ROYAL INSTITUTE
OF TECHNOLOGY

Intrusion Detection and Firewalls
IV1013

Markus Hidell, mahidell@kth.se
KTH School of ICT

Acknowledgements

- The presentation builds upon material from
  - Previous slides by Markus Hidell and Peter Sjödin
  - Material by Vitaly Shmatikov, Univ. of Texas
  - *Network Security Essentials*, 5th ed, William Stallings, Pearson
  - *Computer Networking: A Top Down Approach*, 5th ed, Jim Kurose, Keith Ross, Addison-Wesley
  - *TCP/IP Protocol Suite*, 4th ed, Behrouz Foruzan, McGraw-Hill

ROYAL INSTITUTE
OF TECHNOLOGY

Intrusion Detection

Intruders

- Often referred to as hacker or cracker
  - One of two most well-known threats (other is viruses)
- Three classes (as of study from 1980)

Masquerader: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account

Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges

Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

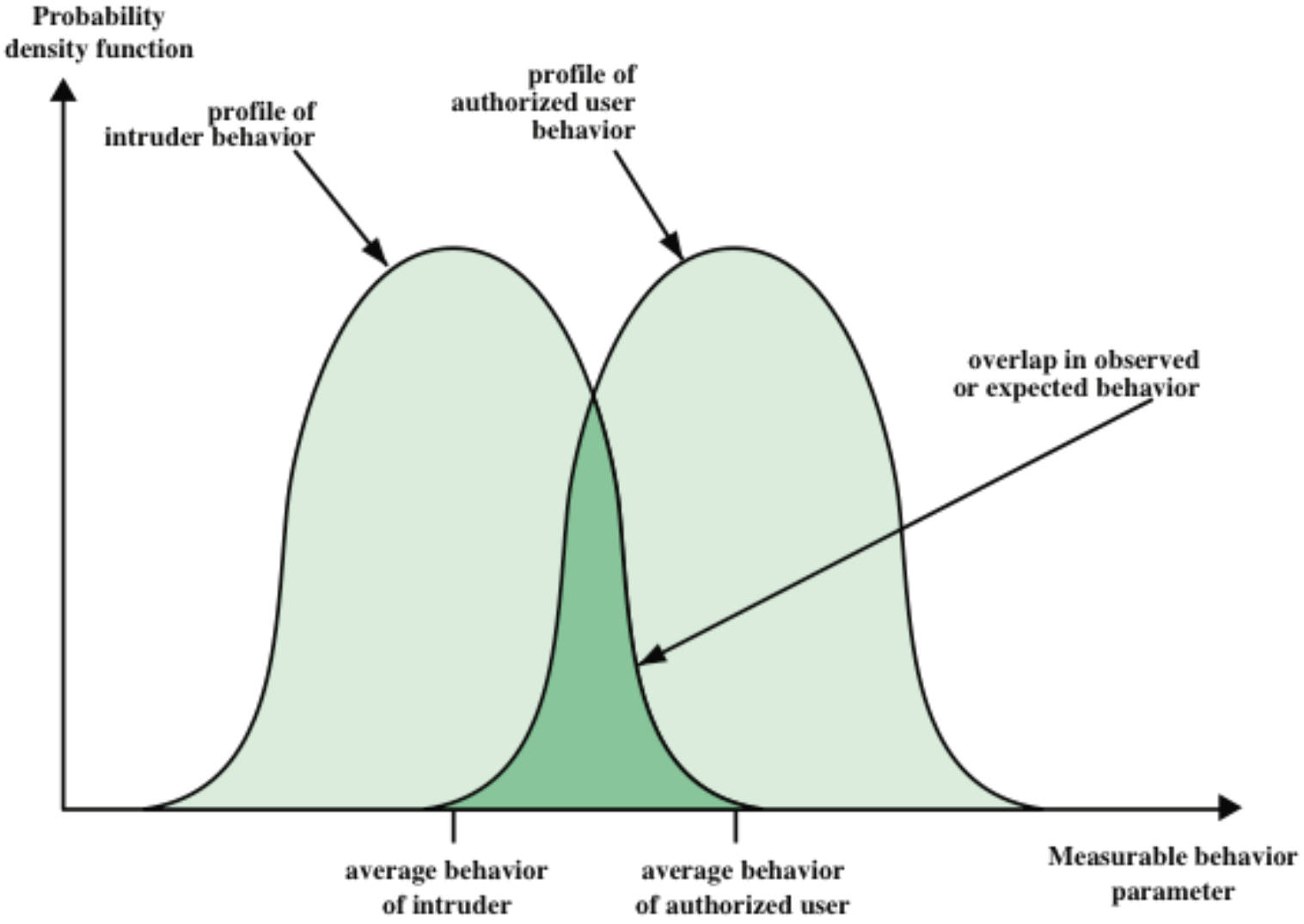
Examples of Intrusion

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password
- Using an unattended, logged-in workstation without permission

