Hot Firewalls -

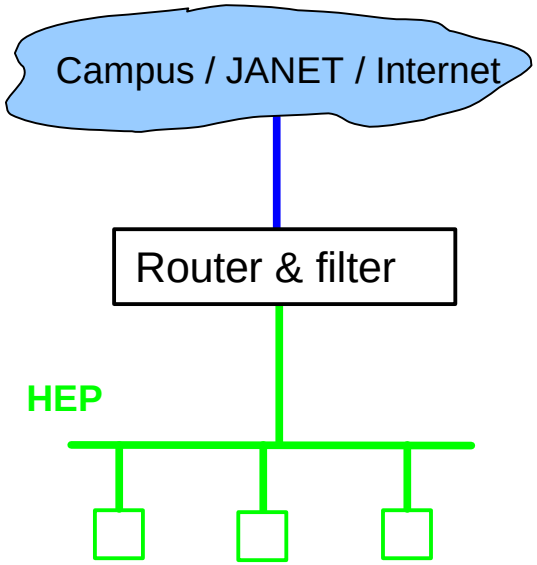
Cool hacks

OR : How to put up a Firewall when surrounded by users

R. Hughes-Jones SysMan Sep 98

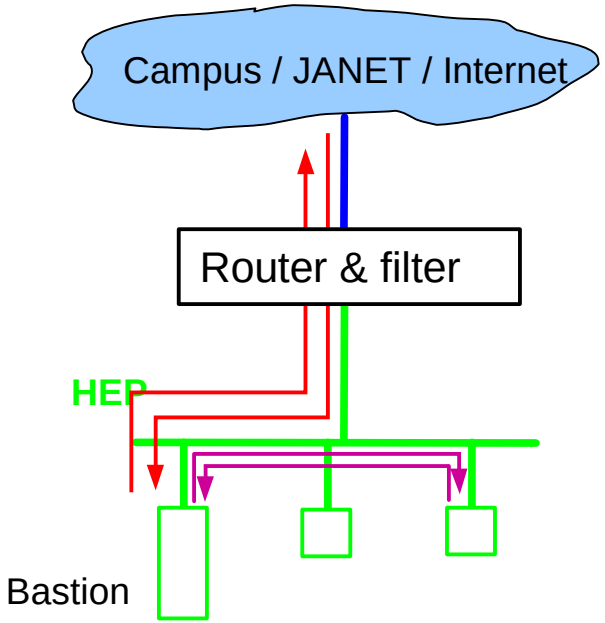
Firewall Architectures

Packet Filtering



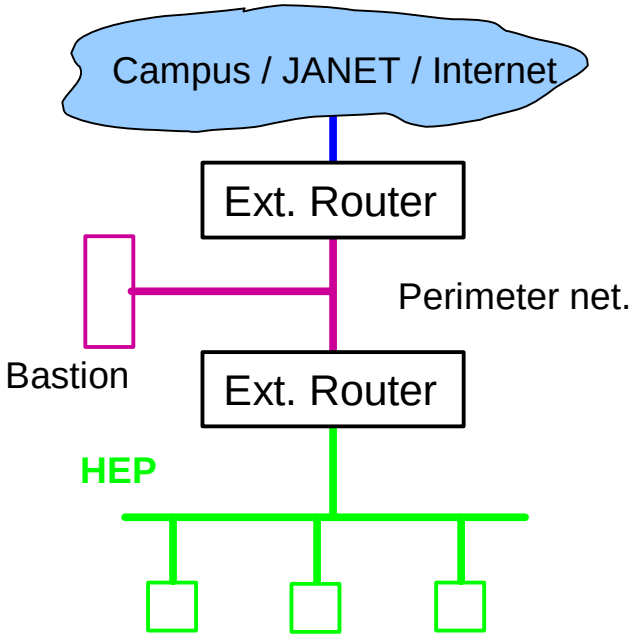
- Filter packets on the fly
- Work close to line speed
- Permit/deny IP services
- Not at user/application level

