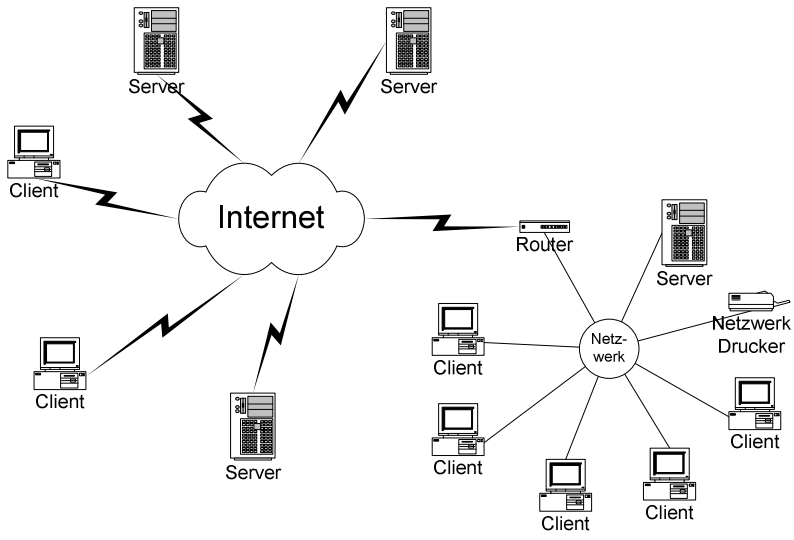
Linux als Firewall

VHS Düsseldorf

Guido Petermann

FW - Infrastruktur



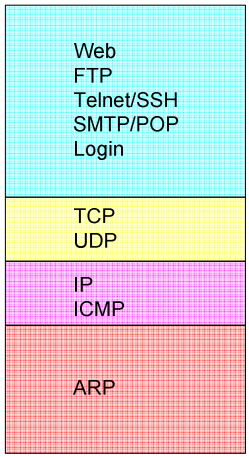
FW - OSI Referenzmodell

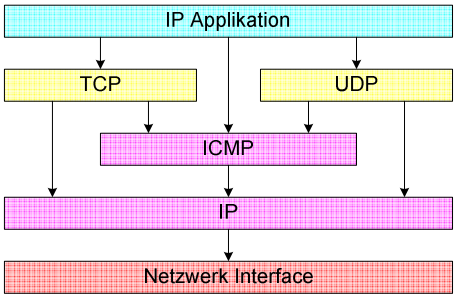
7	**application layer**	Verarbeitungsschicht	Anwendungsunterstützung
6	**presentation layer**	Darstellungsschicht	Interpretation, Konvertierung
5	**session layer**	Kommunikationsschicht	Prozessverbindung
4	**transport layer**	Transprotschicht	Punkt zu Punkt-Verbindung
3	**network layer**	Vermittlungsschicht	Verbindungsaufbau
2	**data link layer**	Sicherungsschicht	Pakete, Fehlererkennung
1	**physical layer**	Bitübertragungsschicht	Kabel, Hardware

FW - OSI <-> Internetprotokoll

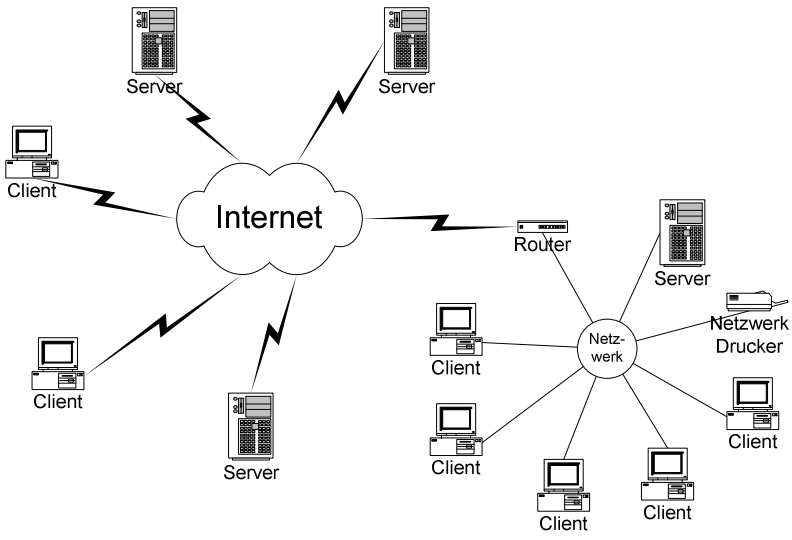
7	**application layer**	Applikations Schicht	Web FTP Telnet/SSH SMTP/POP Login
6	**presentation layer**		
5	**session layer**		
4	**transport layer**	Transport Schicht	TCP UDP
3	**network layer**	Internet Schicht	IP ICMP
2	**data link layer**	Netzwerk Schicht	ARP
1	**physical layer**		Medium

FW - IP Schichten

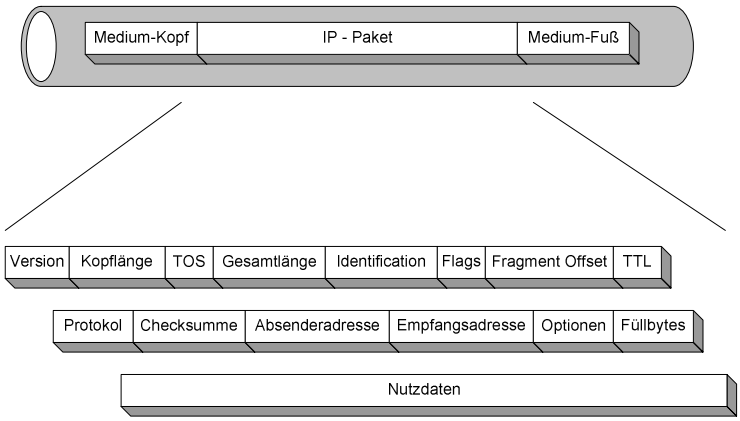




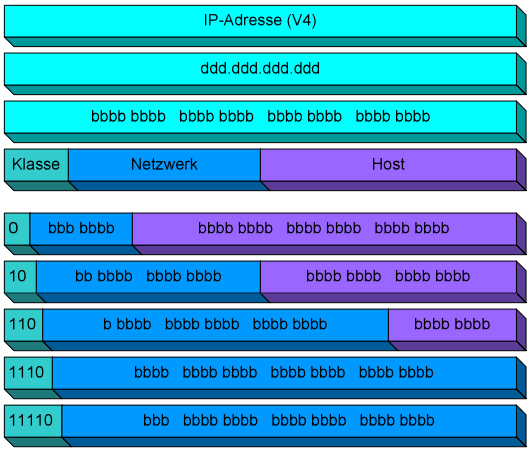
FW - HUB / Switch



FW - IP Aufbau



FW - IP Adressaufbau



32 Bit Adressaufbau

Dezimalschreibweise Bsp 210.120.6.67

Bitweiser Aufbau

Aufteilung in Klasse, Netzwerk, Host

A - Klasse Adresse (24-Bit Hostadresse)

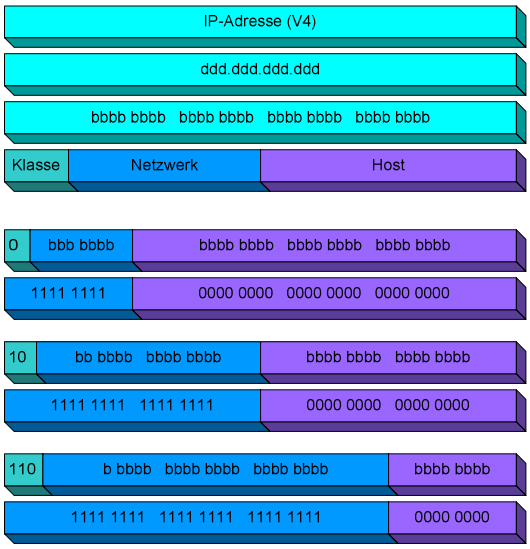
B - Klasse Adresse (16-Bit Hostadresse)

