Network Interconnection

Covers different approaches for ensuring border or perimeter security

Lecture : Private Network Interconnection

- We've described an internet that's a single level of abstraction

- Privacy is an issue in a single level internet architecture

- A two level architecture distinguishes between internal and external datagrams.
- Goal: Keep internal datagrams private while still allowing external communication.

Lecture: Private Network Interconnection

- Easiest way to assure privacy is with a ‘private’ network
- Traditional techniques
  - Point-to-point: leased lines, ISDN
  - Network services: ATM, Frame Relay, Private IP

Lecture: Private Network Interconnection

- Advantages of a private network
  - Security
  - Reliability
- Disadvantage:
  - cost

- Two Issues:
  - How can an organization use a public network but keep its data private?
    - From outside-to-inside access: access control through firewalls!!
  - How can an organization with a private network interconnect with the Internet?
    - Virtual Private Network!!

Introduction

- The firewall is inserted between the premises network and the Internet
- Aims at protect the premises network from Internet-based attacks
- By examining packets and make decisions about allowed or not

Firewall Environments

- There are different types of environments where a firewall can be implemented.
- Simple environment can be a packet filter firewall
- Complex environments can be several firewalls and proxies

Type is Firewalls

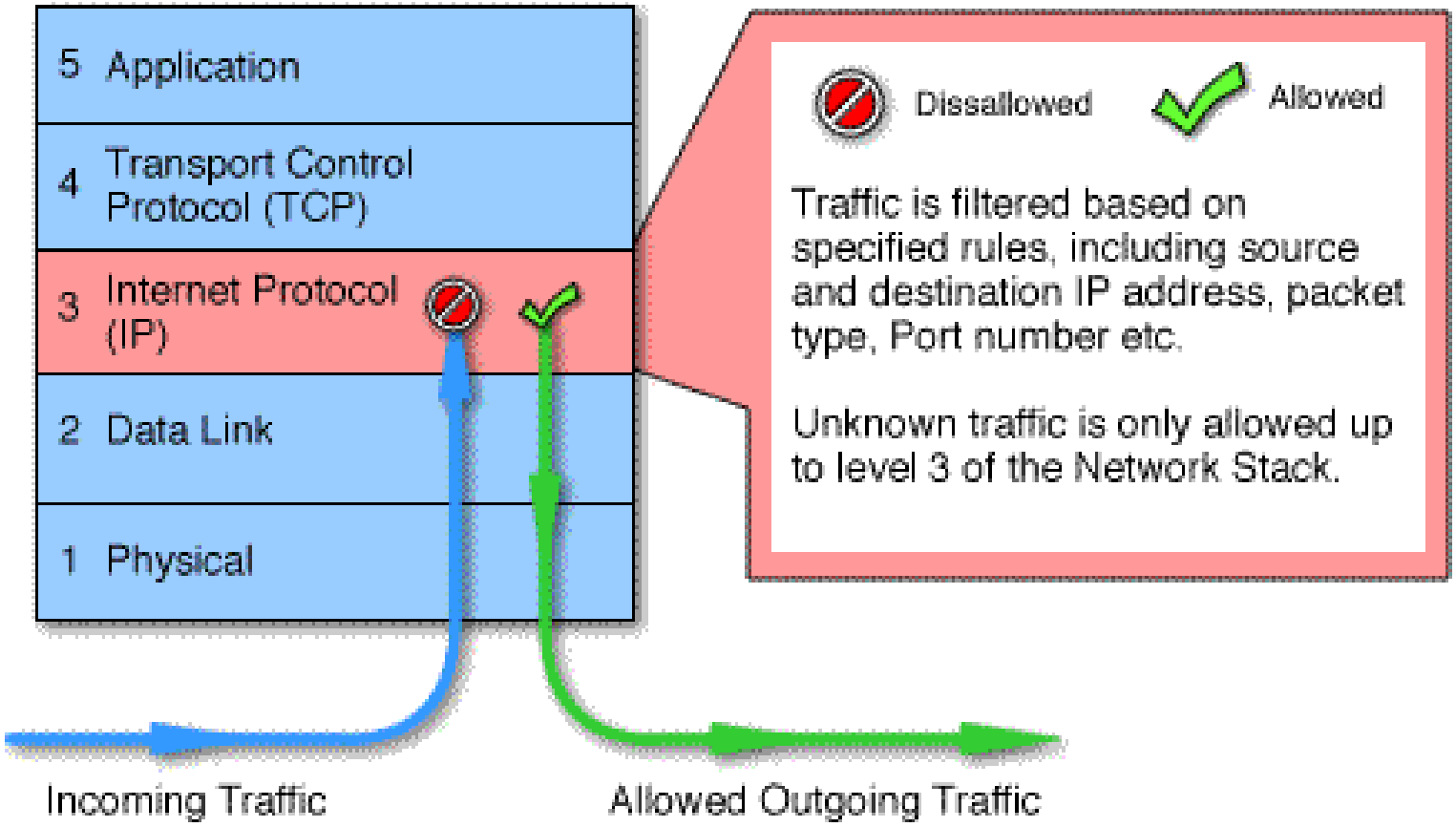
- Firewalls fall into four broad categories
- Packet filters
- Circuit level
- Application level
- Stateful multilayer

Packet Filter

- Work at the network level of the OSI model
- Each packet is compared to a set of criteria to make decisions

  [match field: action field]
- Match field: src/dst IP address, tcp port, etc
- Action field: drop, forward

