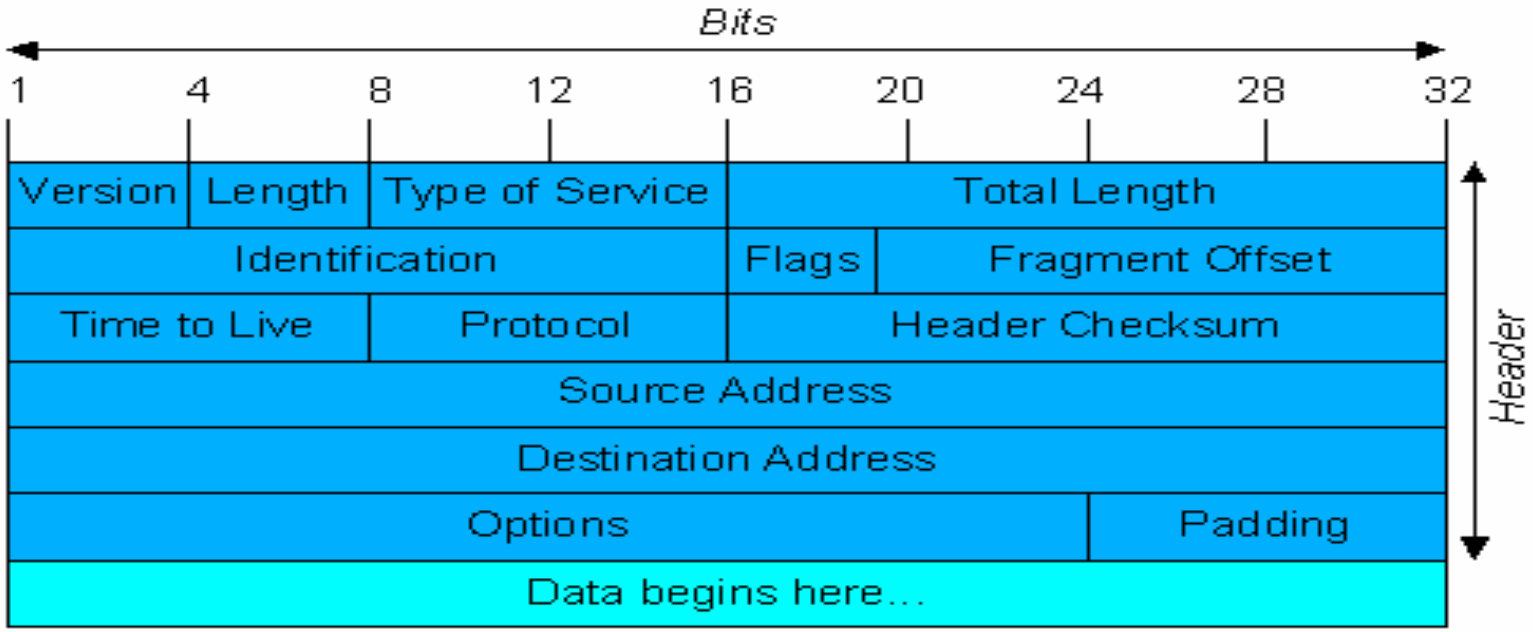
Eigenschaften einer Firewall

R|R|Z|N

- Eine Firewall ist ein eigenständiges Gerät**,** welches besonders für diese Aufgabe konfiguriert ist.
- Viele einzelne Regeln legen fest, welche Kommunikationsverbindungen erlaubt oder verboten sein sollen.
- Die Regeln sind individuell auf die Kommunikationsbedürfnisse der zu schützenden Institution zugeschnitten.
- Die Regeln sind verbindlich für das gesamte Institutsnetz und alle angeschlossenen Rechner.

- Kommunikation im Internet = Austausch von Datenpaketen.
- Jedes Paket wird von einem Quell-Rechner an einen Ziel-Rechner geschickt.
- Auch "Verbindungen" sind eigentlich nur Datenpakete, die zwischen zwei Rechnern ausgetauscht werden.
- Eine Verbindung besteht aus mehreren Phasen:
  - Verbindungsaufbau
  - Austausch der eigentlichen Daten
  - Verbindungsabbau

- Der Aufbau dieser Datenpakete ist durch verschiedene **Protokolle** genau vorgeschrieben.
- Nur so können Quell- und Ziel-Rechner sich verstehen und eine sinnvolle Kommunikation realisieren.
- Beispiele für Protokolle sind: IP, TCP, UDP, ICMP, …



Flags:

DF

MF

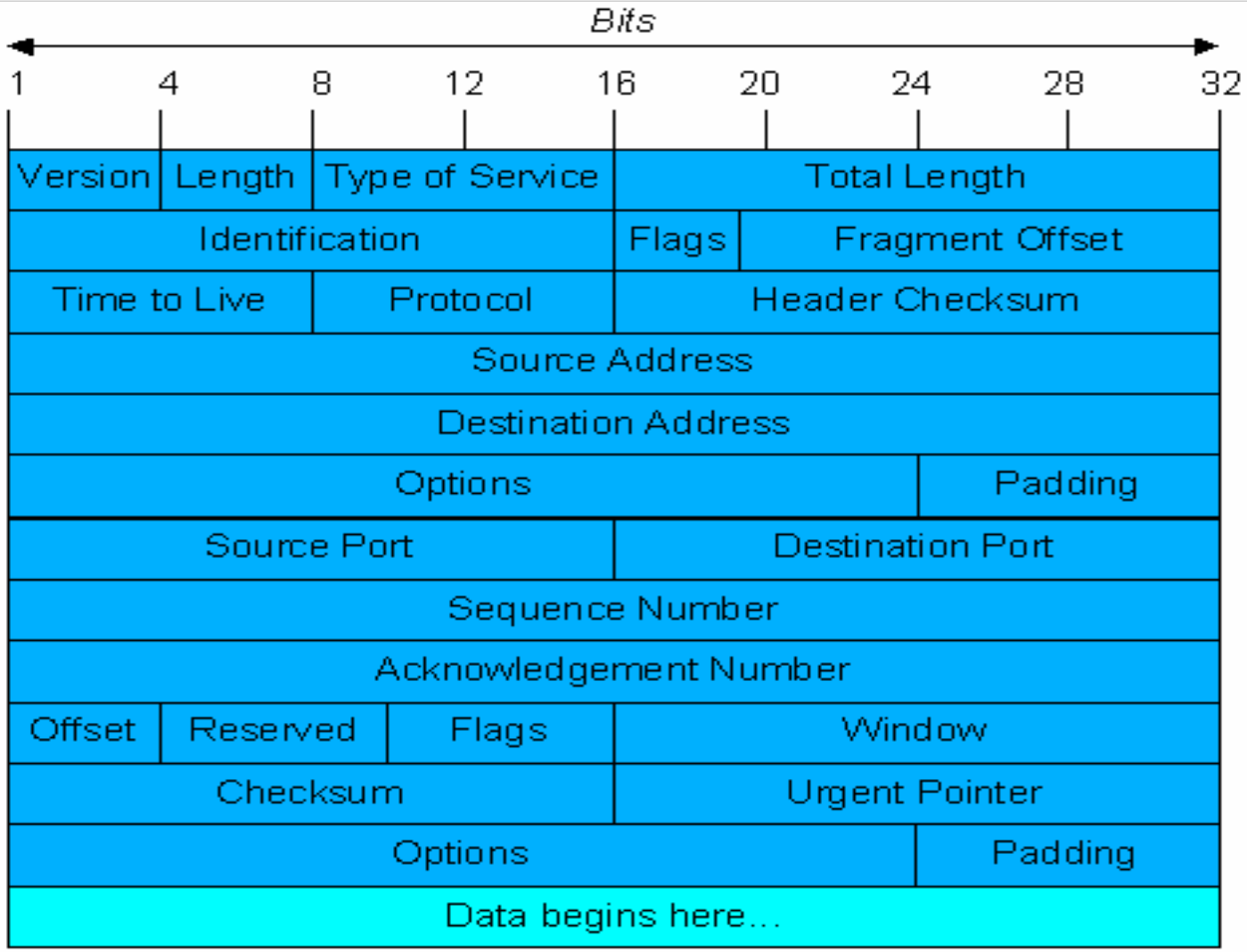
Grundlagen: Datenkommunikation im Internet