C - Kasse Adresse (8-Bit Hostadresse)

D - Multicast Adresse

E - undefiniert

FW - IP Subnet Mask



32 Bit Adressaufbau

Dezimalschreibweise Bsp 210.120.6.67

Bitweiser Aufbau

Aufteilung in Klasse, Netzwerk, Host

A - Klasse Adresse (24-Bit Hostadresse)

255.0.0.0

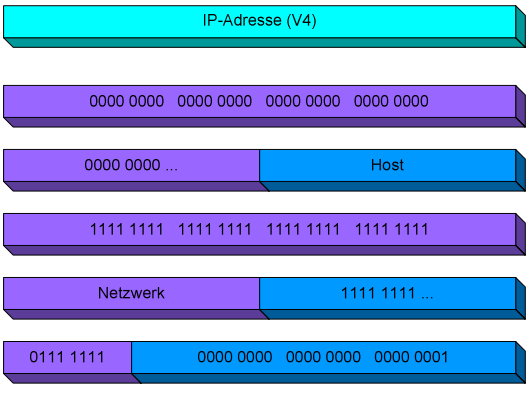
B - Klasse Adresse (16-Bit Hostadresse)

255.255.0.0

C - Kasse Adresse (8-Bit Hostadresse)

255.255.255.0

FW - IP Besondere Adressen



Host selbst Bsp 0.0.0.0

Host im aktuellen Netz Bsp 0.0.0.65

Broadcast für das aktuellen Netz

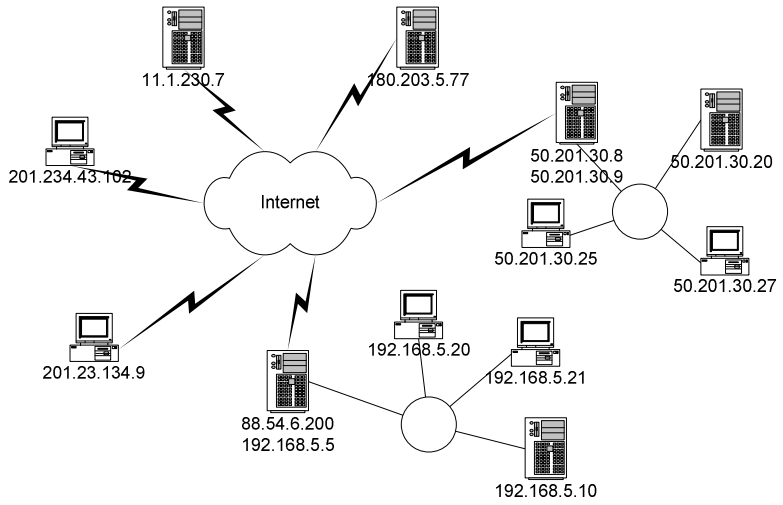
Broadcast für das Netzwerk Bsp 210.70.255.255

Loopback Bsp 127.0.0.1

Private IP-Adressen

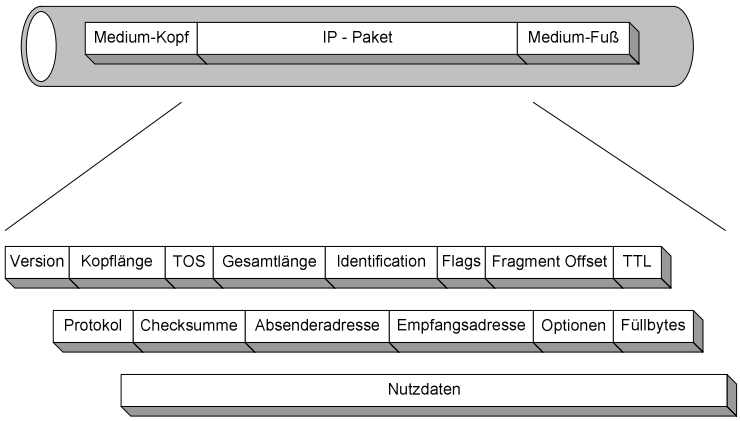
10.0.0.0 - 10.255.255.255 (Klasse A)
172.16.0.0 - 172.31.255.255 (Klasse B)
192.168.0.0 - 192.168.255.255 (Klasse C)

FW - Eindeutige IP-Adressen

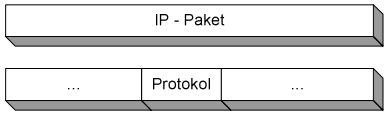


FW – IP Adressierung Übung

FW - IP Aufbau

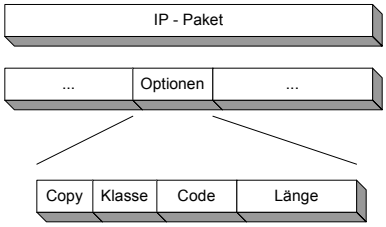


FW - IP Protokolle



Protokollcode	Protokoll
1	ICMP - Internet Control Message
2	IGMP - Internet Group Management
3	GGP - Gateway-to-Gateway
6	TCP - Transmission Control
8	EGP - Exterior Gateway
17	UDP - User Datagramm

FW - IP Optionen



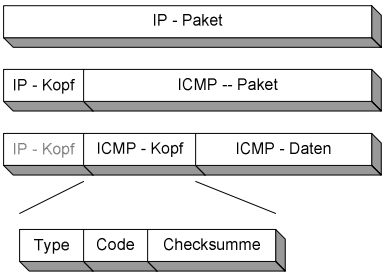
Copy	Optionen fragmentieren (1/0)

Klasse - Code - Länge K - C - L	
0 - 0 - 0	Ende der Option
0 - 1 - 0	Platzhalter (ohne Bedeutung)
0 - 2 - 11	reserviert
0 - 3 - ??	Vorgegebene Route verfolgen
2 - 4 - ??	Zeitstempel vom Router erhalten
0 - 7 - ??	Route aufzeichnen
0 - 9 - ??	zwingend Vorgegebene Route verfolgen

FW - IP ICMP

Internet Control Message Protocol

Status und Betriebsstörungen melden



Type	
0	Echo Reply - Antwort auf Echo
3	Destination Unreachable - Ziel nicht erreichbar
4	Source Quench - Netzwerküberlastung
5	Redirect - Aufforderung anderen Router zu nutzen
8	Echo - Echo Anfrage
9	Router Advertisement - Router IP-Adresse
10	Router Solicitation - Router IP-Adresse anfordern
11	Time Exceeded - IP Zeitlimit erreicht
12	Parameter Problem - IP-Kopf fehlerhaft
13	Timestamp - Host Uhrzeit anfordern
14	Timestamp Reply - Antwort auf Timestamp
15	Information Request - Abfrage der Netzwerknr.
16	Information Reply - Antwort auf Inform. Request
17	Address Mask Request - Anfrage der Subnet-Mask
18	Address Mask Reply - Antwort auf Add. Mask Req.

