Network Security
Chapters 26, 40

Security Policy

Inadequate: *Make it secure.*

Must define the goals.

What sort of access must be permitted?

What sort of access must be prevented?

Applies both to networks and hosts.

Security Aspects

Data Integrity
Prevent unauthorized change.

Data Availability
Legit users can get the data.

Data Confidentiality
Non-legit users can't.

Privacy
Sender or client is anonymous.

Who Done It?

Accountability
Who added or accessed that datum?

Authorization
Who said that person could add or access that datum?

Control
Access to machines and data must be controlled.

Encryption

Symmetrical Encryption
$M = decrypt(K, encrypt(K, M))$

Difficult to transmit K.

Public Key Encryption
$M = decrypt(K_{pri}, encrypt(K_{pub}, M))$
$M = decrypt(K_{pub}, encrypt(K_{pri}, M))$
$K_{pub} \neq K_{pri}$

Safe to transmit K_{pub}.

Digital Signatures

Message M
Signature $S = encrypt(K_{pri}, M)$

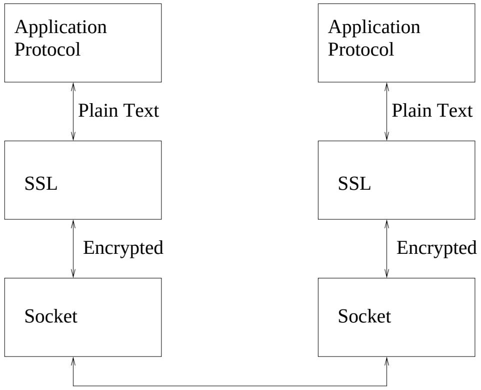
Only holder of K_{pri} can produce $\langle M, S \rangle$
Verify that $M = decrypt(S)$.

Alternative signature: $S = encrypt(K_{pri}, digest(M))$
Verify that $digest(M) = decrypt(S)$.

Second version produces a smaller signature.

Secure Socket Layer

SSL adds a layer between socket and the higher-level protocol.
Such as HTTP.



SSL Handshake

SSL must begin by establishing a secure link
before sending user data.

Symmetric encryption is not secure.
Must share a key.

Public key encryption is slow.

Use public-key encryption to send a symmetric key.

The conversation proceeds using symmetric encryption
on this key.

SSL Handshake

Each side sends some randomly-generated data to the other.

The server sends a certificate containing
its public key to the client.

The client generates a secret which it sends
to the server using its public key.

Both sides use the same secret to produce the same session key.

Optionally, the server may authenticate the client.
Client sends a certificate and signed message.

Certificates

A message signed by a trusted third party.
Certificate Authority.

Contains:
Server's public key
Server's domain name
Issuer's domain name
Issuer's signature

Clients contain a list of CA's and their public keys.

If signature can be verified, the CA vouches
for the server's identity.

If a CA's private key leaks, it's all over.

SSL Services

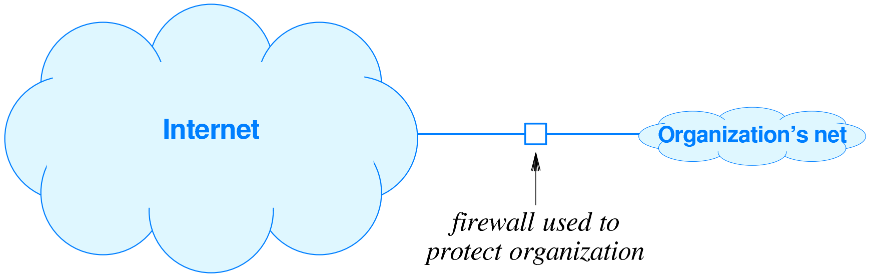
HTTPS

SSH

SFTP

Firewalls

A monitored gateway, really.



Firewall Properties

All traffic entering or leaving passes through.

Rejects traffic outside the security policy.

Cannot be attacked.
Best to run no other services on it.

Packet Filters

Examine each packet.