R|R|Z|N

- Protokolle bilden die Basis des Datenaustausches im Internet
  - Die Pakete kommen an die richtige Adresse
- Auf der Grundlage der Protokolle, die prinzipiell eine Verbindung organisieren, können einzelne Rechner nun verschiedene Dienste anbieten.

  Hierbei tauschen Server- und Anwenderprogramme bestimmte Daten aus.
  - der Mail-Client auf der Anwenderseite mit der Mailserver-Software auf der Serverseite
  - Der Browser auf der Anwenderseite mit der Webserver-Software auf der Serverseite
- Ein Rechner kann mehrere unterschiedliche Dienste anbieten.
- Zur Unterscheidung der unterschiedlichen Dienste benötigt man Ports.
  - Für weit verbreitete Dienste werden feste Port-Nummern vergeben.

Grundlagen: Datenkommunikation im Internet



Flags:

SYN

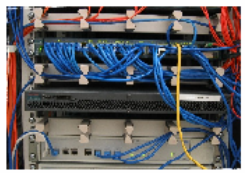
ACK

RST

FIN

:

Beispiel Dienstleister RRZN

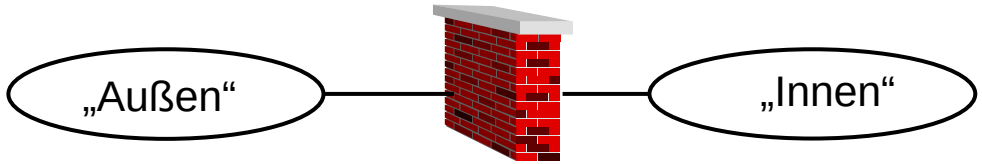


Telefon- oder Datennetz

Öffentlicher Zusteller

Hauspost

Wie arbeitet eine Firewall



- Jedes einzelne Datenpaket wird untersucht und auf Zulässigkeit überprüft:
  - IP-Adresse des Absenders (von wem kommt das Paket?)
  - IP-Adresse des Empfängers (wohin soll das Paket?)
  - welches Protokoll: IP, TCP, UDP, ICMP
  - Ziel-Port-Nummer: welcher Netzwerk-Dienst soll angesprochen werden?
  - gehört das Paket zu einer bereits bestehenden Verbindung (stateful inspection) oder soll eine neue Verbindung geöffnet werden?
- Eine Firewall kann Kommunikationsverbindungen
  - als erwünscht erkennen und erlauben oder
  - als unerwünscht erkennen und ablehnen.

Eine Regel in Firewall-verständlicher Syntax hat folgende Komponenten:

- **Aktion:** Deny oder Permit
- **Protokoll:** IP,TCP, ...
- **Quelladresse:** alle, einzelne IP oder Netzbereich
- **Quellport:** 1 – 65.535
- **Zieladresse:** alle, einzelne IP oder Netzbereich
- **Zielport:** 1 – 65.535 oder Name des Dienstes

Beispiele: (SUB = Subnetz des Institutes)

permit tcp host 130.75.SUB.a host *130.75.x.y* eq pop3

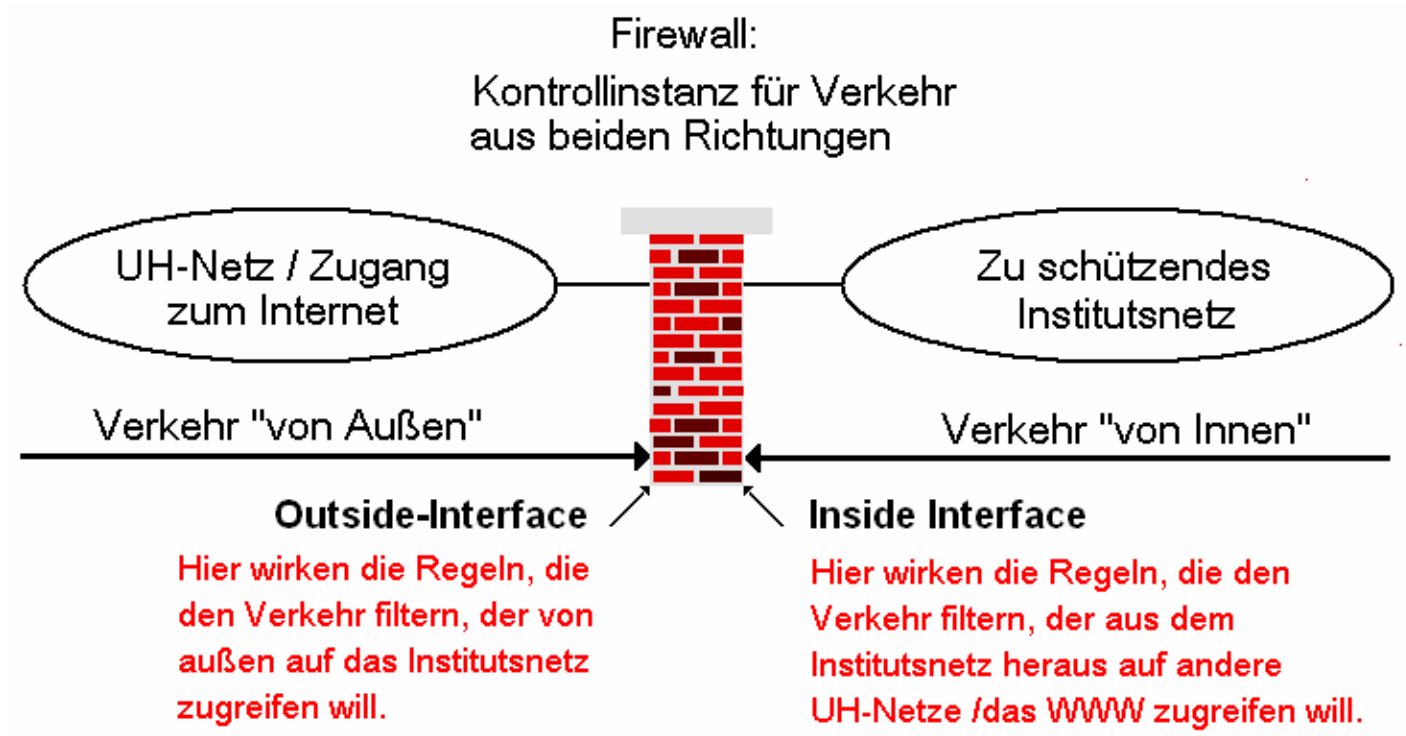
permit tcp host 130.75. SUB.b gt 1024 host 130.75.x.z gt 1024