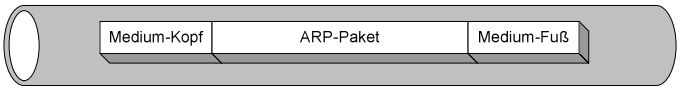
Beispielcode für Type 3 - Destination Unreachable

Code	
0	Netz nicht erreichbar
1	Host nicht erreichbar
2	Protokoll nicht erreichbar
3	Port nicht erreichbar
4	Fragmentierung notwendig
5	Route fehlerhaft
6	Netz nicht bekannt
7	Host nicht bekannt
8	Host isoliert
9	Netzzugriff wurde verwehrt
10	Hostzugriff wurde verwehrt
11	Netz nicht erreichbar (TOS)
12	Host nicht erreichbar (TOS)

FW - IP ARP

Address Resolution Protocol

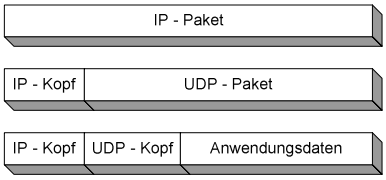
IP-Adressen <-> physikalische Netzadressen



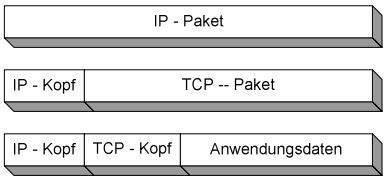
Parket Aufbau
- Hardware Adress Art
- Protokoll Adress Art
- Länge der Hardware Adresse
- Länge der Protokoll Adresse
- Befehl
- Hardware Adresse Sender
- Protokoll Adresse Sender
- gesuchte Hardware Adresse
- gesuchte Protokoll Adresse

FW - IP ICMP/ARP Übung

FW - IP UDP/TCP



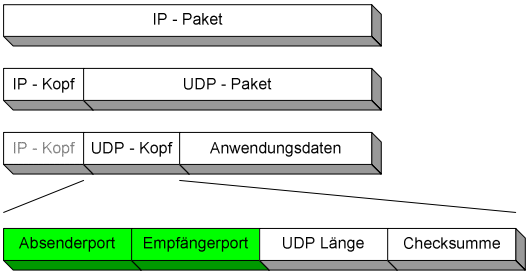
User Datagram Protokoll
ungesicherte Kommunikationsverbindung