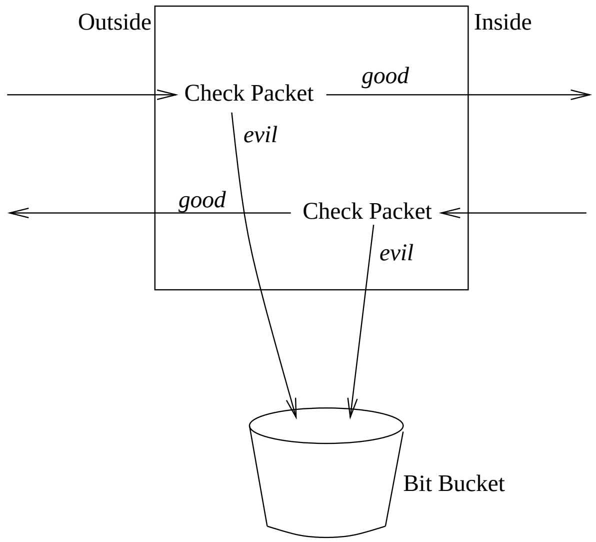
Rules determine if we like this packet.

If we don't it's gone.

Rules primarily examine the source and destination host and port.

For instance:
Discard HTTP packets going to machines not the web server.
Discard packets from fred.edu.
Discard packets from outside claiming to be from inside.

Packet Filters



Packet Filter Types

Stateless

Examine each packet in isolation.

Stateful

Remember previous packets.

Handles Connections Better.

Network Address Translation

Multiple interfaces
Like any router

Rewrites packets passing through.
Change source outbound; change destination inbound

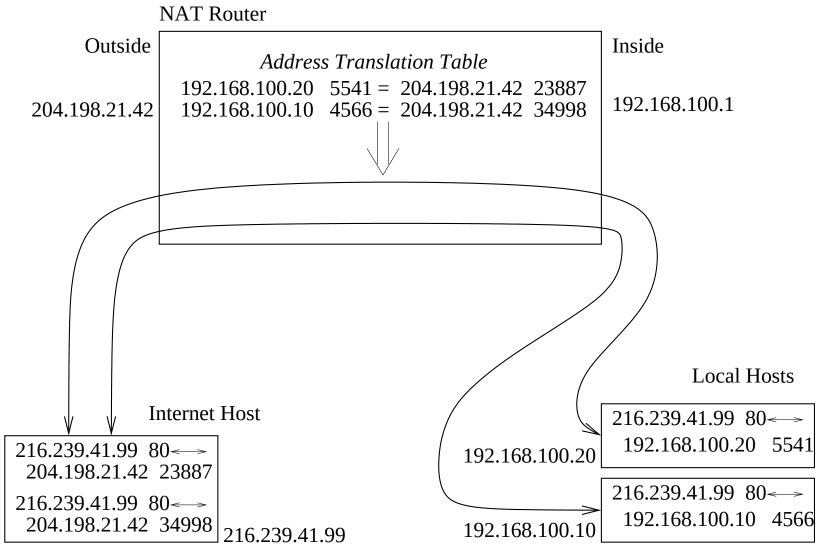
Represents internal hosts with its own local port numbers.

Internal hosts see only the external host.

External hosts see only the outside of the NAT router.

Multiple internal addresses can use one external address.
Multiple local addresses become multiple port numbers.

NAT Routers



NAT Router

Outside

204.198.21.42

Address Translation Table

192.168.100.20 5541 = 204.198.21.42 23887
192.168.100.10 4566 = 204.198.21.42 34998

Inside

192.168.100.1

Internet Host

216.239.41.99 80 ⟷ 204.198.21.42 23887

216.239.41.99 80 ⟷ 204.198.21.42 34998

216.239.41.99

Local Hosts

192.168.100.20

216.239.41.99 80 ⟷ 192.168.100.20 5541

192.168.100.10

216.239.41.99 80 ⟷ 192.168.100.10 4566

Proxy Servers

Clients connect to the proxy.

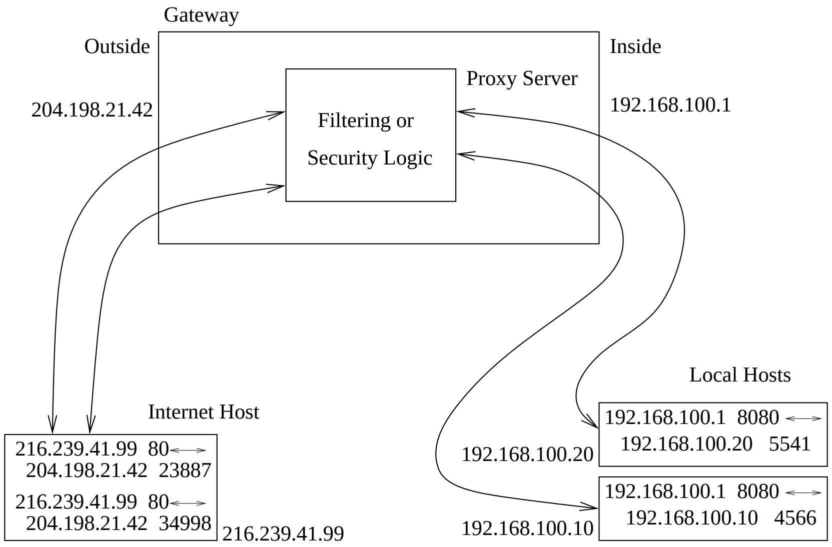
Proxy connects to the external host.