deny tcp any any eq 445

Alle Regeln zusammen bilden die sogenannte Access-Control-List (ACL)

Eine Access-Control-List besteht aus zwei Abschnitten:

- **Outbound: Zur Regelung des Verkehrs von „innen“ nach „außen“.**
- **Inbound: Zur Regelung des Verkehrs von „außen“ nach „innen“.**



Die Reihenfolge der Regeln ist wichtig:

- **Die Regeln werden sukzessive nach abgearbeitet.**
- **Sobald eine passende Regel erreicht wird, werden die restlichen Regeln nicht mehr durchlaufen.**

Beispiel: (SUB = Subnetz des Institutes)

...

permit tcp any host *130.75.x.y* eq ssh

...

deny tcp host 130.75. SUB.7 host *130.75.x.y* eq ssh

Paket:
Quell-IP: 130.75. SUB.7
Ziel-IP: 130.75.x.y
Zielport: 22 (ssh)

Passende Regel gefunden,
Paket ist erlaubt
und wird durchgelassen

Eine optimal konfigurierte Firewall arbeitet nach der Maxime:

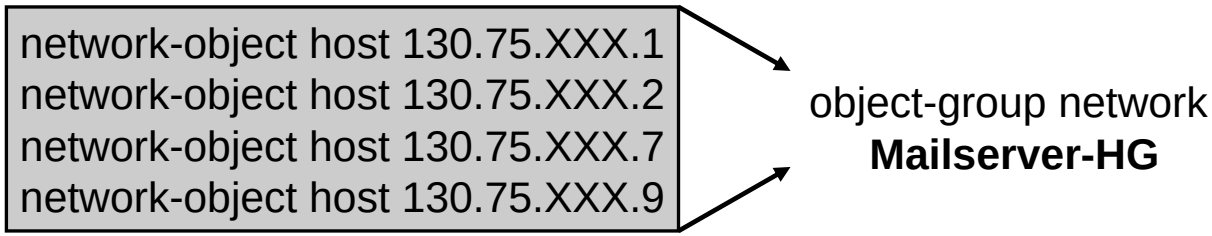
„Default-Deny“

- Alle Pakete, die nicht durch eine spezielle Regel erlaubt werden, sollen automatisch verboten sein:
  - Für jede ankommende Verbindung wird der Regelsatz sukzessive abgearbeitet, ob eine Regel passt.
  - Alle Verbindungen, für die im Regelsatz keine „passende“ Regel gefunden wird, gelten als prinzipiell unerwünscht und werden abgeblockt:
    - als letzte Regel jeder ACL findet sich die Cleanup–Regel

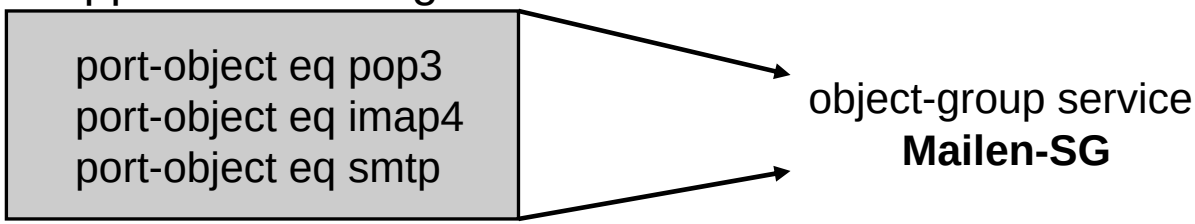
      deny ip any any log

Strukturierungs-Möglichkeit für Firewall-ACLs:

- **Bildung von Network-Groups:** verschiedene IPs können zu einer Gruppe zusammengefasst werden



- **Bildung von Service-Groups:** verschiedene Ports/Dienste können zu einer Gruppe zusammengefasst werden



- **Konfiguration vereinfacht sich, die ACL wird übersichtlicher:**
  - permit any object-group Mailserver-HG Mailen-SG

Wie arbeitet eine Firewall

R|R|Z|N

- **Eine Firewall kann nicht alle Risiken ausschalten.**
- **Sie bietet insbesondere keinerlei Schutz vor „importierten“ Angriffen!**
  - Gefahr durch E-Mail-Anhänge.
  - Gefahr beim „Surfen“ durch „aktive“ Web-Inhalte und unbedachte Downloads.

  ➔ Die Firewall kann keine Aktivitäten verhindern, die **scheinbar legal** auf erlaubten Wegen ausgeführt werden!

  ➔ Die Disziplin der Anwender ist ein ganz wichtiger Sicherheits-Faktor.

  - Das Firewall-System kann nur vor Rechnern „vor“ der Firewall schützen, nicht aber vor den Geräten innerhalb des Institutes.

  ➔ Wird ein Rechner kompromittiert oder schleppt ein Benutzer einen Wurm in den Institutsbereich ein, sind trotz der Firewall alle Systeme gefährdet.

  ➔ Es muss also weiterhin für die Sicherheit der Einzelsysteme gesorgt werden.