Transport Control Protocol
gesicherte Kommunikationsverbindung

FW - IP UDP

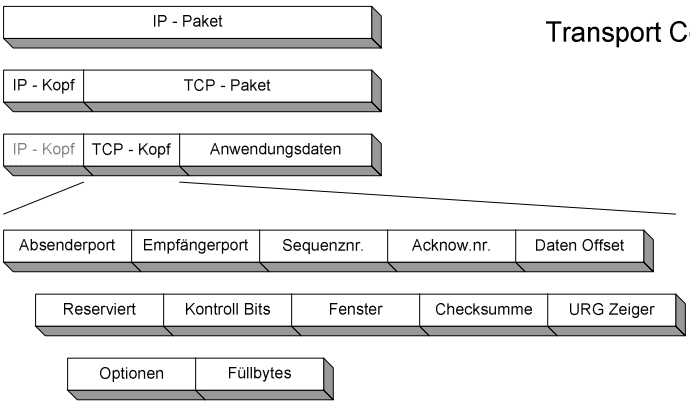
User Datagram Protokoll



Anwendungen adressieren die Pakete über IP- und Port-Adresse

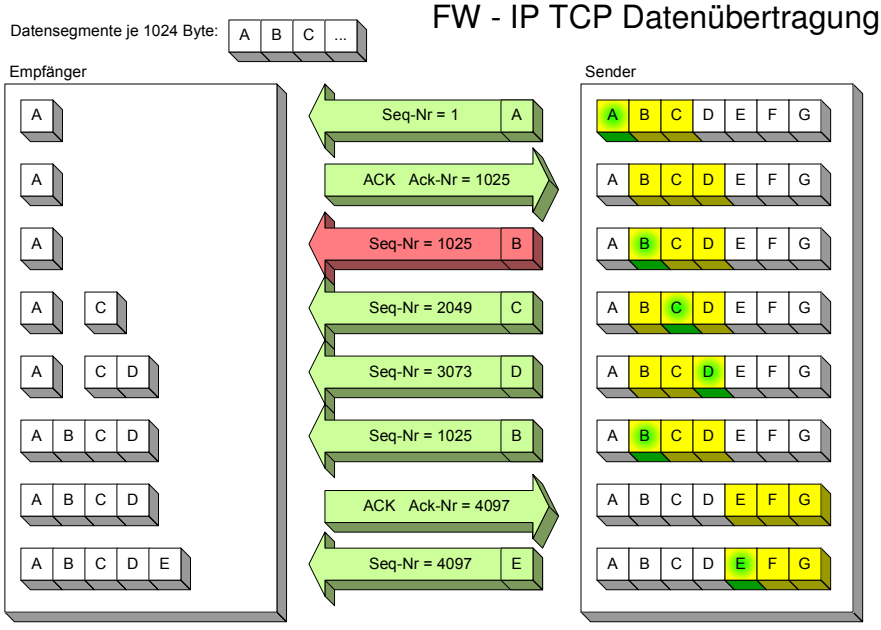
FW - IP TCP

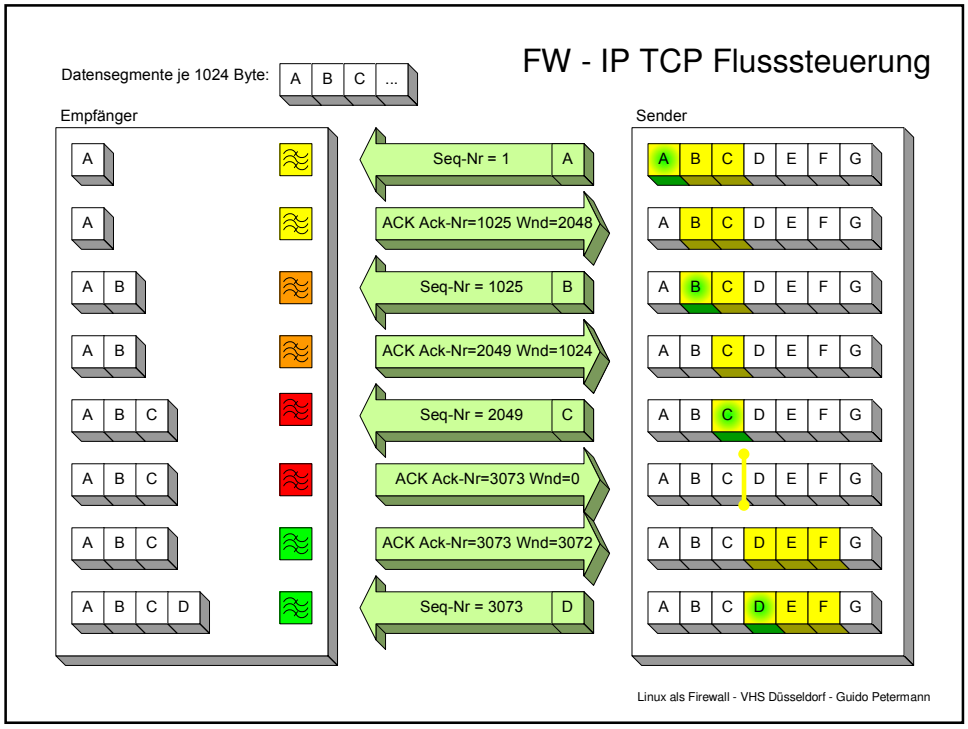
Transport Control Protocol

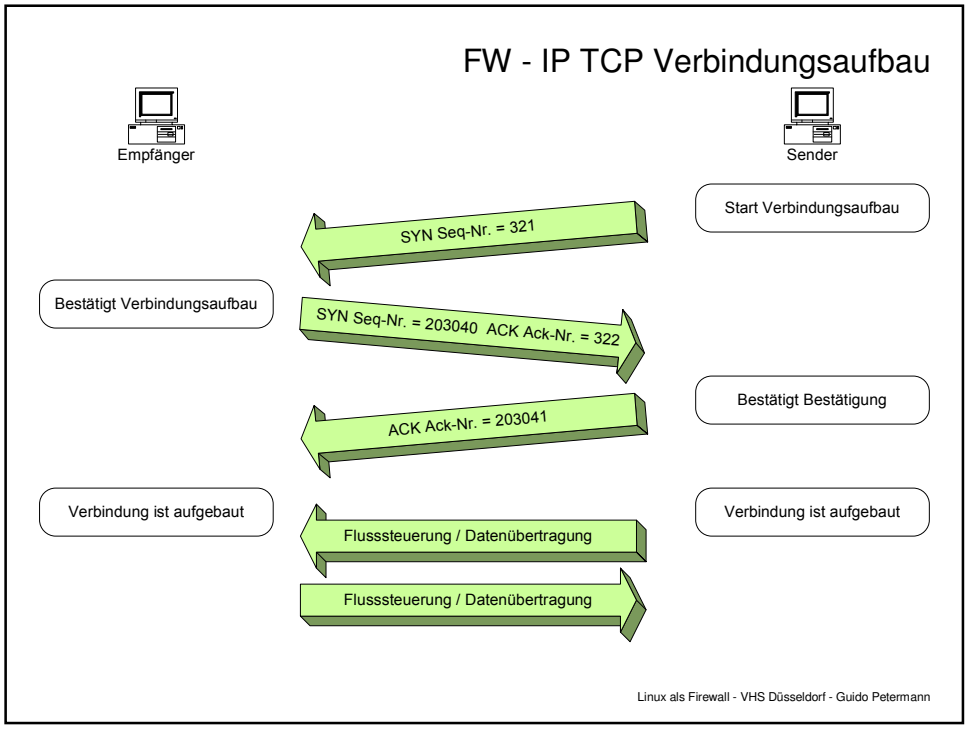


Kontroll Bits
URG - Urgent, Dringend (-> URG-Zeiger)
ACK - Acknowledge, Bestätigung
PSH - Push, Sofort Weitergeben
RST - Reset, Zurücksetzen
SYN - Sync, Verbindungsaufbau und Synchronisation
FIN - Finish, Beenden

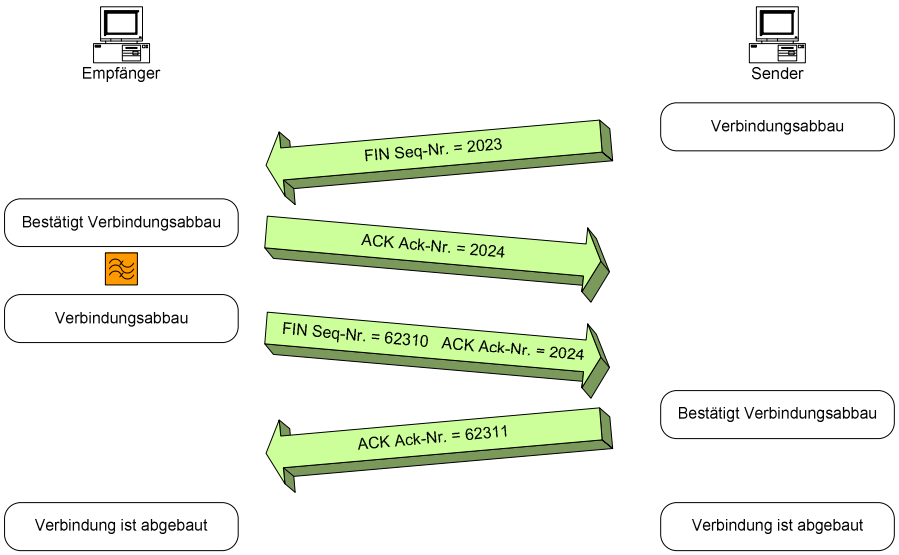
FW - IP TCP Datenübertragung



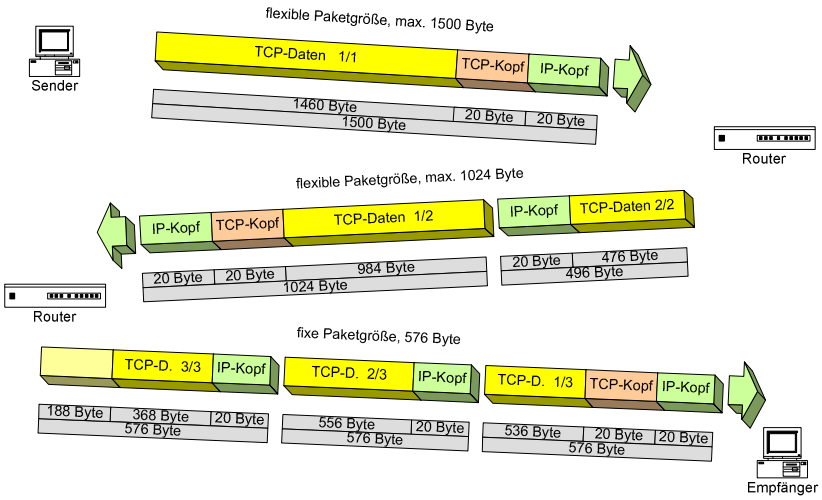

FW - IP TCP Flusssteuerung
Datensegmente je 1024 Byte:
A B C ...
Empfänger
Sender
Seq-Nr = 1 A
ACK Ack-Nr=1025 Wnd=2048
Seq-Nr = 1025 B
ACK Ack-Nr=2049 Wnd=1024
Seq-Nr = 2049 C
ACK Ack-Nr=3073 Wnd=0
ACK Ack-Nr=3073 Wnd=3072
Seq-Nr = 3073 D
Linux als Firewall - VHS Düsseldorf - Guido Petermann


FW - IP TCP Verbindungsaufbau
Empfänger
Sender
Start Verbindungsaufbau
SYN Seq-Nr. = 321
Bestätigt Verbindungsaufbau
SYN Seq-Nr. = 203040 ACK Ack-Nr. = 322
Bestätigt Bestätigung
ACK Ack-Nr. = 203041
Verbindung ist aufgebaut
Verbindung ist aufgebaut
Flusssteuerung / Datenübertragung
Flusssteuerung / Datenübertragung
Linux als Firewall - VHS Düsseldorf - Guido Petermann

FW - IP TCP Verbindungsabbau



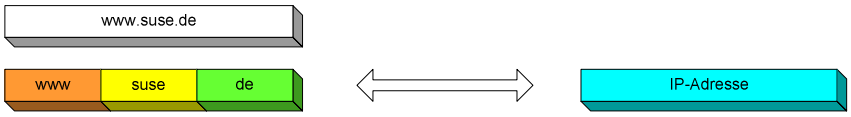
FW - IP TCP Paketgröße



FW - IP Dienste/Anwendungen

- DNS - Domain Name System
- FTP - File Transfer Protokoll
- SSH - Secure Shell
- Telnet
- SMTP - Simple Mail Transfer Protocol
- POP - Post Office Protocol
- SNMP - Simple Network Management Protocol
- Gopher
- Finger
- HTTP - Hypertext Transport Protocol
- NNTP - Network News Transfer Protocol
- DHCP - Dynamic Host Configuration Protocol
- NFS - Network File System

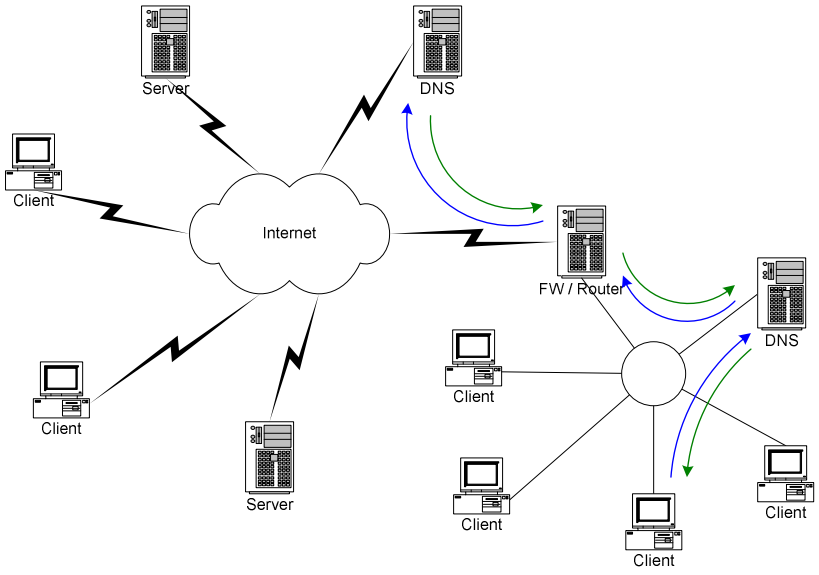
FW - IP DNS



Top-Level-Domain	de, com, net, org, gov, edu, fr, it, ...
Second-Level-Domain	suse, spiegel, duesseldorf, ibm, microsoft, ...
Rechnername / Gruppe	www, ftp, otto, … / support, einkauf, de, ...