Bastion Host



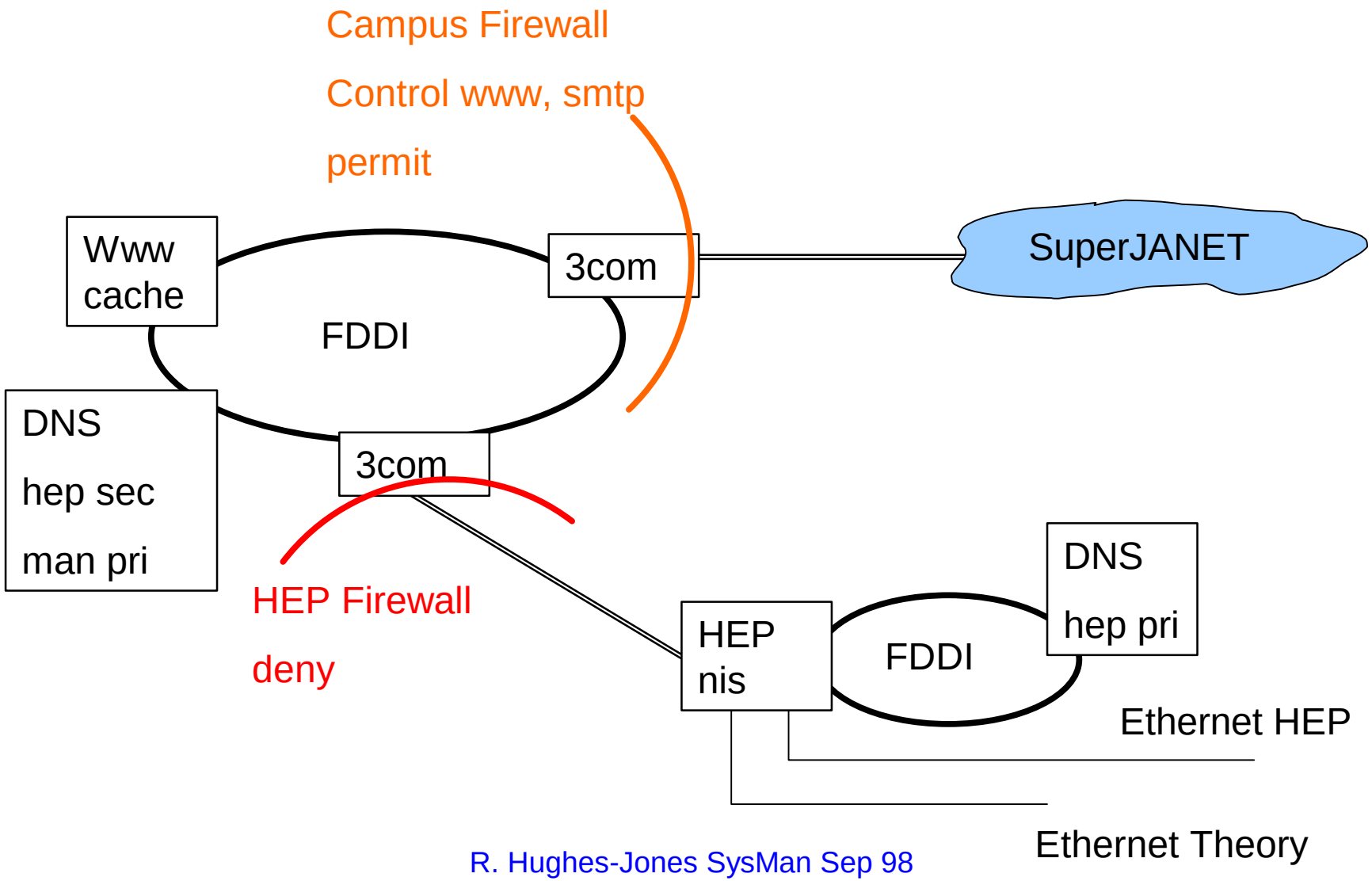
- Only Bastion accessed externally
- Acts as proxy for IP service
- Check user/application level

Screened Subnet



- High security
- Bastion can't snoop
- 2 routers

Site Configuration



Objectives

- Block Hacker access NOW
- … file seen
- Log files altered
- Sniffer suspected
- Limit information hacker can extract from Manchester HEP
- Provide better security :
  - Integrity of OS and User / Physics data - intrusion
  - Availability of resources - denial of service
  - Contribute to security of HEP community
- Disrupt users as little as possible - hmm