Nachteile einer Firewall

R|R|Z|N

- **Der Datenverkehr wird kategorisiert, bewertet und reglementiert:**
  - D.h. eventuell auch als kritisch oder unnötig eingeschätzt und verboten.
  - Dadurch sind manche liebgewonnenen Zugriffe nicht mehr möglich.
- **Bei neuen Anforderungen an den Datenverkehr muss erst die Policy geändert werden.**
- **Die Einrichtung einer Firewall mit allen begleitenden Maßnahmen verursacht zunächst einmal Arbeit und kostet Zeit.**
  - Mittelfristig wird durch den Einsatz von Firewall-Technologie die Arbeit weniger werden.

Zentraler RRZN-Netzschutz:

R|R|Z|N

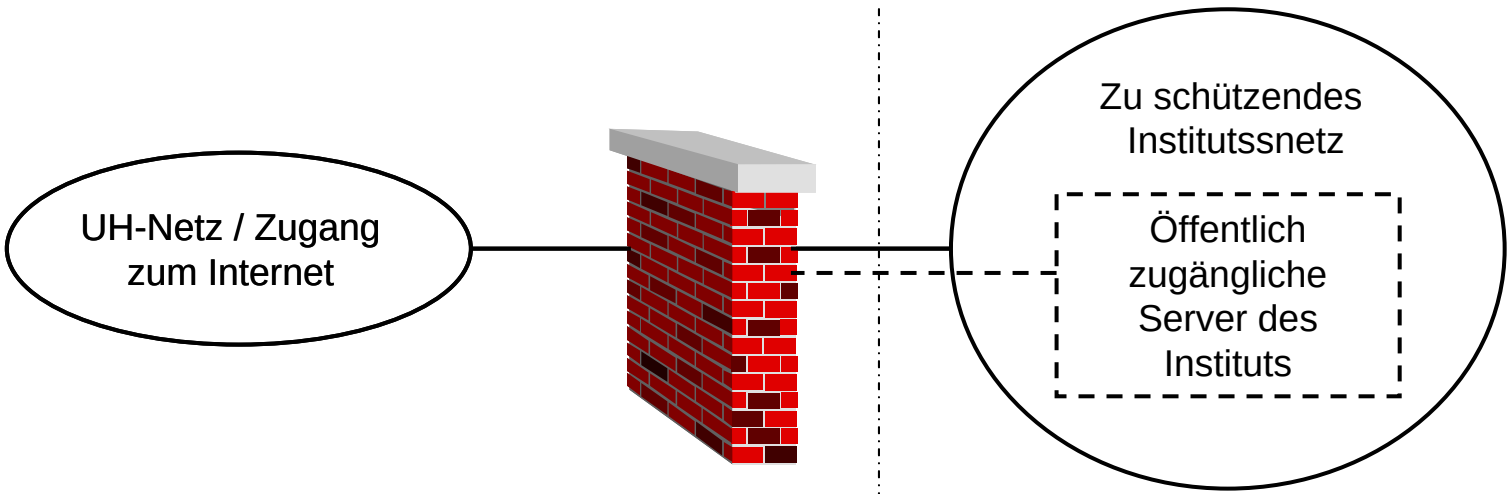
Das RRZN betreibt ein einstufiges Firewall-System.

Institute können sich hinter dieses Firewall-System schalten lassen.

- Das Institut definiert seine Kommunikations-Anforderungen.
- Im gemeinsamen Gespräch zwischen Institut und RRZN wird eine Sicherheitspolicy für das Institut erarbeitet.
- Das RRZN überträgt die Ergebnisse in Firewall-Regeln.
- Das RRZN administriert die Geräte.
- Das RRZN trägt Änderungen ein.
- Das RRZN stellt die Logdaten auf einem zentralen Server zur Verfügung.
- Das Institut ist verantwortlich für die Abholung der Log-Daten und deren Kontrolle.

Dieser Service ist kostenlos für Institute der UH.

Zentraler RRZN-Netzschutz:



Verantwortungsbereich RRZN
(Filterregeln nach Institutsbedarf)

Verantwortungsbereich Institut
(Log-Analyse durch Institut)

Zentraler RRZN-Netzschutz:

R|R|Z|N

Vorteile der Firewall im RRZN

- zeitlicher Aufwand für Institut ist sehr gering
- kein zusätzlicher personeller Aufwand
- kostenlos
- regelmäßige Wartung der Firewall ist sichergestellt
- Bei Problemen: Unterstützung durch das RRZN
- keine Nachfolgerproblematik
- redundante Systeme
- Hilfsmittel zur Analyse von Logdaten werden zur Verfügung gestellt

Nachteile der Firewall im RRZN

- Änderungen: mit Zeitverzögerung
- keine DMZ möglich
- es existiert eine Warteliste

Zentraler RRZN-Netzschutz:

R|R|Z|N

- **Verfahrensablauf in mehreren Phasen / Stufen:**
  - Vorbereitungsphase
  - Stufe 1: Umstellung mit vereinfachter Policy
  - Stufe 2: Verfeinerung der Regeln aus Stufe 1
  - Parallel zu Stufe 1 und 2: Nachbesserungen

Vorbereitende Tätigkeiten im Institut:

- **Für jedes Institut - beziehungsweise gegebenenfalls für den entsprechenden Teilbereich - müssen ein(e) „Netzschutz-Ansprechpartner(in) und eine Vertretung benannt werden.**
  - Nur diese erhalten Auskünfte über die Firewallkonfiguration und Dokumente / Dateien mit institutsinternen, eventuell vertraulichen Daten wie z.B.:
    - die momentan aktiven Firewallregeln
    - Logdaten.
  - Nur von diesen nimmt das RRZN (schriftlich) Wünsche für Änderungen am Regelwerk entgegen.

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- Bei Instituten mit sehr unterschiedlichen internen Strukturen kann es unter Umständen auch möglich sein, dass nur für bestimmte Bereiche ein Firewall-Schutz realisiert werden kann.
- Eine Umstrukturierung bei der Vergabe von IP-Adressen kann notwendig werden.
- Benutzer müssen informiert und ev. befragt werden .
- Wünschenswert: Schulung der Benutzer über sicherheitskonformes Anwenderverhalten.

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- **Für den Firewallbetrieb muss im Institut zunächst eine „Verkehrsanalyse“ betrieben werden :**
  - Identifizierung der Server-Systeme: auf welche Systeme muss überhaupt ein Zugriff von außerhalb des Institutes möglich sein.
  - Welche Applikationen laufen und welche Dienste werden angeboten.
  - Identifizierung der Ports, auf die ein Zugriff erlaubt werden muss.

