Firewalls and NAT

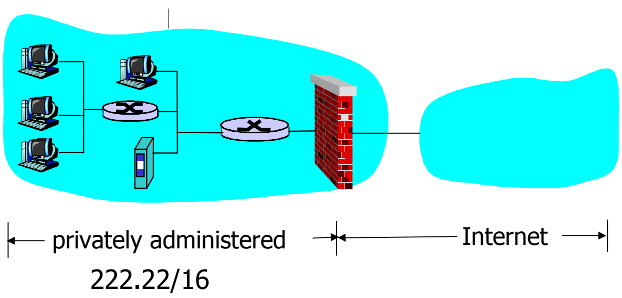
1

Firewalls

By conventional definition, a firewall is a partition made of fireproof material designed to prevent the spread of fire from one part of a building to another.

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



2

Firewalls: Goals

- All traffic from outside to inside and vice-versa passes through the firewall
- Only authorized traffic, as defined by local security policy, will be allowed to pass
- Firewall itself is immune to penetration

3

Firewalls: Taxonomy

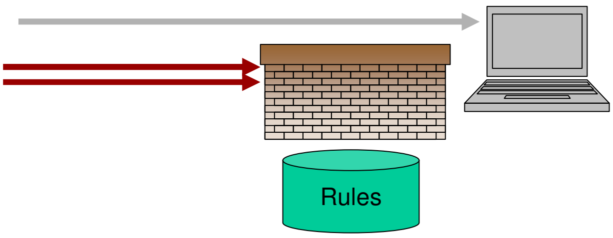
1. Traditional packet filters
   - Filters often combined with router, creating a firewall
2. Stateful filters
3. Application gateways

Major firewall vendors:
Checkpoint
Cisco PIX

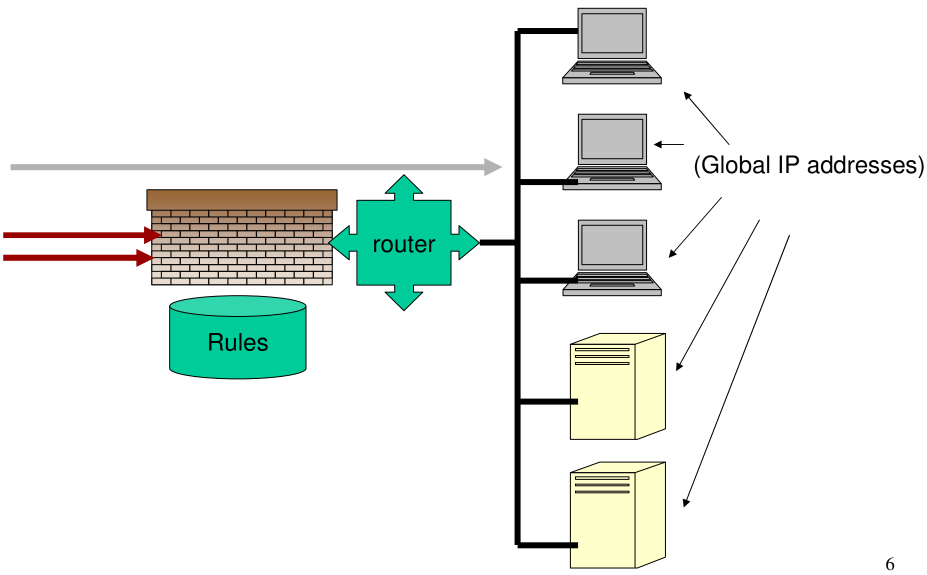
4

Firewall

- Firewall == system that filters TCP/IP UDP/IP packets according to rules
- Either software on user machine or network router



Firewall



6

Traditional packet filters

Analyzes each datagram going through it; makes drop decision based on:

- Source IP address
- Destination IP address
- Source port
- Destination port
- TCP flag bits
  - SYN bit set: datagram for connection initiation
  - ACK bit set: part of established connection
- TCP or UDP or ICMP
  - Firewalls often configured to block all UDP
- Direction
  - Is datagram leaving or entering internal network?
- Router interface
  - Decisions can be different for different interfaces

Filtering rules - examples

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
Outside connections to public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a Smuft DoS attack.	Drop all ICMP packets going to a "broadcast" address (e.g. 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP unreachables

Access control lists

Apply rules from top to bottom:

action	source address	dest address	proto	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Access control lists (2.)