The proxy generally forwards traffic.
Blocks and alters as required.

Proxies understand user-level protocols.
HTTP, FTP, etc.

Client is aware of the proxy.

Proxies



Gateway

Outside

204.198.21.42

Proxy Server

Filtering or
Security Logic

Inside

192.168.100.1

Internet Host

216.239.41.99 80 ⟷ 204.198.21.42 23887

216.239.41.99 80 ⟷ 204.198.21.42 34998

216.239.41.99

Local Hosts

192.168.100.20

192.168.100.1 8080 ⟷ 192.168.100.20 5541

192.168.100.10

192.168.100.1 8080 ⟷ 192.168.100.10 4566

Transparent Proxies

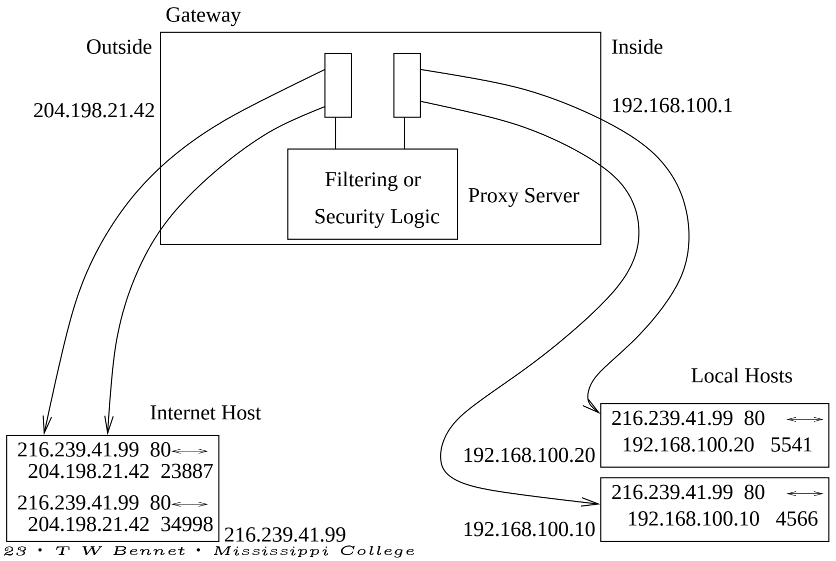
Proxies of which the client is not aware.

Clients connect to the external host, but the gateway modifies the traffic.

Normal proxies operate without changing the operation of TCP or IP.

Transparent proxies need the IP layer to send them packets addressed elsewhere.

Transparent Proxies



Gateway

Outside

Inside

204.198.21.42

192.168.100.1

Filtering or Security Logic

Proxy Server

Internet Host

216.239.41.99 80 ↔ 204.198.21.42 23887

216.239.41.99 80 ↔ 204.198.21.42 34998

216.239.41.99

Local Hosts

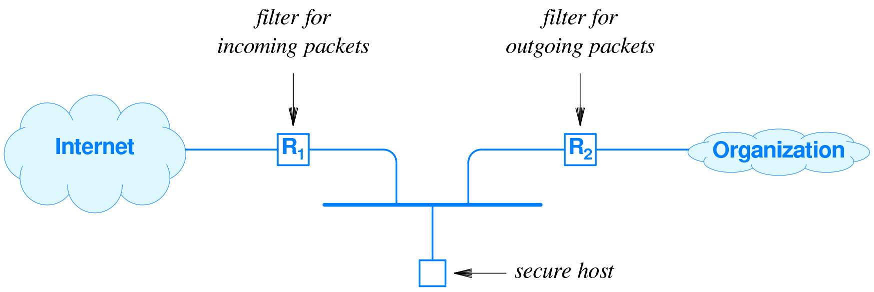
216.239.41.99 80 ↔ 192.168.100.20 5541

216.239.41.99 80 ↔ 192.168.100.10 4566

192.168.100.20

192.168.100.10

A Hardened Gateway



filter for incoming packets

filter for outgoing packets

Internet

R_1

R_2

Organization

secure host

Breaking In

Goals

Run commands.