- **Daraus ergibt sich eine Aufstellung der Anforderungen an das zukünftige Regelwerk :**
  - welche Dienste / Protokolle / Ports
  - zwischen welchen IPs / IP-Bereichen
  - in welcher Richtung

  sollen erlaubt / verboten sein.

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

Zur Erleichterung dieser Aufgabe bietet das RRZN eine Muster-Policy:

- Diese enthält ein Standard-Profil, welches die meisten Anforderungen eines Institutes abdeckt.
- Sie kann einfach ausgefüllt und um spezifische Institutsbedürfnisse ergänzt werden.

Philosophie der Musterpolicy:

- **Verkehr von innen nach außen wird wenig reglementiert**
  - Nur sicherheitsrelevante Ports werden verboten.
  - Ungehindertes Arbeiten soll möglich sein.

- **Verkehr von außen nach innen wird viel stringenter behandelt:**
  - Nur was unbedingt nötig ist, wird erlaubt.
  - Alles Andere wird verboten.

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- **Vorbereitende Tätigkeiten im RRZN:**
  - Vorbereitende Umstellung der Netzwerkkonfiguration: ca. 1 Woche.
  - Bereitstellung eines Accounts auf dem Logdaten-Server des RRZN.
  - Erstellung der Access-Listen: 1-2 Tage.

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- **Vorbereitungen für den Logdaten-Transfer:**
  - Das RRZN stellt auf dem im RRZN betriebenen Logserver einen User mit einem Standard-Passwort bereit.
  - Dieser User muss vom Institut durch Vergabe eines geeigneten Passwortes „initialisiert“ werden.
  - Erst ab dann ist eine Übertragung der Logdaten möglich.

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- Es wird ein (günstiger) Termin für die Umstellung verabredet.
- Die Benutzer im Institut müssen informiert werden, da es durch die Umleitung auf jeden Fall zum Abbruch aktiver Verbindungen kommt.
- Für die Dauer der Umstellung muss ein Ansprechpartner im Institut telefonisch direkt erreichbar sein.
- Der Institutsverkehr wird am verabredeten Termin über die Firewall geleitet:
  - Dies erfolgt nach nochmaliger gegenseitiger Absprache.
- Die Firewall wird zunächst im Betriebsmodus „Stufe 1“ betrieben.

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Umstellung des Institutes mit einfachster Policy:

- Institut nennt die IPs der Rechner, die von außen erreichbar sein müssen.
- Verkehr von Innen nach Außen:
  - WinFS- und P2P-Ports werden gesperrt.
  - Alles andere ist erlaubt.
- Verkehr von Außen nach Innen:
  - Die IPs der Liste werden freigeschaltet.
    - Auf Wunsch des Institutes können auch hier schon Einschränkungen für einzelne freizuschaltende Rechner angegeben werden.
  - Zugriffe auf alle anderen IPs des Institutsnetzes werden verboten.

Formular für die Stufe 1-Policy:

Freizuschaltende Ips in Stufe 1 für das Subnetz 130.75.SUB.x-y

Zugriffe von Außen (aus dem UH-Netz und dem WWW ins Institutsnetz):

folgende Ips sollen für die Dauer der Stufe 1 komplett für den Zugriff von außen freigeschaltet werden (alle anderen Rechner des Institutsnetzes sind von außen nicht erreichbar).

Protokoll	Port	Quell-IP - „außen“	Ziel-IP - „innen“
ip	any	any	130.75.x.a 130.75.x.b 130.75.x.c

Haben Sie einen institutseigenen Mailserver? Ja [ ] Nein [X]

Zur Konfiguration Ihrer Firewall benötigen wir eine freie IP aus dem Subnetz, die uns als Management-IP zur Verfügung gestellt wird: Diese IP kann institutsintern dann **nicht** mehr für andere Zwecke vergeben werden.

Bitte tragen Sie hier die Management-IP ein: 130.75.x.y

Muster

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Standard: Komplette Freischaltung:

Protokoll	Port	Quell-IP - „außen“	Ziel-IP - „innen“
ip	any	any	130.75.x.a 130.75.x.b 130.75.x.c

Alternativ: Einschränkungen für einzelne, freizuschaltende Rechner:

Protokoll	Port	Quell-IP - „außen“	Ziel-IP - „innen“
tcp	http https	any / 130.75.x.x / andere IPs	130.75.x.a 130.75.x.b
tcp	ssh	Any / 130.75.x.x / andere IPs	130.75.x.c

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Auszug aus FW-ACL am Outside-Interface : access-list outside_access_in

```
object-group network IPs-Stufe1-INST-HG
  network-object host 130.75.x.r1
  network-object host 130.75.x.r2
object-group network www-INST-HG
  network-object host 130.75.x.r3
…
object-group service www-TCP-SG
  port-object eq www
  port-object eq https
…
 access-list outside_access_in extended permit tcp any object-group www-INST-HG eq object-group www-TCP-SG log
access-list outside_access_in extended permit ip any object-group IPs-Stufe1-INST-HG log
…
access-list outside_access_in extended deny ip any any log
```

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Auszug aus FW-ACL am Inside-Interface: access-list inside_access_in

… permit tcp any object-group Mailserver-RRZN-HG object-group Mailuser-send-empf-SG

… permit tcp any any object-group TCP-allgemein-SG

:

Regeln für DNS- , Time- , Datensicherungs- ,Lizenz-Server, ... im RRZN

:

… deny tcp any any object-group WinFS-TCP-SG log

… deny tcp any any object-group P2P-tcp-SG

… permit tcp any gt 1024 any log

:

… permit ip any any log

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Vorteile:

- Lässt sich für Institut und RRZN schnell realisieren:
  - Sobald das Institut die freizuschaltenden IPs benannt hat, kann die Realisierung meistens im Laufe von 1 Woche erfolgen.
- Auch diese rudimentäre Policy bringt schon eine sehr akzeptable Schutzfunktion.
- Obwohl die manchmal zeitaufwendige Verkehrsanalyse im Institut noch nicht komplett abgeschlossen ist, kann das Institutsnetz schon geschützt werden.
- Das Institut bezieht schon Logdaten, diese können bei der Analyse hilfreich sein.

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Ab dem Umstellungstermin ist institutsseitig Folgendes zu erledigen:

- Anhand der Logdaten kann der Verkehr analysiert werden:
  - Für jeden freigeschalteten Rechner wird untersucht, welche Ports genau für den Zugriff freigegeben werden müssen.
  - Welche Verbindungen sind noch explizit zu verbieten (zur Verminderung des Logdatenaufkommens).
- Aus den Ergebnissen dieser Analysen ergeben sich die verfeinerten Regeln für Stufe 2.
- Diese neuen oder angepassten Regeln pflegt das RRZN bei Übergang zu Stufe 2 im Firewall-System ein.