- Each router/firewall interface can have its own ACL
- Most firewall vendors provide both command-line and graphical configuration interface

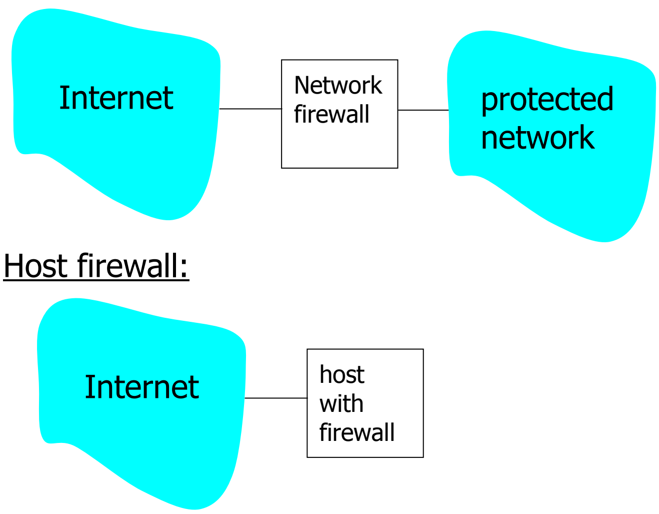
Traditional packet filters

- Advantages
  - One screening router can protect entire network
  - Can be efficient if filtering rules are kept simple
  - Widely available. Almost any router, even Linux boxes
- Disadvantages
  - Can be penetrated
  - Cannot enforce some policies. For example, permit certain users.
  - Rules can get complicated and difficult to test

11

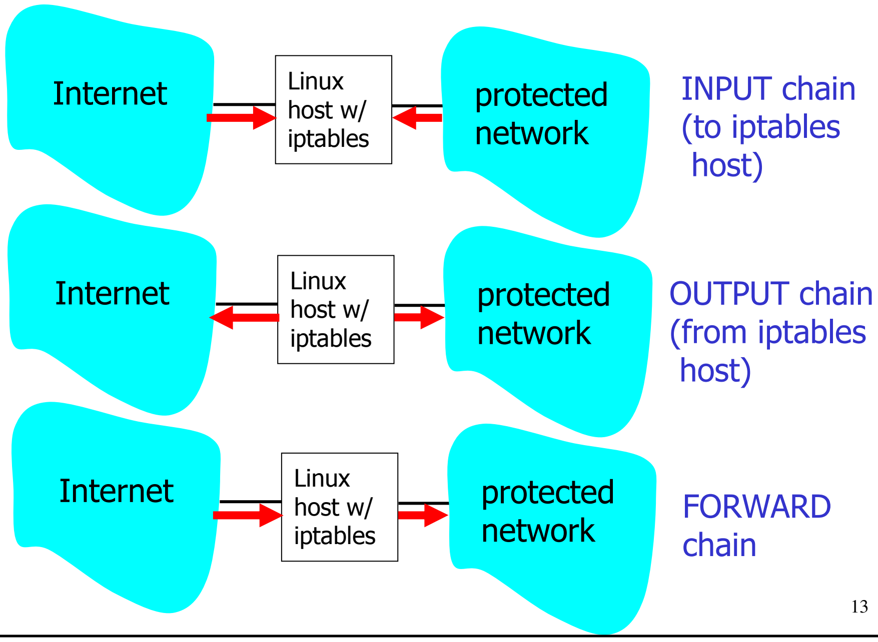
Network or host firewall

Network firewall:



12

Example: Iptables – chain types



13

Iptables: Example command

```
iptables -A INPUT -i eth0 -s 232.16.4.0/24 -j ACCEPT
```

- Sets a rule
  - Accepts packets that enter from interface eth0 with source address in 232.16.4/24
- Kernel applies rules in order
  - First matching rule determines action for packet
- Append: -A
  - Adds rule to bottom of existing rules

14

Stateful filters

- Stateless filters: Any packet with ACK=1 and source port 80 gets through
  - Attack with malformed packets: send ACK=1 segments
- Stateful filter: Adds more intelligence to decision-making process
  - Stateful = remember past packets
  - Needs very dynamic state table

15

Stateful filters: Example

- Log each TCP conn initiated through firewall: SYN segment
- Timeout entries without activity after, e.g., 60 seconds

source address	dest address	source port	dest port
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Rule table indicates check of stateful table:
See if there is a connection entry in stateful table

Stateful filters can remember outgoing UDP segments

16

Stateful example: Example (2.)