Whois über: www.internic.net, www.nic.com, www.denic.de, (www.iana.com)

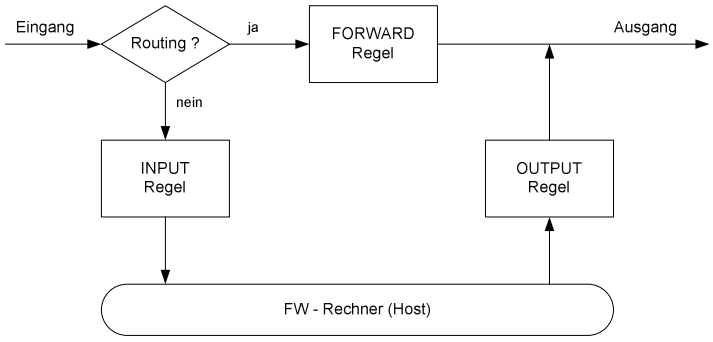
FW - IP DNS



FW - IP DNS Übung

iptables

(ab Kernel 2.4.x)



Filterregeln werden in Filterregelnketten (chains) mithilfe des Befehls iptables zusammengefaßt

FW - Filterregeln Aufbau

Grundaufbau von Filterregeln

Filterregeln werden in Filterregelnketten (chains) mithilfe des Befehls iptables zusammengefaßt

FW - Filterregeln Operation

Grundaufbau von Filterregeln

Filterregeln erweitern:	Anhängen	iptables -A chain rule ...	(Append)
	Einfügen	iptables -I chain position rule ...	(Insert)
Filterregeln löschen:	Passende	iptables -D chain rule ...	(Delete)
	Position	iptables -D chain position ...	(Delete)
	Alle	iptables -F [chain]	(Flush)
Filterreglen ändern:	Ersätzen	iptables -R chain position rule ...	(Replace)
Verschiedenes:	Standard Regelkette festlegen	iptables -P chain ...	(Policy)
	Zähler der Regelkette löschen	iptables -Z [chain]	(Zero)
	Regelkette umbenennen	iptables -E name_alt name_neu	(Exchange)
	Alle Regeln anzeigen	iptables -L [chain]	

FW - Filterregeln Regeln

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Protokolle:	TCP, UDP, ICMP	iptables -A chain -p proto	proto = tcp, udp oder icmp
	iptables -A INPUT -p udp		
Adressen:	Quell- bzw. Zieladresse	iptables -A chain -s source_ip iptables -A chain -d destination_ip	Quelladresse Zieladresse
	iptables -A INPUT -s 10.1.3.0/255.255.255.0 iptables -A INPUT -s 10.1.3.23 -d 10.1.1.102		
Interface:	Eingabe- bzw. Ausgabeinterface	iptables -A INPUT -i in_interface iptables -A FORWARD [-i in_interface] [-o out_interface] iptables -A OUTPUT -o out_interface	
	iptables -A OUTPUT -o eth0 iptables -A INPUT -i ippp+	Interfacegruppen mit „+“ möglich	
Fragmente:	Prüfung von fragmentierten Paketen (zweite bis letzte Paket) Die Angabe von Protokollen und des SYN-Flags sind nicht erlaubt	iptables -A INPUT -f ...	
Negation:	Negation über „!“ möglich		
	iptables -A chain -s ! 10.1.3.22	alle Quelladressen außer 10.1.3.22	
Erweiterungen:	...		

FW - Filterregeln Regelnerw. I

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Erweiterungen

TCP	Quellport	iptables … -p tcp --sport [!] port …	
	Zielport	iptables … -p tcp --dport [!] port …	
	port = Portname, Portnummer, Portbereich Bsp: www, 22, 4000:4050, :128, 1024:		
	Flags	iptables … -p tcp --tcp-flags [!] mask setflags	
	mask = Flags die geprüft werden sollen (SYN, FIN, RST, PSH, ACK, URG, ALL, NONE) setflags = Flags die gesetzt sein müssen (SYN, FIN, RST, PSH, ACK, URG, ALL, NONE)		
	iptables -A INPUT -p tcp --tcp-flags SYN,ACK SYN … iptables -A INPUT -p tcp --tcp-flags ALL NONE …		
	Verbindungsaufbau	iptables … -p tcp [!] --syn	(flags: SYN,RST,ACK SYN)
	Option	iptables … -p tcp ---tcp-option [!] option-nr	
	option-nr = Optionskennung		
UDP	Quellport	iptables … -p udp --sport [!] port …	
	Zielport	iptables … -p udp --dport [!] port ...	
	port = Portname, Portnummer, Portbereich Bsp: www, 22, 4000:4050, :128, 1024:		

FW - Filterregeln Regelnerw. II

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Erweiterungen

Multiport

Quellport	iptables … -p tcp|udp -m multiport --source-port port[,port] ...	
Zielport	iptables … -p tcp|udp -m multiport --destination-port port[,port] ...	
Quell-/Zielport identisch	iptables … -p tcp|udp -m multiport --port port[,port] ...	

port = Portname, Portnummer, Portbereich Bsp: www, 22, 4000:4050, :128, 1024:

ICMP

Type/Code — iptables … -p icmp --icmp-type [!] icmpspec

icmpspec = type[/code] Bsp. 8/0, echo-request

echo reply	Antwort auf Ping	0/0
destination unreachable	Ziel nicht erreichbar	3/x (x>0)
source quench	Ziel überlastet	4/0
redirect	Anderen Router benutzen	5/x (x>0)
echo request	Pinganfrage	8/0
time exceeded	Zeitüberschreitung	11/0

Verbindungszustand

Neu	iptables … -m state --state NEW …
Bestehend	iptables … -m state --state ESTABLISHED …
Notwendig	iptables … -m state --state RELATED …
Rest bzw. Fehlerhaft	iptables … -m state --state INVALID …

FW - Filterregeln Regelnerw. III

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Erweiterungen

Netzwerkadressen MAC-Adressen — iptables … -m mac --mac-source [!] mac-addr

iptables -A INPUT -m mac --mac-source 1B:20:3A:B4:FA:03 ...

Beschränkung

Mengen-/Zeitbeschränkung	iptables … -m limit …	default 5 Pakete, 20 Min
(Matching-Rate)	iptables … -m limit --limit rate …	

rate = x/s, x/m, x/h, x/d Bsp. 3/h entspricht 20 Minuten

iptables … -m limit-burst number …

Wenn die Anzahl der Pakete laut „limit-burst number“ erreicht wurde, wird alle „limt rate“ nur ein Paket verarbeitet. Solange bis „limit-burst number“ mal „limt rate“ kein Paket eintrifft.

Syn-Flood-Protection: iptables -A chain -p tcp --syn -m limit --limit 5/s

Owner-Prüfung

User ID	iptables … -m owner --uid-owner userid ...
Group ID	iptables … -m owner --gid-owner groupid ...
Process ID	iptables … -m owner --pid-owner processid ...
Session ID	iptables … -m owner --sid-owner sessionid ...