Zentraler RRZN-Netzschutz: Stufe2

R|R|Z|N

Der Übergang zu Stufe 2 hängt von folgenden Faktoren ab:

- Verkehrsanalyse im Institut ist abgeschlossen.
- Personelle Situation im Institut .
- Situation im RRZN / Zustand der Warteliste.
- Das Institut wünscht den Übergang zu Stufe 2.
- Das Institut wünscht den Übergang zu Stufe 2 nicht.
  - Nachsicht bei Verkehr von Innen nach Außen.
  - **Vorsicht** bei Verkehr von Außen nach Innen: Regeln für die Zugriffe auf die Server **sollten** angepasst werden!

Zentraler RRZN-Netzschutz: Stufe2

R|R|Z|N

vorgeschlagene Standard-Regeln für den Verkehr aus dem Institutsnetz nach aussen

- **erlaubt:**
  - Zugriffe auf die Dienste des RRZN
    - Mail, DNS, Time, News, Lizenzserver, Anwendungsserver, SAP-Server;
    - Backup (Asterix) Daten-Restore;
  - Mail holen vom studserv.
  - Allgemeine Netzdienste (Zugriff weltweit erlaubt)
    - http, https, ssh, telnet, ftp,
  - Zugriffe von Innen auf alle Ports über 1024 weltweit
    - es kann empfehlenswert sein diese Regel nicht zu aktivieren (z.B. für CIP-Pools)

- **verboten:**
  - Windows-Filesystem-Dienste P2P-Ports
  - Mail versenden/holen über andere Server außer RRZN-Server und studserv (Ausnahmen sind möglich).

Zentraler RRZN-Netzschutz: Stufe2

R|R|Z|N

Zugriffe von Innen (aus dem Institutsnetz nach „außen“):

	Protokoll /Dienst	Port	Quell-IP - „innen“	Ziel-IP - „außen“	Zweck
1	Mail:SMTP	25	IP des Mail-Servers	Mail-Server RRZN	Institutseigener Mailserver sendet Mail über RRZN
2	Mail: pop	110	Alle	Mailserver RRZN und 130.75.176.2	falls kein institutseigener Mailserver vorhanden ist 130.75.176.2 = studserv
3	Mail: imap	143	Alle	Mailserver RRZN und 130.75.176.2	
4	SSH	22	Alle	Alle	
5	HTTP	80	Alle	Alle	
6	HTTPS	443	Alle	Alle	
7	tcp/nntp	119	Alle	Newsserver RRZN	News
8	udp/ntp	123	Alle	Time-Server RRZN	Zeitsynchronisation
9	ICMP		Alle		echo, echo request
	FTP	21	Alle	Alle	
10	DNS	53	Alle	DNS-Server RRZN	
11	TCP	3299	IP des SAP-Gerätes	SAP-Server	SAP-Zugriff
12	TCP		Instituts-IPs	Asterix	Backup
13	TCP		alle? spezielle IPs	Lizenzserver RRZN	
14					

Muster

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Auszug aus FW-ACL am Inside-Interface: access-list inside_access_in

… permit tcp any object-group Mailserver-RRZN-HG object-group Mailuser-send-empf-SG

… permit tcp any any object-group TCP-allgemein-SG

:

Regeln für DNS- , Time- , Datensicherungs- ,Lizenz-Server, ... im RRZN

… deny tcp any any object-group WinFS-TCP-SG log

… deny tcp any any object-group P2P-tcp-SG

… permit tcp any gt 1024 any log

:

(… permit ip any any log) wird ersetzt durch:

… deny ip any any log

Zentraler RRZN-Netzschutz: Stufe2

R|R|Z|N

vorgeschlagene Standard-Regeln für den Verkehr von außen in das Institutsnetz

- **erlaubt:**
  - Zugriffe auf die Server des Institutes
    - Mail, Web, SSH, DNS, ...
  - Backup (Asterix), Datensicherung;
  - Zugriffe von den Mailserver des RRZN über Port 25
  - Ev. Anwendungs-Server des RRZN;

- **verboten:**
  - prinzipiell alles, was nicht explizit erlaubt ist
  - speziell: Windows-Filesystem-Dienste
  - speziell: P2P-Ports

Zentraler RRZN-Netzschutz: Stufe2

R|R|Z|N

Zugriffe von Außen (aus dem UH-Netz und dem WWW ins Institutsnetz):

	Protokoll /Dienst	Port	Quell-IP - „außen“	Ziel-IP - „innen“	Zweck
1	Mail : Pop3/Imap	110/ 143	alle	IP des Mailservers	Mail abholen vom Instituts-Mailserver
2	Mail/ident	25/113	Mail-Server RRZN	IP des Mailservers	RRZN sendet Mail an Instituts-Mailserver
3	SSH	22	Alle	IP des SSH-Servers	Zugriff auf SSH-Server
4	FTP	21	Alle	IP des FTP-Servers	Zugriff auf FTP-Server
5	HTTP	80	Alle	IP des WWW-Servers	
6	HTTPS	443	Alle	IP des WWW-Servers	
7	eventuelleDienste, die angeboten werden	???	Alle?	IP des Servers, der den Dienst anbietet	z.B. eigener News-Server, DNS-Server
8	tcp		Asterix	Instituts-IPs	Backup
9	tcp	6000 bis 6063	Anwendungsserver RRZN	keine ? alle ? spezielle Ips ?	für Zugriffe auf spezielle Software auf RRZN-Rechnern (Maple, Partran, Abaqus .....)
10					

Muster

Zentraler RRZN-Netzschutz: Nachbessserung

R|R|Z|N

- Eventuell nicht mehr funktionierende Anwendungen müssen auf Zusammenhang mit der Scharfschaltung der Firewall untersucht werden.
- Um nicht funktionierende Zugriffe in den Logdaten finden zu können, sind folgende Daten hilfreich :
  - Zugriffszeitpunkt
  - IP des ausführenden Rechners
  - nicht funktionierende Anwendung/Dienst
  - wenn möglich die IP des Zielsystems
- Haben Sie herausgefunden, welche Kommunikation noch erlaubt werden muss, melden Sie dies per E-Mail Ihren Ansprechpartnern im RRZN, damit die nötigen Regeln eingepflegt werden.
- Sollten sich Schwierigkeiten bei der Problem-Einkreisung ergeben, wenden Sie sich an das RRZN, dann kann auch ein „Live-Zugriff“ untersucht und überwacht werden.

Die Analyse der Logdaten liegt im Aufgabenbereich des Institutes.