1) Pkt arrives from outside: src=37.96.87.123, src port=80, dst=222.22.1.7, dst port=12699, SYN=0, ACK=1
2) Check filter table ➜ check stateful table

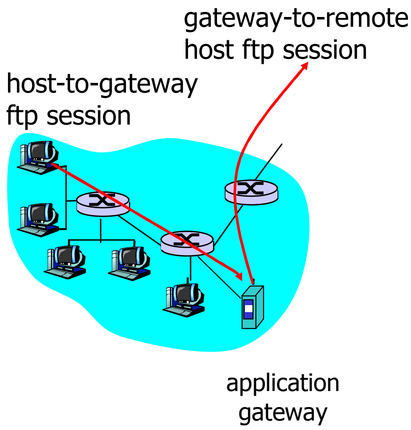
action	source address	dest address	proto	source port	dest port	flag bit	check conn
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	x
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	x
deny	all	all	all	all	all	all	

3) Connection is in connection table ➜ let packet through

17

Application gateways (aka proxy servers)

- App gateway between user (inside) and server (outside)
- User and server talk through proxy
- Allows fine grained/ sophisticated control
- Hinders protocol attacks
- E.g.: ftp server may not allow files >= size X



18

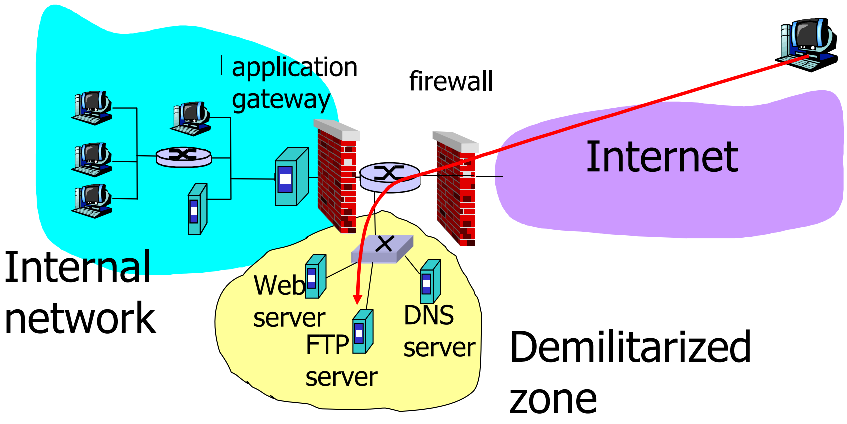
Mail servers and proxy Web servers

- Local mail server is application gateway
  - Virus detection and removal
- So is Web proxy cache
  - E.g.: virus detection and removal

Proxy gateways

- Advantages
  - Can log all connections, activity in connections
  - Can provide caching
  - Can do intelligent filtering based on "content"
  - Simplifies service control
    - Can perform user level authentication
    - Simplifies firewall rules
- Disadvantages
  - Not all services have proxied versions
  - Need different proxy server for each service
  - Requires modification of client
  - Performance
  - Hinders end-to-end encryption

Demilitarized Zone (DMZ)



- Used for: Gateways and public services
- Advantage: Hacked server – limited damage

IP traceback

Problem: How do we determine where malicious packet came from ?

- Why? Attackers can spoof source IP address
- Benefits:
  - Determine attacker
  - Determine zombie machine participating in DDoS attack
- Alternative: Use ingress filtering

Methods for finding source

- Manual using current IP routing
  - Link testing: how?
    - Start from victim and test upstream links
    - Recursively repeat until source is located
    - Assume attack remains active until trace complete
  - Link testing: problem
    - Handle ISPs
    - Located zombie …
  - Logging
- Automatic using marking algorithms

Logging

- Key routers log packets (useful for forensics)
- Use data mining to find path
- Pros
  - Post mortem – works after attack stops
- Cons
  - High resource demand:
    need to store and process tons of data