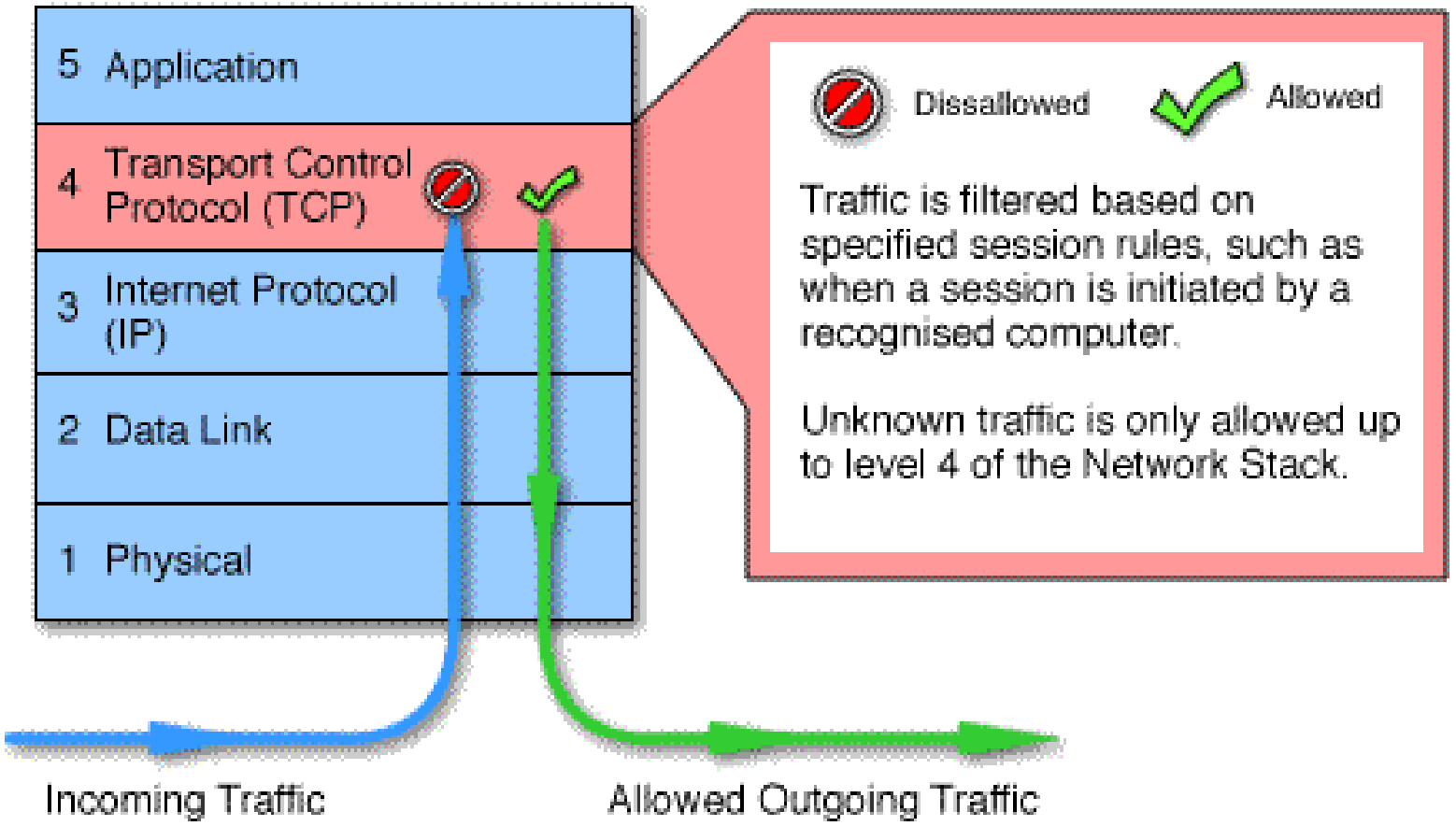
Packet Filtering



Circuit level

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP
- Monitor and track TCP layer sessions between hosts to determine whether a session is legitimate or not.

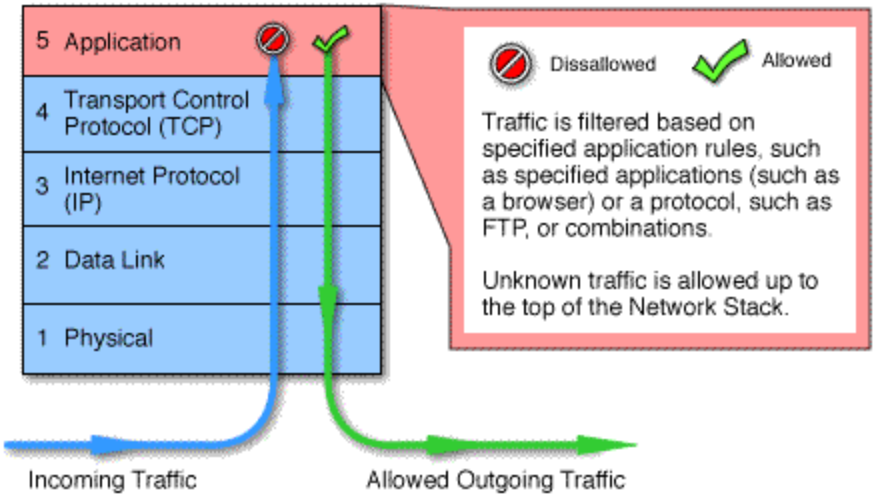
Circuit Level



Application Level

- Application level firewall works at the application layer, i.e., all browser traffic or all ftp traffic.
- It can "understand" which applications and protocols a packet belongs to (such as FTP, DNS, and HTTP).

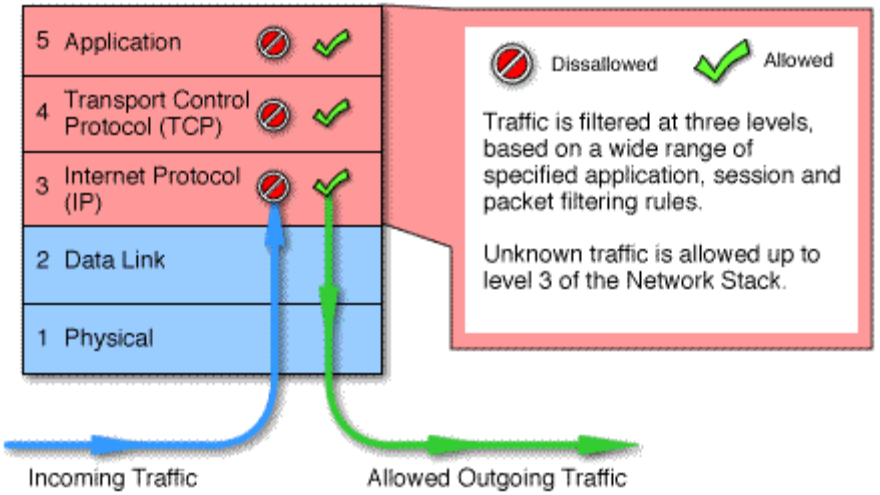
Application Level



Stateful Multilayer

- Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls
- They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer

Stateful Multilayer



Exercise

- Learn iptables, which is a flexible firewall utility built for Linux
- Google “The Beginner’s Guide to iptables, the Linux Firewall” and go over it
- Try to make “ping 8.8.8.8” fail on your machine (remember to use sudo)