Run privileged commands.

Means

Hijack a server.

Log in and hijack some local program.
Perhaps steal a password.

Fool someone into running the commands for you.

Passwords

Talk someone out of one.

Find one written down.

Snoop the net.

Guess.
Some web servers make this easy.

Buggy Servers

Provide services they are not s'posed to.

Buffer overflow

Temp file problems

Known bugs get posted on hacker sites.

Port scanning.
nmap

Trojans

Trick a legit user into running the code for you.
Email viruses are a form of this.

A trojan can start a surreptitious server.
Back orifice.

Firewall Security

Prevent outside access to services.
Running deliberately or not.

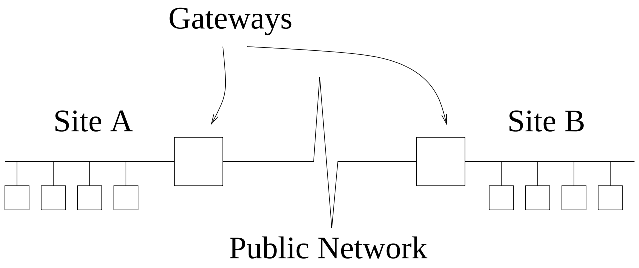
Prevent outside access to servers run by idiots.
Deployed thoughtfully or not.
Usually not.

Allow a concentration of attention on one machine.
Easier to secure one server than all the desktops.

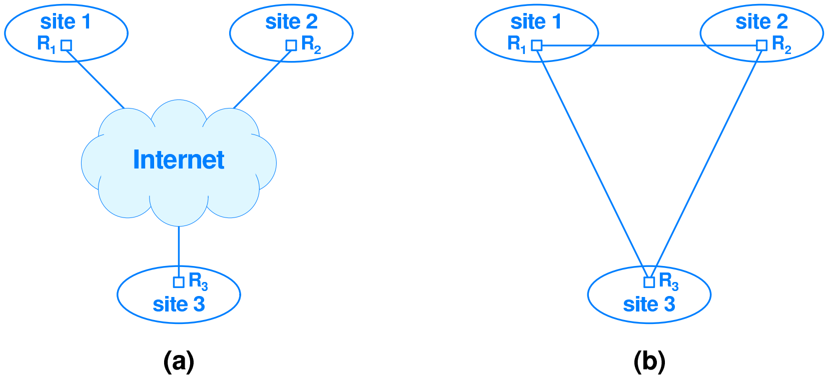
Prevent a hacker from learning about the network.
Port scans don't go past the firewall.

Virtual Private Network

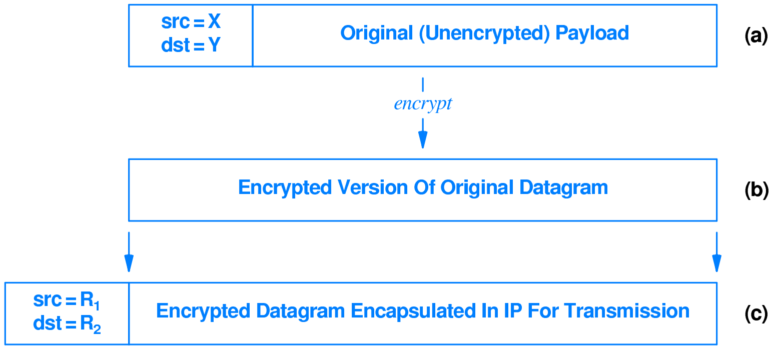
Use public Internet as a private link.



Virtual Private Network



Virtual Private Network Encoding



src = X
dst = Y | Original (Unencrypted) Payload (a)

encrypt

Encrypted Version Of Original Datagram (b)

src = R_1
dst = R_2 | Encrypted Datagram Encapsulated In IP For Transmission (c)

Tunneling

Sources

Comer, *Computer Networks and Internets*
(Our beloved textbook.)

http://www.pseudonym.org/ssl/ssl_intro.html