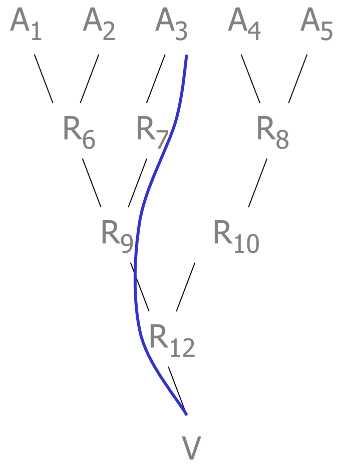
Marking algorithms

- Mark packets with router addresses
  - Deterministically or probabilistically
- Trace attack using marked packets
- Strengths
  - Independent of ISP management
  - Little network overhead, traffic
  - Trace distributed attacks, attacks post-mortem

25

Marking: Assumptions

- Most routers remain uncompromised
- Attacker sends many packets
- Route from attacker to victim remains relatively stable



26

Marking: Summary

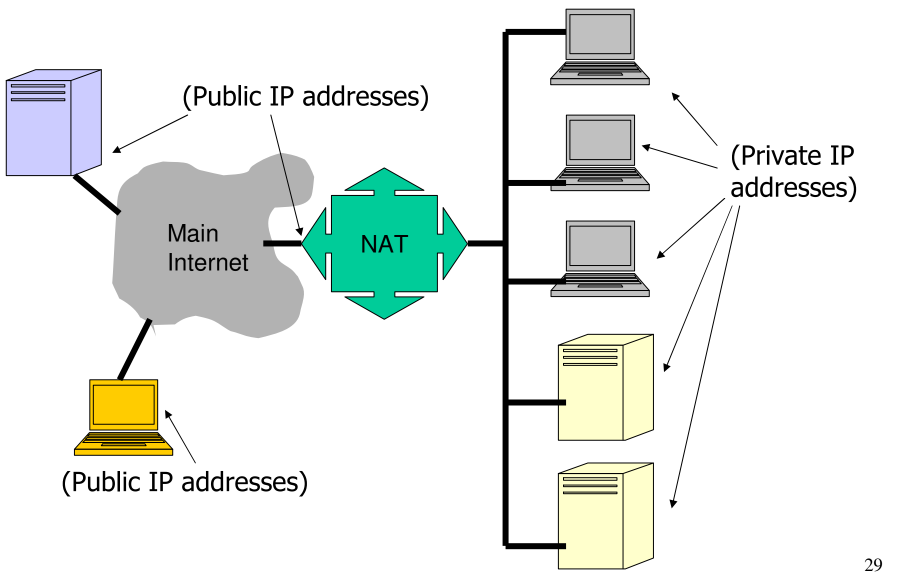
- Can determine attack path with a relatively small number of attack packets
- Need to include addresses, counter in IP datagram (e.g., via fragment fields)
- E.g.: "Practical Network Support for IP Traceback" by Savage et al.
- Status:
  - Lots of RFCs
  - But not ?yet? deployed…

27

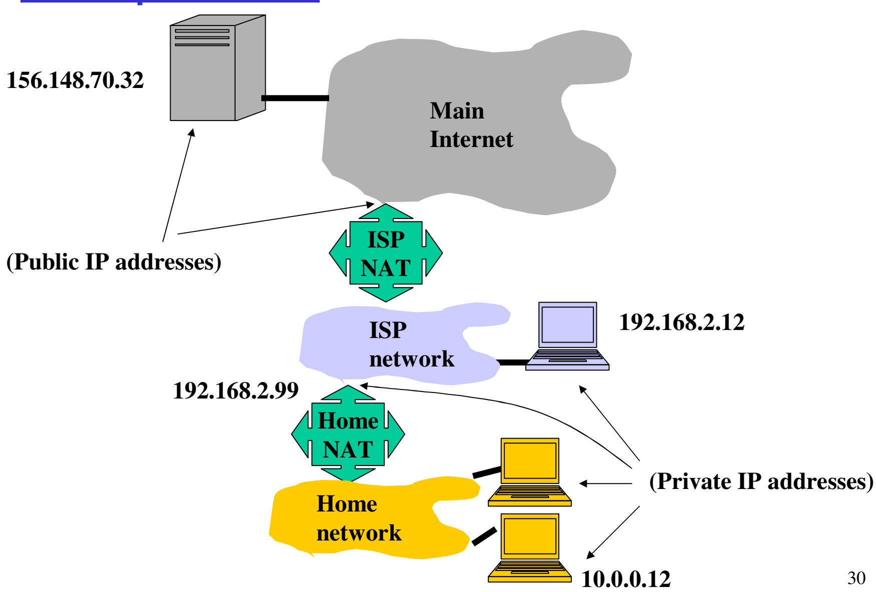
Network address translation (NAT)