Two ways

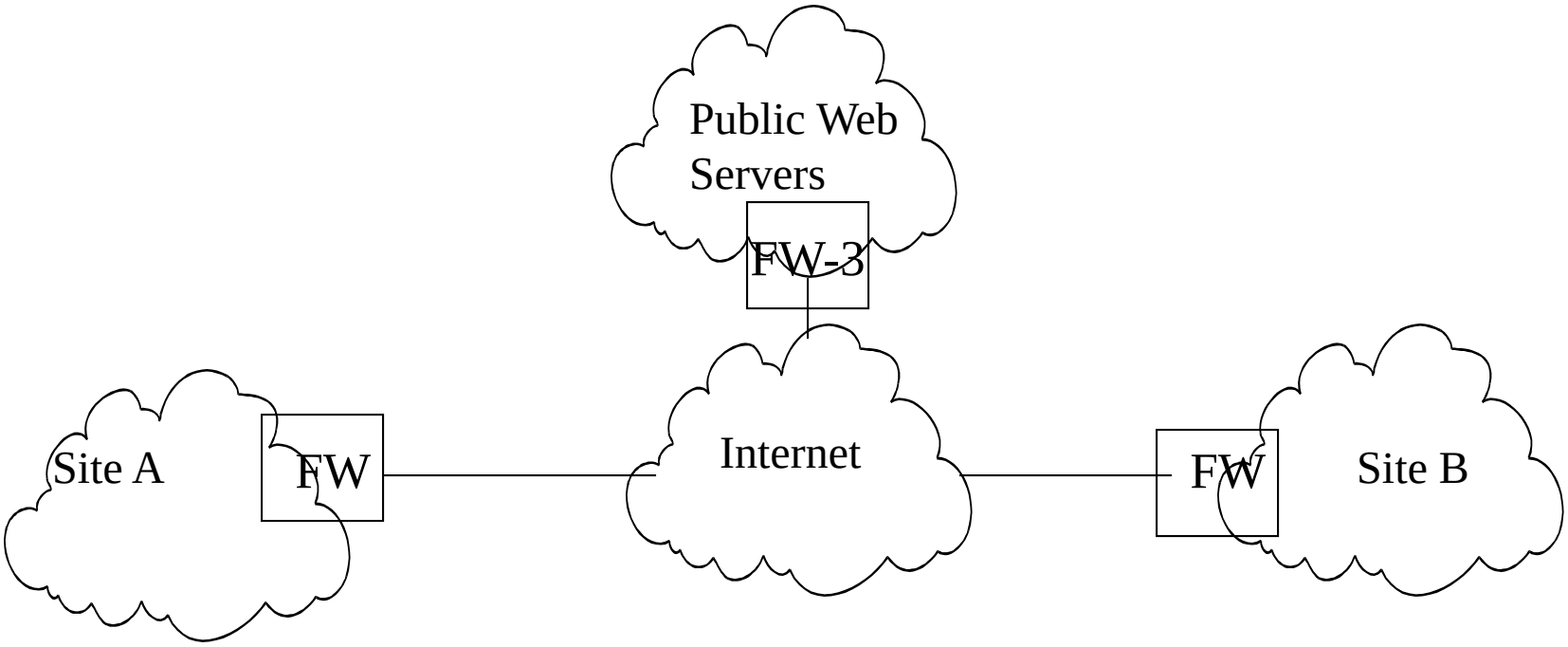
- sudo iptables -A OUTPUT -d 8.8.8.8 -j DROP
- sudo iptables -A INPUT -s 8.8.8.8 -j DROP

Lecture: Private Network Interconnection

•The cornerstone of access control: the firewall!!!

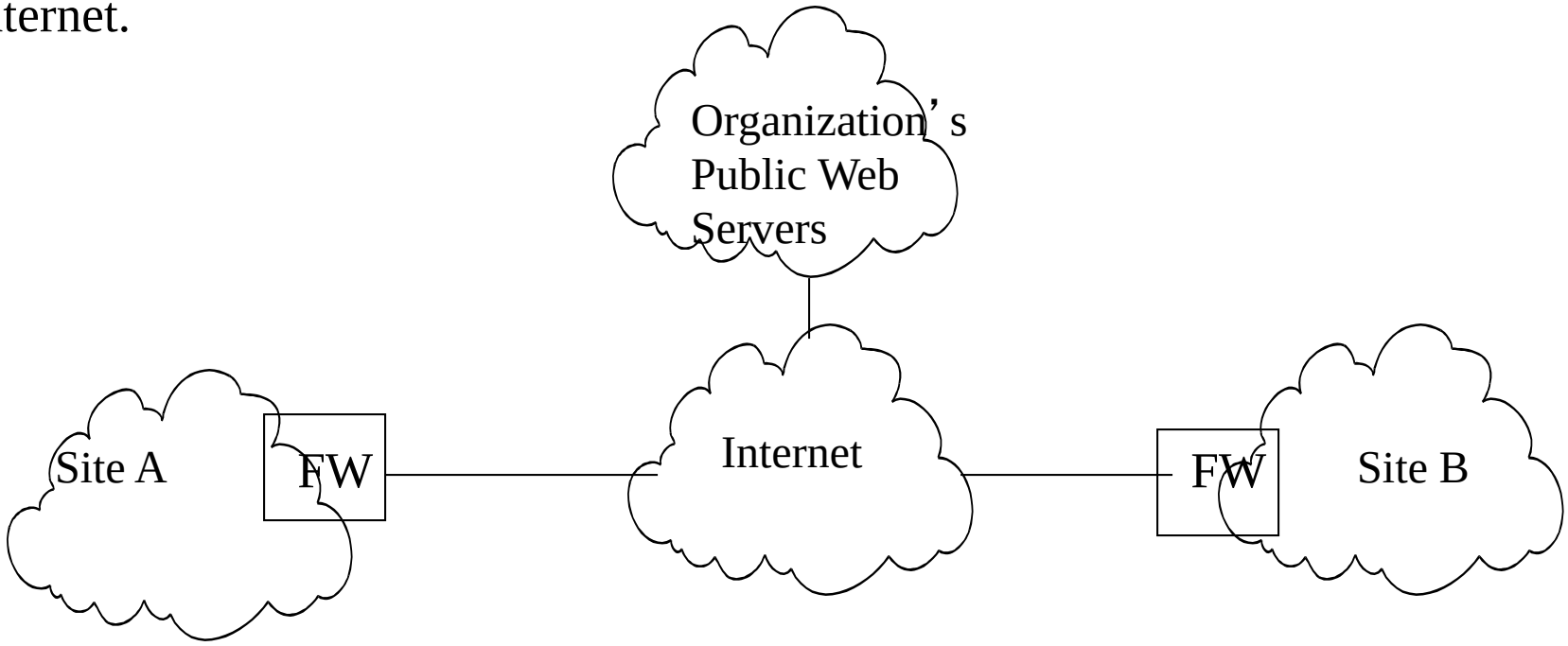
FW-3's filter table:

Interface	src addr	dst addr	src port	dst port	protocol
int0	*	server	*	8 0	tcp



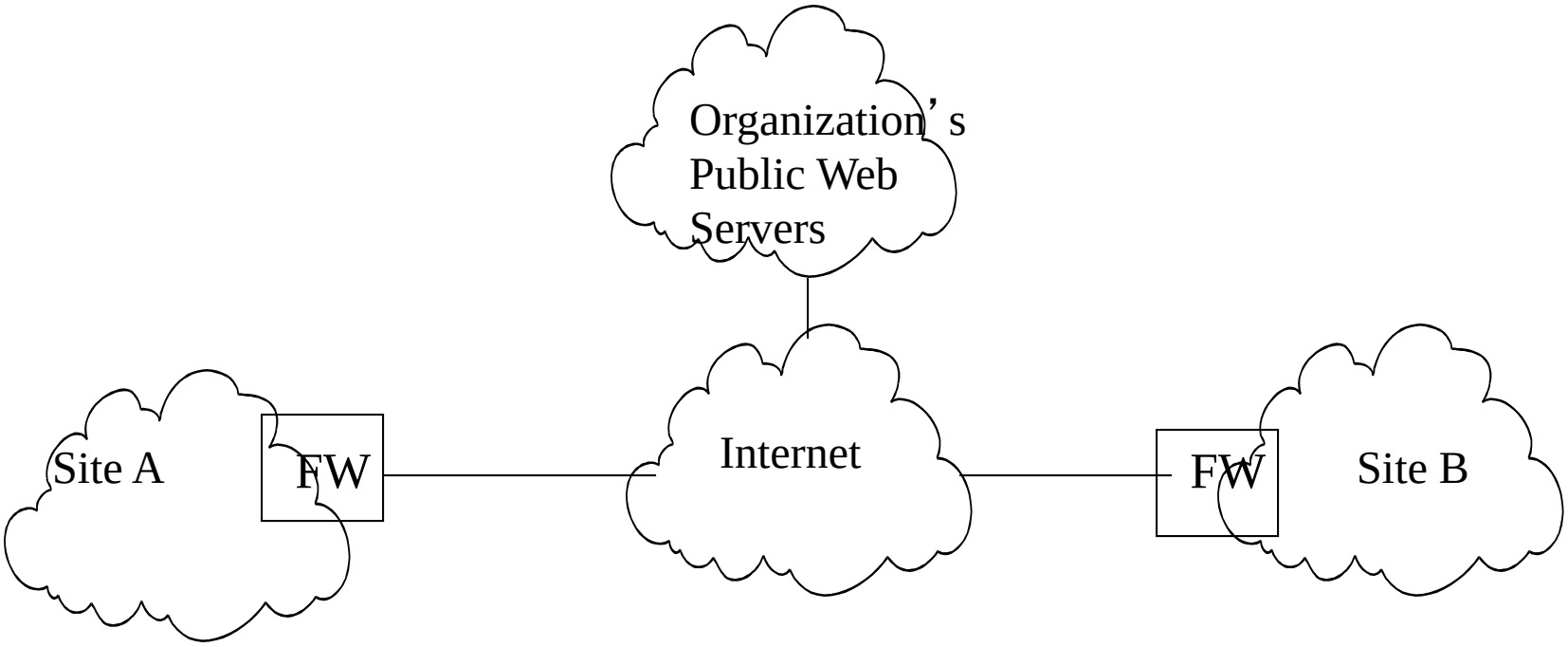
Lecture: Private Network Interconnection

•What if Site A, B are a part of a ‘private’ network, how can data be kept private ?
•How about a VPN
•A Virtual Private Network refers to customer connectivity deployed on a shared infrastructure with the same policies as a private network. The shared infrastructure can leverage a SP’s IP, FR, ATM backbone and may or may not utilize the public Internet.