Dazu einige prinzipielle Anmerkungen:

- Logdaten sind sensible Daten!
- Es lassen sich unter Umständen Rückschlüsse auf einzelne Personen ziehen.
  - Damit unterliegen Logdaten dem Datenschutz und es existieren gewisse Auflagen, wie mit ihnen umgegangen werden muss.
- Das Erkennen von Sicherheitsproblematiken ist der einzige Grund für das Sichten von Logdaten.
- Die Kontrolle über die Logdaten sollte auf jeden Fall ein Mitarbeiter des Institutes innehaben, der auf das Datengeheimnis verpflichtet wurde.
- Dieser Mitarbeiter sollte sich seiner Verantwortung bewusst sein.

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

- Vom Sicherheitsaspekt her ist die Analyse der Logdaten von nicht zu unterschätzender Wichtigkeit:
  - Nur durch regelmäßige Sichtung der Logdaten können Unregelmäßigkeiten rechtzeitig erkannt werden.
  - Auch wenn sich „nichts“ tut: nur durch regelmäßige Beschäftigung mit den Logdaten bekommt man ein Gespür für den „normalen“ Verkehr.
- Service des RRZN: grafische und tabellarische Aufbereitung der Logdaten:
  - allgemeine Tagesübersicht: Wie war das Verkehrsaufkommen über den Tag verteilt.
  - verschiedene tabellarische Auswertungen
  - Die Logdaten-Auswertungen sind auf einer Webseite einsehbar (Username / Passwort erforderlich).

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

Beispiel für eine Tagesübersicht (Werktag):

5er-Netz RRZN am Di. 01. Nov 2005

logx 2005/09/14 H.Kessener RRZN

Tagesverlauf

Stunde	Verbindungen		Volumen [Bytes]	
	eingehend	ausgehend	eingehend	ausgehend
0	40	542	182.361.831	23.803.812
1	33	618	25.409	9.769.542
2	36	622	395.201.239	13.488.367
3	36	611	49.785	8.963.173
4	103	618	203.500	45.208.641
5	51	701	5.077.062	9.584.944
6	35	1.458	25.887	33.923.941
7	42	4.202	26.860	198.526.179
8	73	9.150	5.334.456	405.300.983
9	115	8.962	3.423.544.010	505.252.578
10	133	10.589	72.654.368	948.005.574
11	281	11.910	8.194.304.173	1.106.807.684
12	145	11.257	2.927.257.665	593.539.022
13	100	9.471	6.368.516	377.554.208
14	132	12.385	11.822.779	1.119.766.185
15	192	11.369	2.580.257.787	1.746.595.563
16	166	10.016	4.363.694	703.816.504
17	76	3.656	1.730.399.825	683.666.045
18	32	2.873	105.377	59.834.281
19	30	1.896	25.227	21.594.949
20	32	2.114	8.052.025	25.301.368
21	24	1.618	23.858	171.617.074
22	28	783	776.967.596	13.276.013
23	37	771	844.829.041	28.722.590
Summe	1.972	118.192	21.169.281.970	8.853.919.220

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

Beispiel für eine Tagesübersicht (Wochenende):

5er-Netz RRZN am So. 30. Okt 2005

logx 2005/09/14 H.Kessener RRZN

Tagesverlauf

Stunde	Verbindungen		Volumen [Bytes]	
	eingehend	ausgehend	eingehend	ausgehend
0	33	439	25.409	5.816.593
1	0	0	0	0
2	73	907	2.343.053.108	89.514.911
3	33	443	26.478	5.869.569
4	122	441	3.553.775.401	60.724.565
5	37	444	2.595.471	5.820.735
6	32	438	24.530	5.893.615
7	34	441	25.492	5.881.487
8	34	498	26.303	5.956.950
9	34	440	27.006	5.818.446
10	32	446	24.530	6.128.716
11	34	443	120.543	5.900.391
12	37	442	5.027.402.575	57.549.671
13	33	442	25.408	5.863.857
14	52	441	5.161.712	6.578.393
15	33	438	30.780	5.841.815
16	32	440	24.560	5.852.380
17	33	440	24.529	5.972.424
18	37	441	27.873	5.858.762
19	33	440	25.166	5.806.752
20	52	464	27.005	6.578.437
21	32	437	24.528	5.838.390
22	35	444	74.916	5.957.964
23	32	443	24.528	6.039.331
Summe	939	10.692	10.932.597.851	327.064.154

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

Detaillierte Auswertungen (Top-50)								
Hosts	**extern**				**intern**			
	nach Verbindungen		nach Volumen		nach Verbindungen		nach Volumen	
	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend
Verbindungen	**eingehend**				**ausgehend**			
	nach Volumen		nach Dauer		nach Volumen		nach Dauer	

Top-50 Hosts extern nach Volumen ausgehend

Nr.	Host	Verbindungen	Bytes
1	[illegible]	47	2.924.778.156
2	[illegible]	4.563	1.538.269.663
3	[illegible]	8	1.144.293.905
4	[illegible]	13	1.118.209.747
5	[illegible]	12.377	658.501.421
6	[illegible]	753	548.450.748
7	[illegible]	182	271.083.246
8	[illegible]	4	244.242.835
9	[illegible]	16	231.348.554
10	[illegible]	2	162.965.852
11	[illegible]	2	148.236.190
12	[illegible]	3	144.944.657
13	[illegible]	347	134.619.350
14	[illegible]	1.470	133.006.482
15	[illegible]	10	120.668.675
16	[illegible]	1.988	112.604.705
17	[illegible]	430	111.701.286

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

Detaillierte Auswertungen (Top-50)								
Hosts	**extern**				**intern**			
	nach Verbindungen		nach Volumen		nach Verbindungen		nach Volumen	
	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend
Verbindungen	**eingehend**				**ausgehend**			
	nach Volumen		nach Dauer		nach Volumen		nach Dauer	

Top-50 Hosts extern nach Verbindungen eingehend

Nr.	Host	Verbindungen	Bytes
1	[illegible]	574	570.672
2	[illegible]	486	5.702.167
3	[illegible]	341	33.956.440
4	[illegible]	283	33.820
5	[illegible]	96	8.521.468.252
6	[illegible]	51	586.242
7	[illegible]	36	2.736
8	[illegible]	36	184.174
9	[illegible]	30	2.352
10	[illegible]	27	2.610.473
11	[illegible]	27	1.068.226
12	[illegible]	24	19.614.559
13	[illegible]	16	119.804
14	[illegible]	12	216
15	[illegible]	9	392.304
16	[illegible]	8	408.392
17	[illegible]	8	4.192
18	[illegible]	7	939.636.510

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

- Durch die tabellarische Aufbereitung kristallisiert sich über Tage und Wochen eine Rangfolge heraus:
  - Mit der Zeit bekommen Sie ein Gespür dafür, welche Rechner „zu Recht“ auf den Top-Plätzen stehen.
  - Es fällt auf, wenn dort plötzlich ein Rechner auftaucht, der an dieser Stelle eigentlich nichts zu suchen hat.