- Also known as
  - Network masquerading
  - IP masquerading
- Re-writes source and/or destination address as they pass through NAT gateway
- Why
  - IPv4 address shortage
  - Standard feature
  - Some believe it enhances privacy, security, …

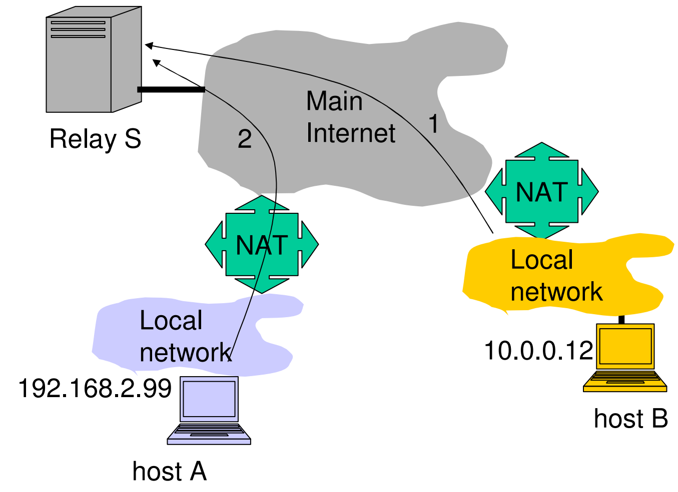
Simple NAT



Multiple NAT

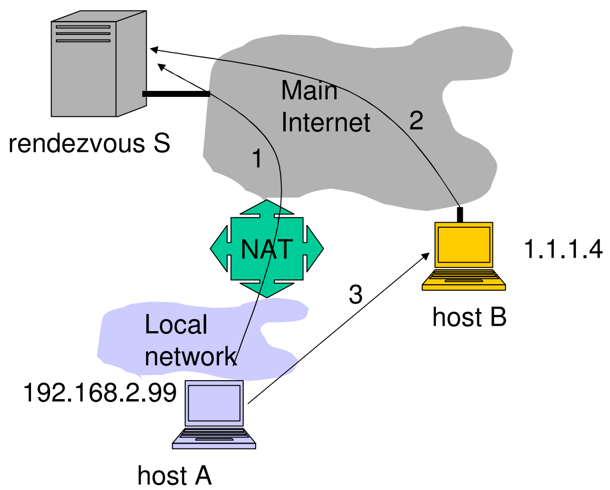


NAT traversal: Relay



31

NAT traversal: Connection reversal



32

TURN protocol

- Protocol for UDP/TCP relaying behind NAT
- Data is bounced to a public TURN server
- No hole punching
- TURN works even behind symmetric NAT

33

Hole punching

- Technique to allow traffic from/to a host behind a firewall/NAT without collaboration of the NAT itself
- UDP: simple ☺
- TCP:
  - Berkeley sockets allows TCP socket to initiate an outgoing or listen for an incoming connections *but not both*
  - Solution: bind multiple sockets to same local endpoint

STUN (RFC 3489)

- Defines operations and message formats to understand type of NAT
- Discovers presence and type of NAT and firewalls between them and Internet
- Allows applications to determine their public NAT IP address

STUNT

- Simple Traversal of UDP Through NATs and TCP too (STUNT)
- Extends STUN to include TCP functionality

NAT traversal: Cooperating NAT

- SOCKS
  - Client server protocol
  - Enables client (behind firewall) to use server (in public Internet)
  - Relays traffic
  - Widely adopted
    - E.g.: Mozilla can use SOCKS

NAT traversal: UPnP

- Defines:
  Internet Gateway Device (IGD) protocol
- Enables:
  - Learning of ones public (external) IP address
  - Enumeration of existing port mappings
  - Adding and removing port mappings
  - Assigning lease times to mappings
  - Applications to automatically configure NAT routing