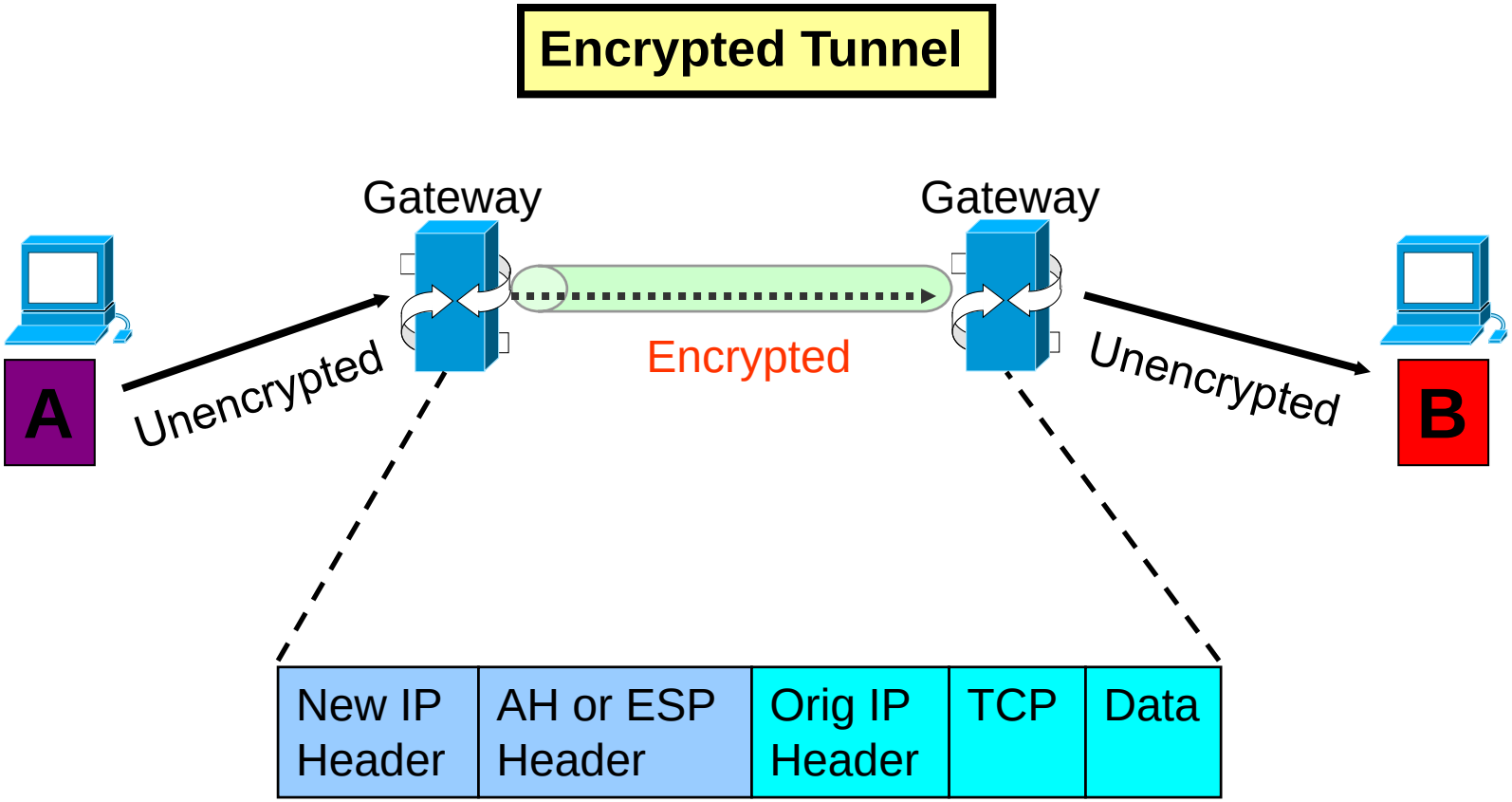


Lecture: Private Network Interconnection

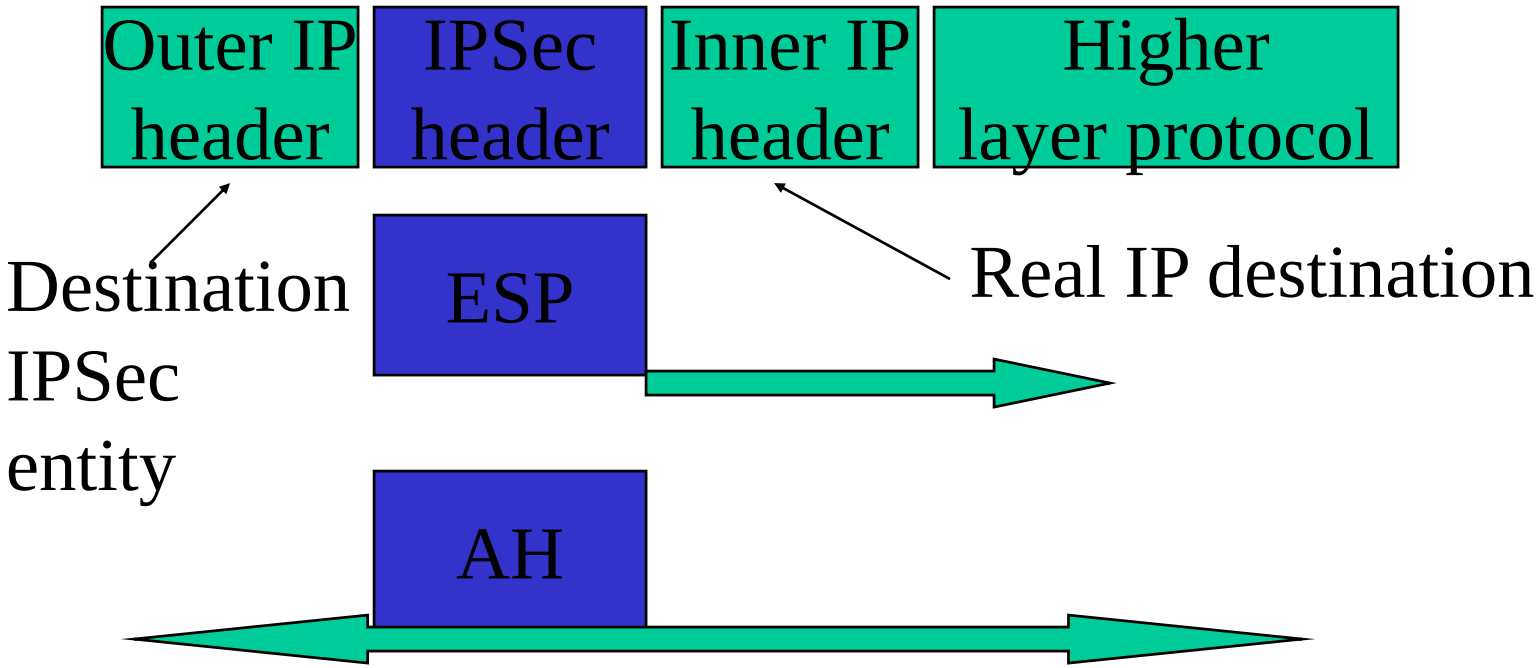
•IPsec: the IETF devised this set of security algorithms along with a general framework that allows a pair of hosts to communicate with varying levels of security.



IPsec Tunnel Mode



Tunnel Mode (II)



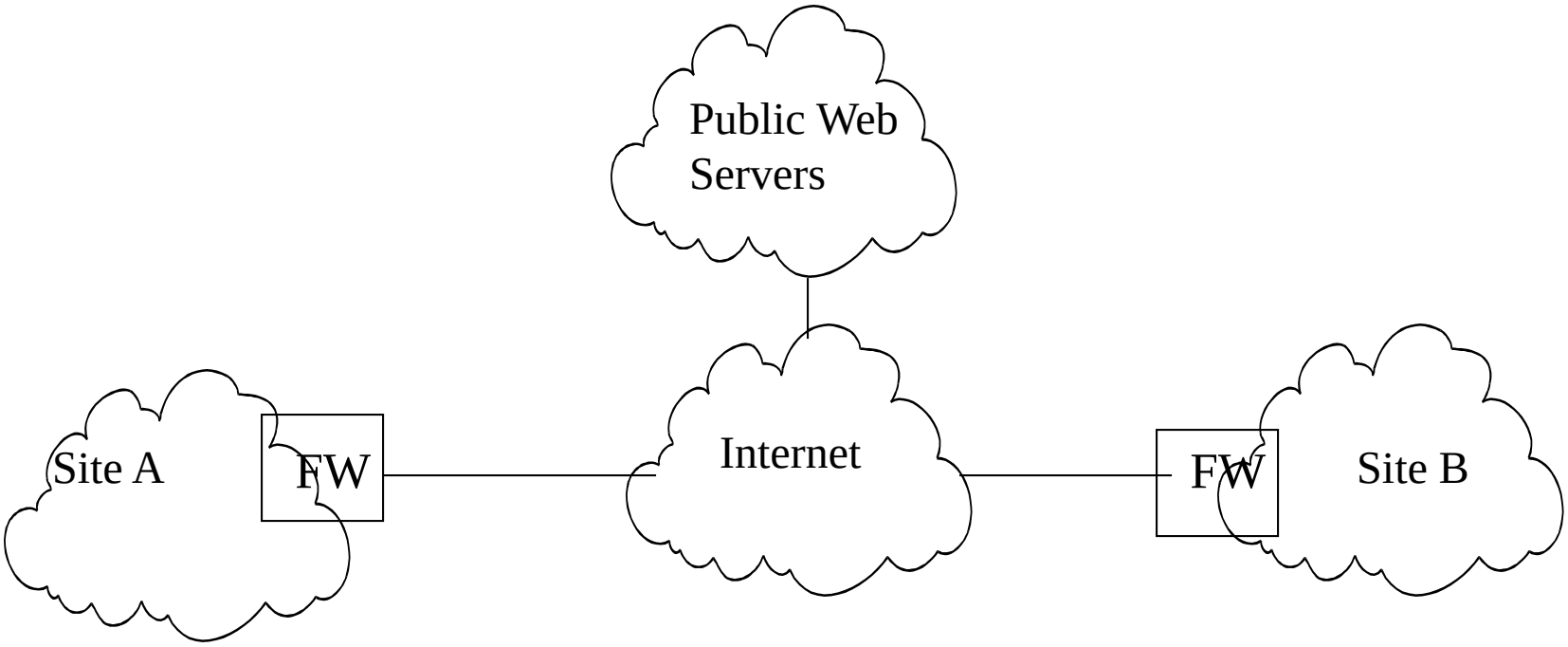
- ESP applies only to the tunneled packet
- AH can be applied to portions of the outer header