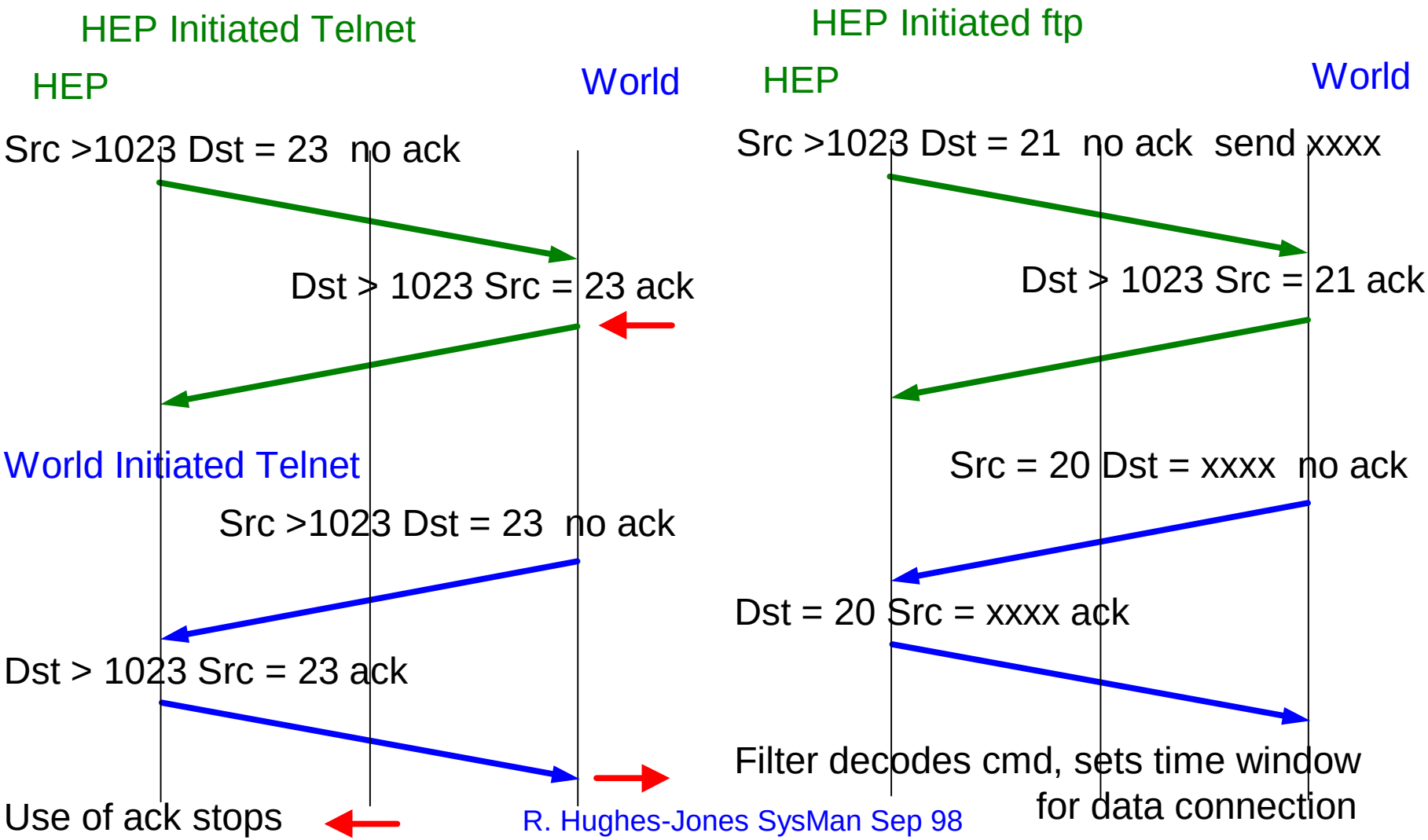
Which interface packet comes from

Source IP address and port

Destination IP address and port

Protocol type

Filtering Packets



Packet Filters

or what they implemented !!

Default action : DENY access

	Protocol	Port	HEP to World	World to HEP	
Passwd	Telnet	23	TCP S>1023 D=23	CERN, DESY,	
			TCP S=23 D>1023 Est	RAL,SLAC to all	
Passwd	ftp	21c 20d	any to any	any to any	
	smtp	25	any to any	any to a2,a3,a4,a13	
	www	80	any to any	any to any	Server only
	dns	53	any to any	any to any	
	ssh	22	any to any	any to any	
	rip	520	any to any	any to any	
	icmp		any to any	any to any	

Packet Filters

or what the users needed !!

Protocol	HEP to World	World to HEP
www cache	TCP S>1023 D=3128	TCP S>1023 D=3128
	TCP S=3128 D>1023 Est	TCP S=3128 D>1023 Est
dns client-srv	UDP S>1023 D=53	UDP S>1023 D=53
	UDP S=53 D>1023	UDP S=53 D>1023
X from CERN display at M/c		TCP S>1023 D=6000
		TCP S=6000 D>1023 Est
X display at CERN	TCP S>1023 D=6005	
	TCP S=6005 D>1023 Est	

NTP	port 123	any	any	
NNTP	port 119	any	none	
Passwd pop3	port 123	any to ONE M/c server	M/c dialup to a13	

NO NFS
TFTP
BSD r
Syslog
SNMP
NIS/YP

Packet Filters

and then some new application comes along ... !! ...

Protocol	HEP to World	World to HEP	
Mbone vic	UDP S=2608 D any	UDP S=2608 D any	& 2609
	UDP D=2608 S any	UDP D=2608 S any	& 2609
Mbone rat	UDP S=1712 D any	UDP S=1712 D any	& 1713
	UDP D=1712 S any	UDP D=1712 S any	& 1713

NetMeeting :		
	TCP 389	Internet Location Server
	TCP 1503	T.120
	TCP 1720	H.323 call setup
	TCP 1731	Audio call control
	TCP Dynamic	H323 call control
	UDP Dynamic	H.323 RTP streaming