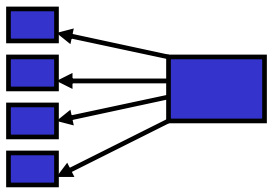
- Rechner oder Tageszeiten, die in der Logdaten-Auswertung auffallen, können nun gezielt in den Logdaten genauer untersucht werden.

Zentraler RRZN-Netzschutz: Logdaten

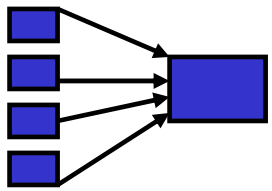
R|R|Z|N

Detaillierte Auswertungen (Top-50)								
Hosts	**extern**				**intern**			
	nach Verbindungen		nach Volumen		nach Verbindungen		nach Volumen	
	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend
Verbindungen	**eingehend**				**ausgehend**			
	nach Volumen		nach Dauer		nach Volumen		nach Dauer	

- Top50-Liste der externen Hosts mit den meisten Verbindungen
  - eingehend
  - ausgehend

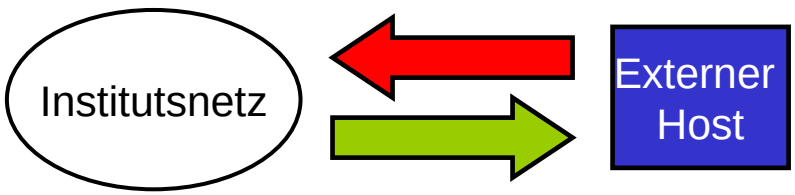


Scan?



Datenspionage?
Adware?

- Top50-Liste der externen Hosts mit dem größten Transfervolumen
  - eingehend
  - ausgehend

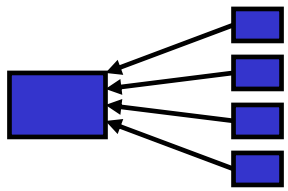


Zentraler RRZN-Netzschutz: Logdaten

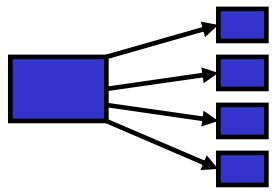
R|R|Z|N

Detaillierte Auswertungen (Top-50)								
Hosts	**extern**				**intern**			
	nach Verbindungen		nach Volumen		nach Verbindungen		nach Volumen	
	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend
Verbindungen	**eingehend**				**ausgehend**			
	nach Volumen		nach Dauer		nach Volumen		nach Dauer	

- Top50-Liste der internen Hosts mit den meisten Verbindungen
  - eingehend
  - ausgehend

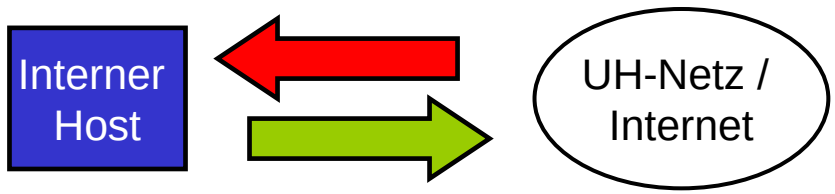


DOS?
Backdoor?



Wurm
Virus?

- Top50-Liste der internen Hosts mit dem größten Transfervolumen
  - eingehend
  - ausgehend



RRZN-Empfehlung: Erweiterung der Instituts-Security-Policy:

Ein Soll:

- Personal Firewalls als zusätzlichen Schutz auf jedem Rechner.

Ein Muss:

- Personal Firewalls auf Laptops.

Über Laptops wird Schadsoftware oft auf dem „Schleichweg“ an der Firewall und den Firewallregeln vorbei ins Institutsnetz eingeschleust.

Begleitende Sicherheitsmaßnahmen

R|R|Z|N

- Personal Firewalls sind verfügbar als
  - im System bereits integrierte Software z.B.
    - Windows-XP-Firewall
    - Iptables bei Linux
  - zusätzliche, kostenpflichtige oder auch frei erhältliche Software
    - Agnitum Outpost (freie Version 1.0)
      http://www.agnitum.com/products/outpostfree/index.php
    - Neu: Sophos Client Firewall (Beta-Version)
      http://www.sophos.de/products/tp/client-firewall/
- Informationen auf den Security-Webseiten des RRZN:
  http://www.rrzn.uni-hannover.de/firewall.html

Sicherheit kann nicht ohne sicherheitsbewusstes Verhalten der Anwender erreicht werden!

Verhaltensempfehlungen für Anwender erforderlich, z. B.

- zum Passwortgebrauch
- zu Einsatz und Update von Anti-Viren-Software

  http://www.rrzn.uni-hannover.de/sophos_remote_update.html
- zum Internet-Gebrauch (Web, Browser, Downloadverhalten, Mail, ...)
- Informationsmöglichkeiten über aktuelle Sicherheitsprobleme einzelner Hersteller http://www.rrzn.uni-hannover.de/abo_sec_mails.html
- Sichere Systeme durch regelmäßiges Installieren von Sicherheitsupdates

  http://www.rrzn.uni-hannover.de/its_sus.html
- Wer ist bei auffälligen Vorkommnissen zu benachrichtigen?

Empfehlenswert: Verteilen Sie Informationen zur Anwendersicherheit in Ihrem Institut:

- Folien des RRZN-Kurses „Sicherheit für Anwender“

  http://www.rrzn.uni-hannover.de/sicherheitstage.html

- Flyer zur IT-Sicherheit mit Tipps und Angeboten des RRZN zum sicheren Betrieb von Rechnern; Download einer Kopiervorlage unter:

  http://www.rrzn.uni-hannover.de/it_sicherheit.html

- Merkblatt zum RRZN-Netzschutz mit den wichtigsten Regeln für ein sicherheitskonformes Anwenderverhalten. Das Merkblatt ist verfügbar unter auf der Webseite zum RRZN-Netzschutz unter „Dokumente zum Download“

  http://www.rrzn.uni-hannover.de/netzschutz.html

Interesse am RRZN-Netzschutz?

R|R|Z|N

Wir hoffen auf zahlreiche neue Teilnehmer!

Melden Sie sich bei Christine Peter;
per E-Mail: peter@rrzn.uni-hannover.de
oder telefonisch: 8021

http://www.rrzn.uni-hannover.de/netzschutz.html