Outbound Packet Processing

- Form ESP payload
- Pad as necessary
- Encrypt result [payload, padding, pad length, next header]
- Apply authentication

Lecture: Private Network Interconnection

- So a VPN will interconnect portions of private networks.
- But how would a host at Site A communicate with a public web site?
  - Application Gateways (aka proxy)
  - Network Address Translation (aka NAT)

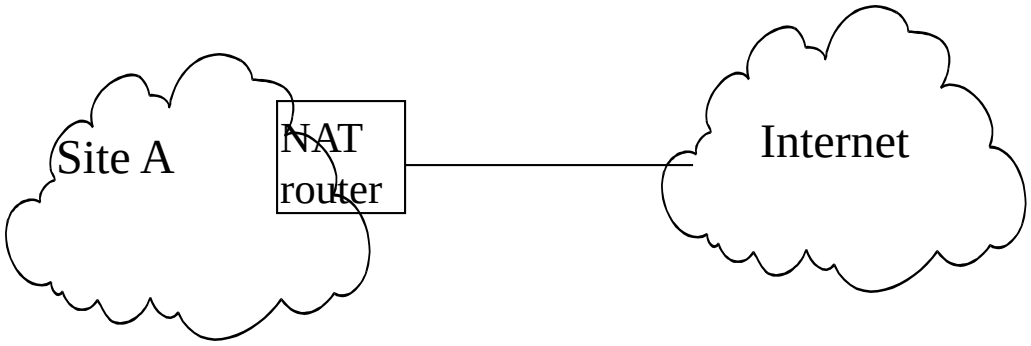


Lecture: Private Network Interconnection

•NAT provides transparent IP-level access to the Internet from a host with a private address

•Defined in RFC 3022:

Basic Network Address Translation or Basic NAT is a method by which IP addresses are mapped from one group to another, transparent to end users. Network Address Port Translation, or NAPT is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. Together, these two operations, referred to as traditional NAT, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses.



Lectur: Private Network Interconnection

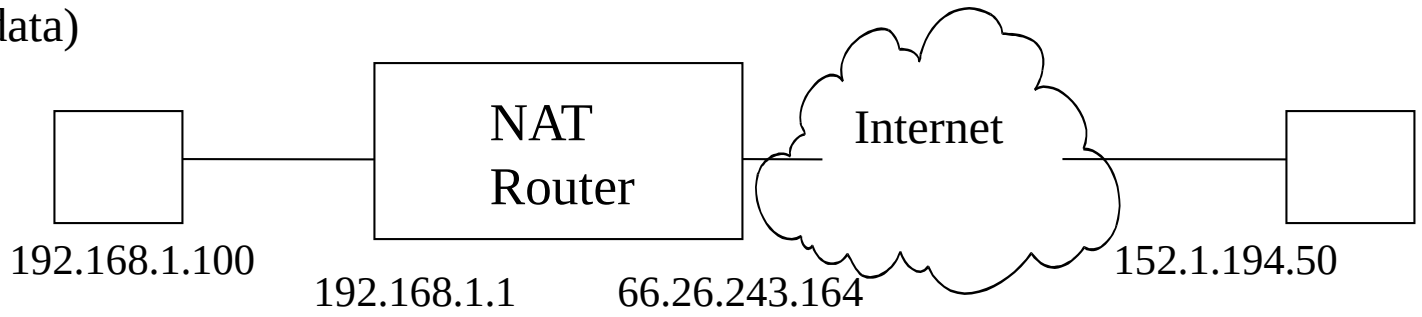
- NAT motivations:
  - solution for private addressing
  - IP V4 IP address depletion problem
- Breaks fundamental IP attribute:
  - does not preserve datagram end-to-end
- Two types defined by ‘basic NAT’
  - Address pool (many-to-a-group or many-to-many)
  - NAPT (network address port translation)

Lecture: Private Network Interconnection

192.168.1.100 > 152.1.194.50: icmp: echo request

4500 0054 01b8 0000 ff01 9da8 c0a8 0164
9801 c232 0800 5753 5e01 0000 1f9e c73a
62cf 0e00 0809 0a0b 0c0d 0e0f 1011 1213
1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
3435 3637

Ping 152.1.194.50
(56 bytes data)



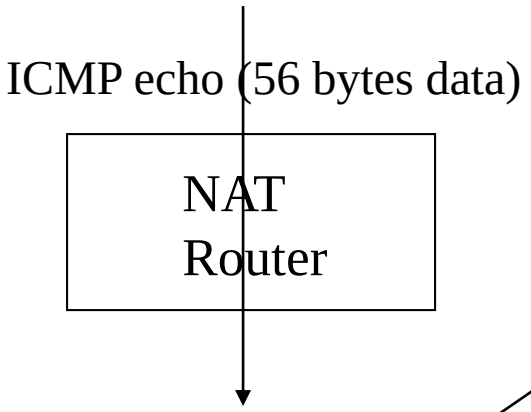
Lecture: Private Network Interconnection