FW - Filterregeln Konsequenz

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Akzeptieren	iptables … -j ACCEPT	(jump to …)
Verwerfen	iptables … -j DROP	
Abweisen	iptables … -j REJECT iptables … -j REJECT --reject-with type	default: Port Unreachable
	type = icmp-net-unreachable, icmp-host-unreachable, icmp-unreachable, tcp-reset	
Regelkette verlassen	iptables … -j RETURN	
Paket an Anwendung weitergeben	iptables … -j QUEUE	
Zu (selbstdefinierter) Regelkette verzweigen	iptables … -j name	name = Name der Regelkette
Protokollieren	iptables … -j LOG	(logging)
Warnstufen (Syslog)	iptables … -j LOG --log-level syslog-prio	
Text max. 29 Zeichen („“)	iptables … -j LOG --log-prefix string	
TCP-Sequenznr.	iptables … -j LOG --log-tcp-sequence	
TCP-Options	iptables … -j LOG --log-tcp-options	
IP-Options	iptables … -j LOG --log-ip-options	
Standardverhalten	iptables -P chain policy	
	policy = DROP, ACCEPT	

FW - Filterregeln Selbstdef.

Selbstdefinierte Regelketten

Erzeugen	iptables -N chain
	chain = bis 31 Zeichen
Löschen	iptables -X [chain]
	Im Vorfeld müssen alle Filterregeln der Regelkette chain gelöscht (iptables -F) sein.

Regelketten speichern/laden

Speichern	iptables > datei.txt
Laden	iptables < datei.txt

Linux als Firewall (II)

VHS Düsseldorf

Guido Petermann

FW - Möglichkeiten

- Ermöglicht Sicherheit über eine Schnittstelle (Netzwerk - Netzwerk)
  -> Verfügbarkeit, Integrität, Vertraulichkeit
- Ermöglicht Protokollierung
- Aber:
  Schützt nicht vor Angriffe von innen

FW - Organisation

- Zugangsschutz gewährleisten
- Aktuelle Informationen bereitstellen
- Kontrollmaßnahmen (Protokolle)
- Netzwerkverkabelung /-infrastruktur pflegen
- Zugriffsberechtigungen pflegen
- Regelmäßig Updates
- Sicherheitsüberprüfungen (extern)
- Dokumentation
- Mitarbeitermotivation

FW - Schwachstellen

- Softwarefehler
- Designfehler
- Fehlendes Knowhow
- Motivationsprobleme
- Durchhaltevermögen

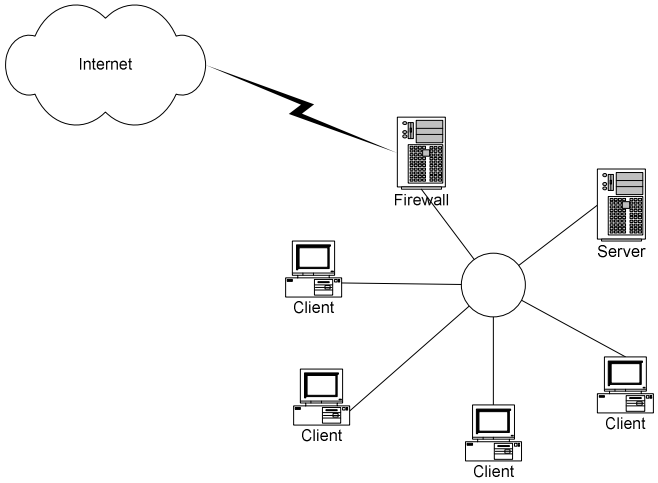
FW - Angriffsmethoden

- Scannen (Dienste, Softwareversionen)
- Sniffen (Pakete mitschneiden)
- Einbruch (Zugriff auf Rechner)
- Brute Force (Massives Probieren)
- Man in the Middle (Zwischen Client/Server)
- Viren, Würmer, Trojanische Pferde
- Denial of Serivce (DoS)
- Distributed Denial of Service (DDoS)

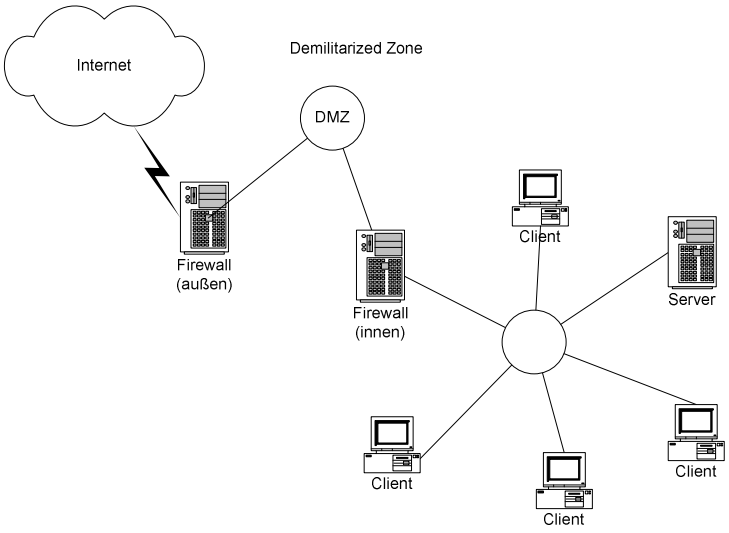
FW - NAT, Socks, Proxi

	NAT	Socks	Proxy
Anwendungsorientiert	Nein	Nein	Ja
Geschwindigkeit	sehr schnell	schnell	langsamer
Protokollierung	IP	TCP	Anwendungsebene
Caching	nein	nein	ja
Autorisierung	IP Adresse	IP Adresse	IP Adresse und Anwendername
Implementierung	Kernel	Zus. Software	Zus. Software
Protokolle	TCP,UDP,ICMP	TCP,(UDP)	TCP
Transparent (Client)	Ja	zum Teil	Nein

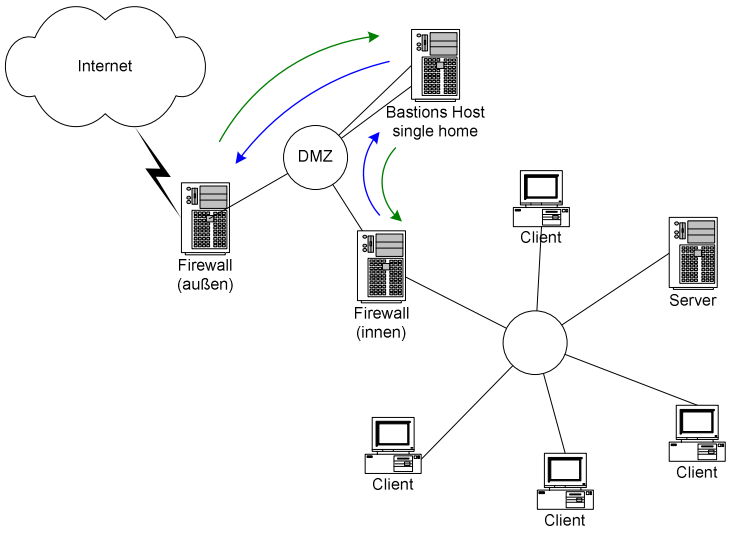
FW - Standalone



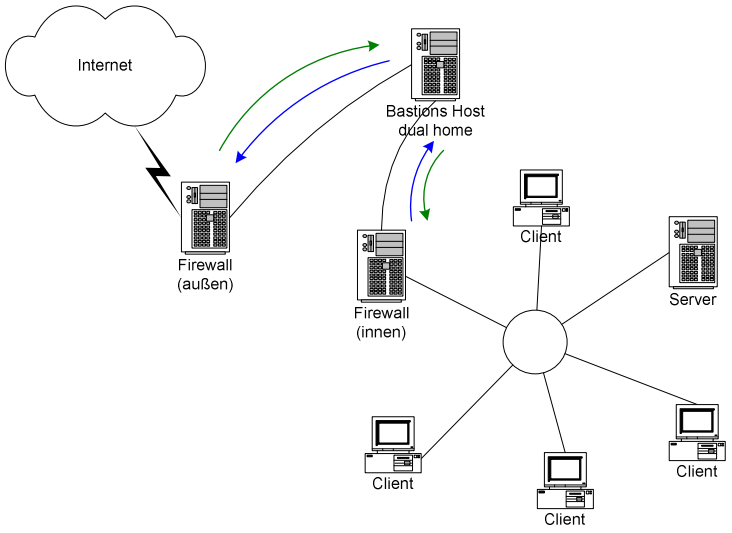
FW - DMZ einfach



FW - DMZ Bastion single



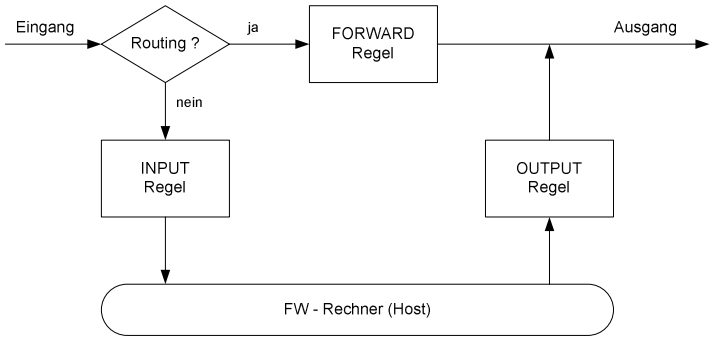
FW - DMZ Bastion dual



iptables

filter, mangle, nat

(ab Kernel 2.4.x)



Filterregeln werden in Filterregelnketten (chains) mithilfe des Befehls iptables zusammengefaßt

FW - Filterregeln Aufbau

Grundaufbau von Filterregeln

Filterregeln werden in Filterregelnketten (chains) mithilfe des Befehls iptables zusammengefaßt

FW - Filterregeln Operation

Grundaufbau von Filterregeln

Filterregeln erweitern:	Anhängen	iptables -A chain rule ...	(Append)
	Einfügen	iptables -I chain position rule ...	(Insert)
Filterregeln löschen:	Passende	iptables -D chain rule ...	(Delete)
	Position	iptables -D chain position ...	(Delete)
	Alle	iptables -F [chain]	(Flush)
Filterreglen ändern:	Ersätzen	iptables -R chain position rule ...	(Replace)
Verschiedenes:	Standard Regelkette festlegen	iptables -P chain ...	(Policy)
	Zähler der Regelkette löschen	iptables -Z [chain]	(Zero)
	Regelkette umbenennen	iptables -E name_alt name_neu	(Exchange)
	Alle Regeln anzeigen	iptables -L [chain] oder -vL [chain]	(List)

FW - Filterregeln Regeln

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Protokolle:	TCP, UDP, ICMP	iptables -A chain -p proto	proto = tcp, udp oder icmp
	iptables -A INPUT -p udp		
Adressen:	Quell- bzw. Zieladresse	iptables -A chain -s source_ip iptables -A chain -d destination_ip	Quelladresse Zieladresse
	iptables -A INPUT -s 10.1.3.0/255.255.255.0 iptables -A INPUT -s 10.1.3.23 -d 10.1.1.102		
Interface:	Eingabe- bzw. Ausgabeinterface	iptables -A INPUT -i in_interface iptables -A FORWARD [-i in_interface] [-o out_interface] iptables -A OUTPUT -o out_interface	
	iptables -A OUTPUT -o eth0 iptables -A INPUT -i ippp+	Interfacegruppen mit „+“ möglich	
Fragmente:	Prüfung von fragmentierten Paketen (zweite bis letzte Paket) Die Angabe von Protokollen und des SYN-Flags sind nicht erlaubt	iptables -A INPUT -f ...	
Negation:	Negation über „!“ möglich		
	iptables -A chain -s ! 10.1.3.22	alle Quelladressen außer 10.1.3.22	
Erweiterungen:	...		

FW - Filterregeln Regelnerw. I

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Erweiterungen

TCP	Quellport	iptables … -p tcp --sport [!] port ...
	Zielport	iptables … -p tcp --qport [!] port …
	port = Portname, Portnummer, Portbereich Bsp: www, 22, 4000:4050, :128, 1024:	
	Flags	iptables … -p tcp --tcp-flags [!] mask setflags
	mask = Flags die geprüft werden sollen (SYN, FIN, RST, PSH, ACK, URG, ALL, NONE) setflags = Flags die gesetzt sein müssen (SYN, FIN, RST, PSH, ACK, URG, ALL, NONE)	
	iptables -A INPUT -p tcp --tcp-flags SYN,ACK SYN … iptables -A INPUT -p tcp --tcp-flags ALL NONE …	
	Verbindungsaufbau	iptables … -p tcp [!] --syn (flags: SYN,RST,ACK SYN)
	Option	iptables … -p tcp ---tcp-option [!] option-nr
	option-nr = Optionskennung	
UDP	Quellport	iptables … -p udp --sport [!] port …
	Zielport	iptables … -p udp --dport [!] port ...
	port = Portname, Portnummer, Portbereich Bsp: www, 22, 4000:4050, :128, 1024:	

FW - Filterregeln Regelnerw. II

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Erweiterungen

Multiport

Quellport	iptables … -p tcp|udp -m multiport --sports port[,port] ...
Zielport	iptables … -p tcp|udp -m multiport --dports port[,port] ...
Quell-/Zielport identisch	iptables … -p tcp|udp -m multiport --ports port[,port] ...

port = Portname, Portnummer, Portbereich Bsp: www, 22, 4000:4050, :128, 1024:

ICMP

Type/Code — iptables … -p icmp --icmp-type [!] icmpspec

icmpspec = type[/code] Bsp. 8/0, echo-request

echo reply	Antwort auf Ping	0/0
destination unreachable	Ziel nicht erreichbar	3/x (x>0)
source quench	Ziel überlastet	4/0
redirect	Anderen Router benutzen	5/x (x>0)
echo request	Pinganfrage	8/0
time exceeded	Zeitüberschreitung	11/0

Verbindungszustand

Neu	iptables … -m state --state NEW …
Bestehend	iptables … -m state --state ESTABLISHED …
Notwendig	iptables … -m state --state RELATED …
Rest bzw. Fehlerhaft	iptables … -m state --state INVALID …

FW - Filterregeln Regelnerw. III

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Erweiterungen

Netzwerkadressen MAC-Adressen — iptables … -m mac --mac-source [!] mac-addr

iptables -A INPUT -m mac --mac-source 1B:20:3A:B4:FA:03 ...

Beschränkung

Mengen-/Zeitbeschränkung	iptables … -m limit …	default 5 Pakete, 20 Min
(Matching-Rate)	iptables … -m limit --limit rate …	

rate = x/s, x/m, x/h, x/d Bsp. 3/h entspricht 20 Minuten

iptables … -m limit-burst number …

Wenn die Anzahl der Pakete laut „limit-burst number“ erreicht wurde, wird alle „limt rate“ nur ein Paket verarbeitet. Solange bis „limit-burst number“ mal „limt rate“ kein Paket eintrifft.

Syn-Flood-Protection: iptables -A chain -p tcp --syn -m limit --limit 5/s

Owner-Prüfung

User ID	iptables … -m owner --uid-owner userid ...
Group ID	iptables … -m owner --gid-owner groupid ...
Process ID	iptables … -m owner --pid-owner processid ...
Session ID	iptables … -m owner --sid-owner sessionid ...