4500 0054 //V4, 20byte header, 84 byte datagram
01b8 0000 //01b8 id , no frag
ff01 9da8   // ttl 255, protocol 1, checksum
c0a8 0164 //src (192.168.1.100)
9801 c232 //dst (152.1.194.50)
0800 5753 //ICMP echo request, checksum
5e01 0000 //Id, seq number
// 56 bytes ICMP data….
1f9e c73a   62cf 0e00 0809 0a0b 0c0d 0e0f
1011 12131415 1617 1819 1a1b 1c1d 1e1f
2021 2223 2425 2627 2829 2a2b 2c2d 2e2f
3031 3233 3435 3637

Lecture: Private Network Interconnection

192.168.1.100 > 152.1.194.50: icmp: echo request

4500 0054 01b8 0000 **ff01 9da8 c0a8 0164**
9801 c232 0800 5753 5e01 0000 1f9e c73a
62cf 0e00 0809 0a0b 0c0d 0e0f 1011 1213
1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
3435 3637



66.26.243.164 > 152.1.194.50: icmp: echo request (captured at dst)

4500 0054 01b8 0000 **f601 32f6 421a f3a4**
9801 c232 0800 5753 5e01 0000 1f9e c73a
62cf 0e00 0809 0a0b 0c0d 0e0f 1011 1213
1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
3435 3637

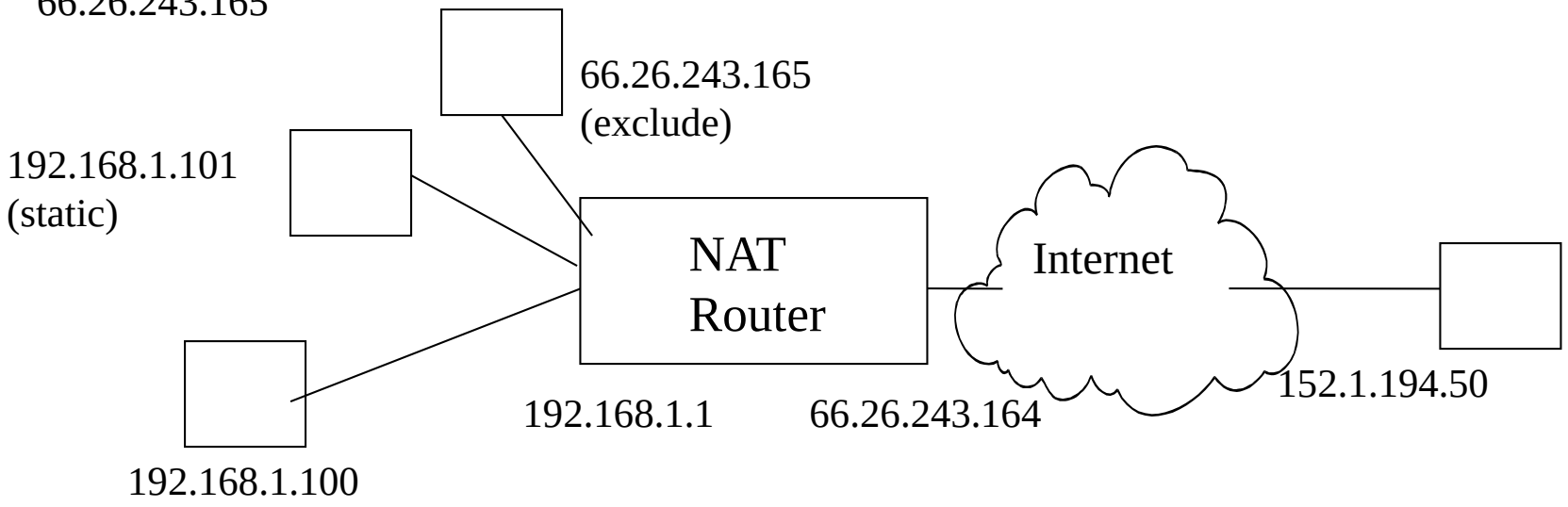
NAT should allocate a new ICMP id (this implementation does not). Why is this required? What if 2 private hosts issued a ping to the same global IP address and each host happened to generate the same ICMP ID? If the NAT router did not modify the ICMP ID on outbound packets, it could not uniquely identify the inbound packets.

Lecture: Private Network Interconnection

NAPT table

-Data structures: Translation Table, Port Map

private address	**private port (ICMPID)**	**NAT address**	**NAT port (ICMP ID)**	**Prot**
192.168.1.100	1050	66.26.243.164	1025	TCP
192.168.1.101	2444	66.26.243.164	1026	TCP
192.168.1.100	5e01	66.26.243.164	1	ICMP
Static entry				
192.168.1.101	80	66.26.243.166	80	TCP
Exclude				
66.26.243.165				



Lecture: Private Network Interconnection

Outbound NAT algorithm

Find table entry
if it does not exist- create

Translate datagram

Inbound NAT algo

Find table entry

If it does not exist ?

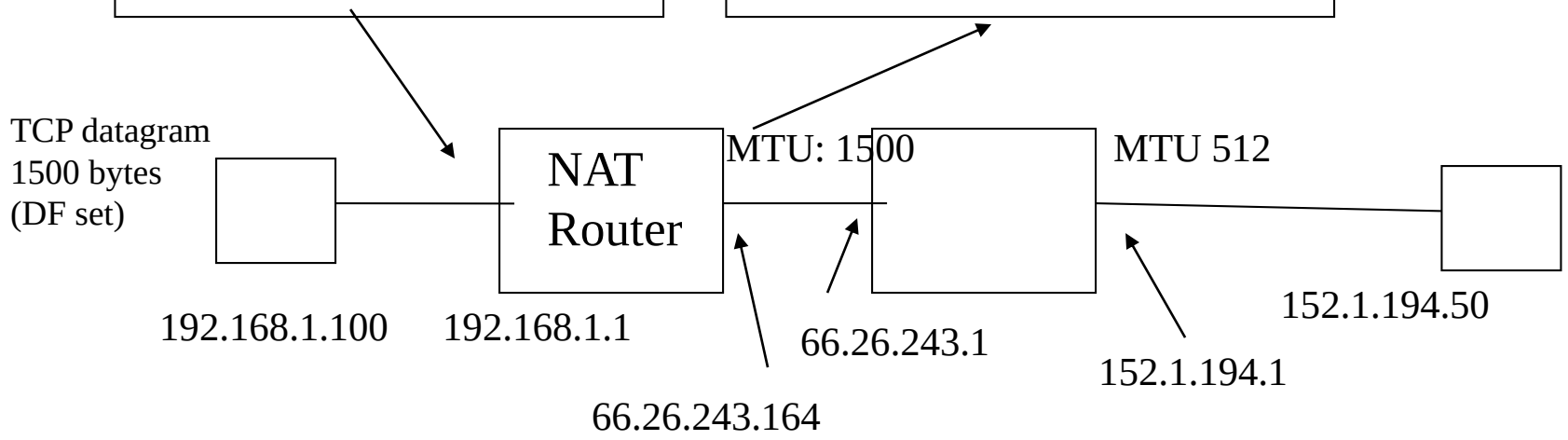
How are table entries removed?

What happens if an inbound datagram is fragmented prior to arriving at the NAT box?

Lecture: Private Network Interconnection

V4, 5bytes, 1500bytes
id:1234, 0x4000 (DF)
ttl:255,TCP, chksum:5678
src:192.168.1.100
dst 152.1.194.50
src port: 2201dst port:5000
seq#: xyz
ack#: abc
len, bits, window
tcp chksum:4321, urgent
1460 bytes data

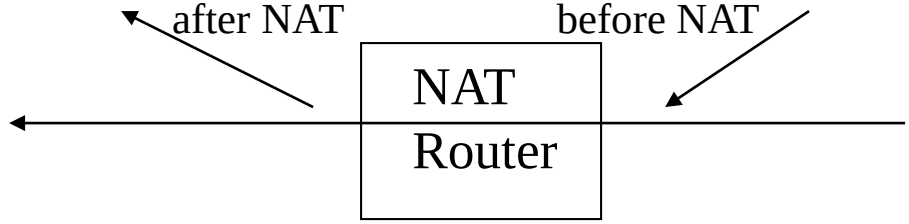
V4, 5bytes, 1500bytes
id:1234, 0x4000 (DF)
ttl:253,TCP, **chksum:9012**
src:66.26.243.164
dst 152.1.194.50
src port: 1025, dst port:5000
seq#: xyz
ack#: abc
len, bits, window
tcp chksum:0987, urgent
1460 bytes data



Lecture: Private Network Interconnection

V4, 5bytes, 56 bytes
id:6767, 0x0000
ttl:253,icmp, **chksum:6565**
src:66.26.243.1
dst192.168.1.100
type 3, code 4, **chksum 4343**
unused
V4, 5bytes, 1500bytes
id:1234, 0x4000 (DF)
ttl:253,TCP, **chksum:6565**
src:192.168.1.100
dst 152.1.194.50
src port: 2201, dst port:5000
seq#: xyz

V4, 5bytes, 56 bytes
id:6767, 0x0000
ttl:255,icmp, chksum:1212
src:66.26.243.1
dst 66.26.243.164
type 3, code 4, chksum 7878
unused
V4, 5bytes, 1500bytes
id:1234, 0x4000 (DF)
ttl:253,TCP, chksum:9012
src:66.26.243.164
dst 152.1.194.50
src port: 1025, dst port:5000
seq#: xyz



ICMP error msg

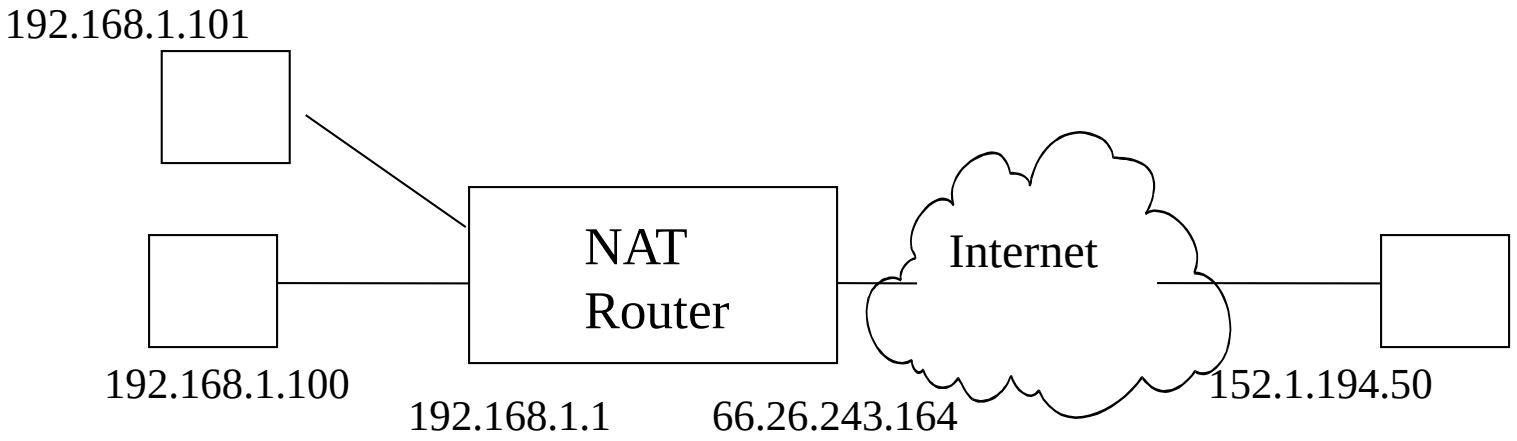
Lecture: Private Network Interconnection

MANY-TO-MANY NAT

-Data structures: Translation table, Address Pool Table

Example Address Pool : range 66.26.243.1 - 66.26.243.32
(note: the actual table might only require the addresses)

private address	NAT address
192.168.1.100	66.26.243.1
192.168.1.101	66.26.243.2



Lecture: Private Network Interconnection

- Many to many NAT
  - original algorithm
  - Example: maps a set of 1024 users to 128 valid global addresses
  - Less demanding than NAT
    - less state (1 entry per host as opposed to 1 / connection)
  - Requires a TO (so does NAPT but not as crucial)
  - Proxy Arp typically used- NAT router must respond to ARP queries on behalf of all global
- Disadvantages: requires multiple IP addresses

Lecture: Private Network Interconnection

- What was the purpose of NAT?

- What's the secondary advantage of NAT (arguably the more important advantage)?

- Does it ensure privacy ?
  - It protects internal addresses from getting out
  - But it does not assure CIA!

Therefore, NAT is not a security protocol- rather it is an "interconnection" method.

Lecture: Private Network Interconnection

- What was the purpose of NAT?
  - To provide private IP to public IP connectivity

- What's the secondary advantage of NAT (arguably the more important advantage)?
  - Hides internal address structure

- Does it ensure privacy ?
  - It protects internal addresses from getting out
  - But it does not provide foundations of security: Confidentiality, Integrity, or Authentication

Therefore, NAT is not a security protocol- rather it is an "interconnection" method.