FW - Filterregeln Konsequenz

Grundaufbau von Filterregeln

Operation	Regel	Konsequenz

Akzeptieren	iptables … -j ACCEPT	(jump to …)
Verwerfen	iptables … -j DROP	
Abweisen	iptables … -j REJECT iptables … -j REJECT --reject-with type	default: Port Unreachable
	type = icmp-net-unreachable, icmp-host-unreachable, icmp-unreachable, tcp-reset	
Regelkette verlassen		iptables … -j RETURN
Paket an Anwendung weitergeben	iptables … -j QUEUE	
Zu (selbstdefinierter) Regelkette verzweigen	iptables … -j name	name = Name der Regelkette
Protokollieren	iptables … -j LOG	(logging)
Warnstufen (Syslog)	iptables … -j LOG --log-level syslog-prio	
Text max. 29 Zeichen („“)	iptables … -j LOG --log-prefix string	
TCP-Sequenznr.	iptables … -j LOG --log-tcp-sequence	
TCP-Options	iptables … -j LOG --log-tcp-options	
IP-Options	iptables … -j LOG --log-ip-options	
Standardverhalten	iptables -P chain policy	
policy = DROP, ACCEPT		

FW - Filterregeln versch.

Selbstdefinierte Regelketten

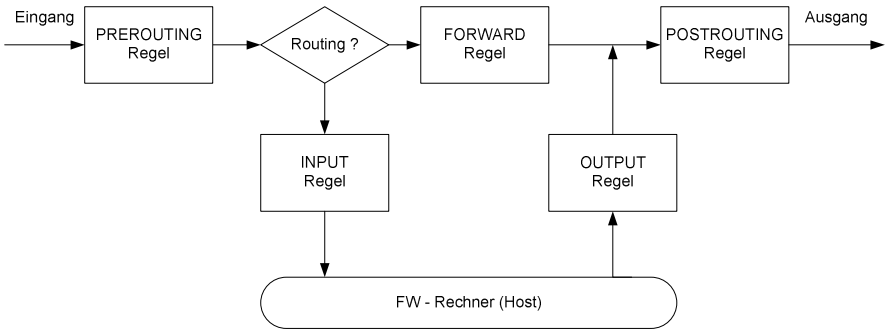
Erzeugen	iptables -N chain
chain = bis 31 Zeichen	
Löschen	iptables -X [chain]

Im Vorfeld müssen alle Filterregeln der Regelkette chain gelöscht (iptables -F) sein.

Regelketten speichern/laden

Speichern	iptables > datei.txt
Laden	iptables < datei.txt

FW - NAT



PREROUTING Destination-NAT (DNAT)
POSTROUTING Source-NAT (SNAT)

FW - SNAT/DNAT

Source-NAT

fest — iptables -t nat -A POSTROUTING … -j SNAT --to-source source

source = ipadd[-ipadd][:port[-port]]
iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to-source 10.3.0.1

dynamisch — iptables -t nat -A POSTROUTING … -j MASQUERADE

iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
„echo 1 > /proc/sys/net/ipv4/ip_dynaddr

es ist jeweils nur das Output-Interface (-o …) erlaubt

Destination-NAT — iptables -t nat -A PREROUTING … -j DNAT --to-destination destination

destination = ipadd[-ipadd][:port[-port]]

iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth1 -j DNAT --to-destination 10.2.0.22
iptables -t nat -A PREROUTING -p tcp --dport 4040 -i eth1 -j DNAT --to-destination 10.2.0.22:4040
iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth1 -j DNAT --to-destination 10.2.0.3-10.2.0.6

es ist jeweils nur das Input-Interface (-i …) erlaubt

FW - Standardregeln I

	intern		extern	
eMail				
Versenden (SMTP)	Client >1023	an	Server 25	TCP
Empfangen (POP3)	Client >1023	an	Server 110	TCP
DNS				
Datenaustausch	Server 53	an	Alle 53	UDP
	Server >1023	an	Alle 53	TCP
	Server 53	von	Alle >1023	TCP
FTP				
Aktiv	Client >1023	an	Alle 21	TCP
	Client >1023	von	Alle 20	TCP
Passiv	Client >1023	an	Alle 21	TCP
	Client >1023	an	Alle >1023	TCP

FW - Standardregeln II

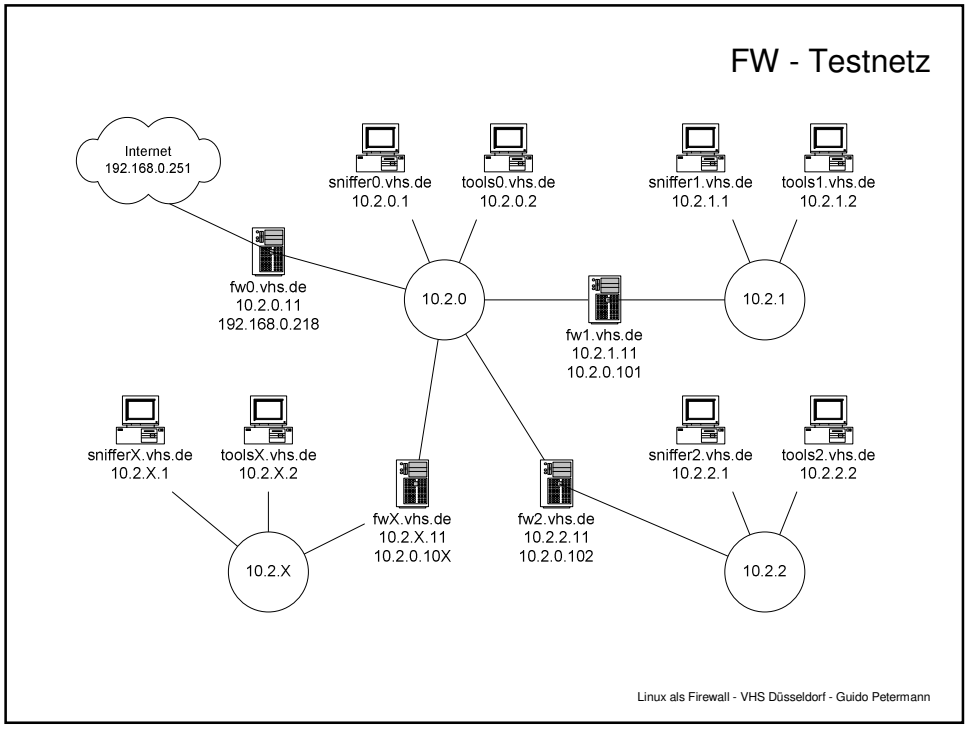
	intern		extern	
NNTP	Client >1023	an	Server 119	TCP
NTP	Client 123	an	Server 123	UDP
	Client >1023	an	Server 123	UDP
HTTP				
Ausgehende Verbindung	Client >1023	an	Alle 80	TCP

FW - Standardscript

```
# /etc/init.d/firewall

case “$1“ in
        start)
                echo “Start Firewall“
                iptables -F
                iptables -t nat -F
                iptables -X

                iptables -P INPUT DROP
                iptables -P OUTPUT DROP
                iptables -P FORWARD DROP

                echo “1“ > /proc/sys/net/ipv4/ip_forward
                echo “1“ > /proc/sys/net/ipv4/tcp_syncookies
                echo “1“ > /proc/sys/net/ipv4/ip_dynaddr

                ***

                ;;
```


FW - Standardscript

```
        stop)
                echo “Stoppe Firewall“
                iptables -F
                iptables -t nat -F
                iptables -X
                ;;

        *)
                echo “Benutze: firewall {start|stop}“
                exit 1
                ;;

esac
exit 0
```


FW - Testnetz
Internet
192.168.0.251
sniffer0.vhs.de
10.2.0.1
tools0.vhs.de
10.2.0.2
sniffer1.vhs.de
10.2.1.1
tools1.vhs.de
10.2.1.2
fw0.vhs.de
10.2.0.11
192.168.0.218
10.2.0
fw1.vhs.de
10.2.1.11
10.2.0.101
10.2.1
snifferX.vhs.de
10.2.X.1
toolsX.vhs.de
10.2.X.2
fwX.vhs.de
10.2.X.11
10.2.0.10X
fw2.vhs.de
10.2.2.11
10.2.0.102
sniffer2.vhs.de
10.2.2.1
tools2.vhs.de
10.2.2.2
10.2.X
10.2.2
Linux als Firewall - VHS Düsseldorf - Guido Petermann