Intrusion Detection

- A system's second line of defense
- Based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified
- Considerations:
  - If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system
  - An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions
  - Intrusion detection enables the collection of information to learn about intrusion techniques
    - Strengthen the protection in the future

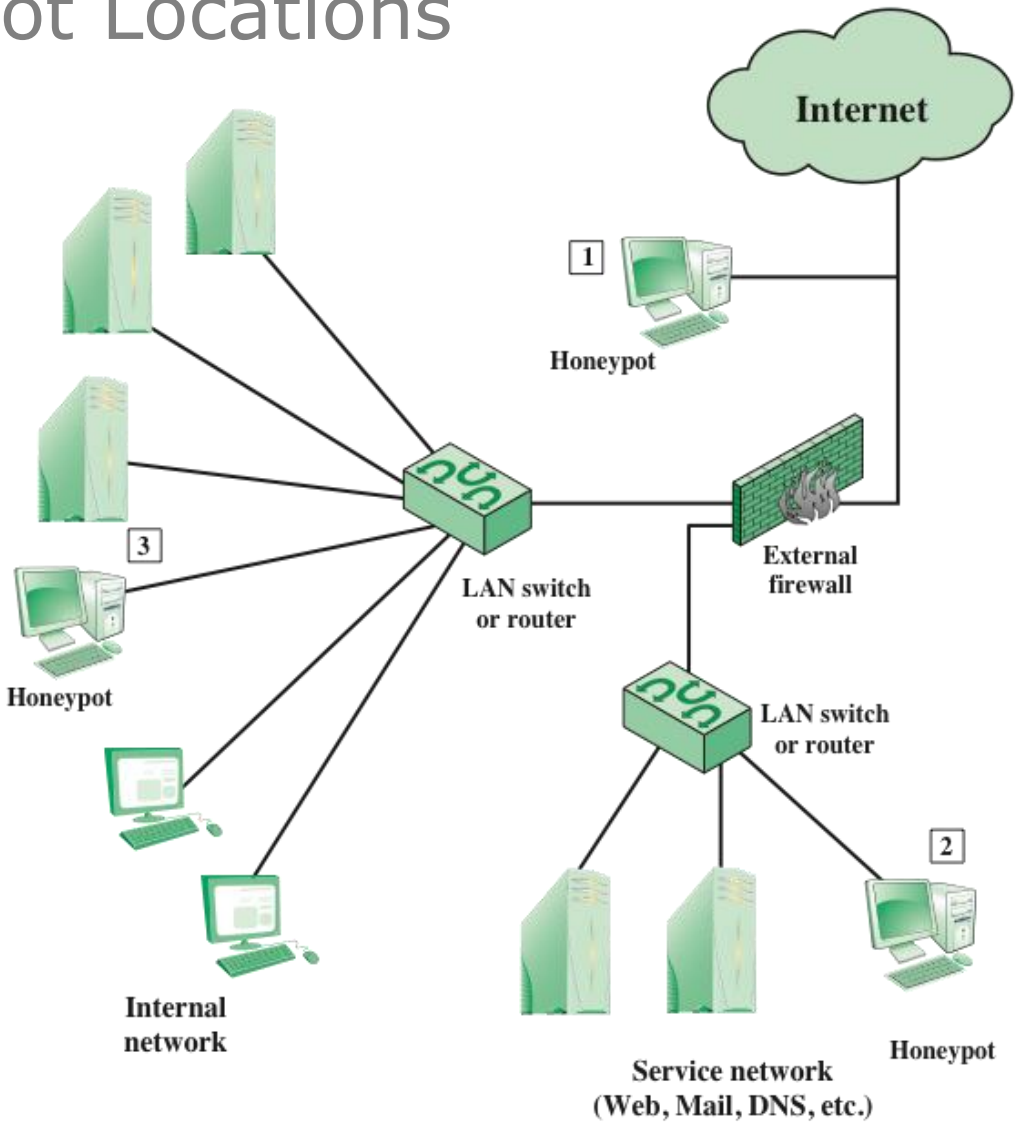
Intrusion Detection in Abstract Terms



Honeypots

- Decoy systems designed to entice a potential attacker away from critical systems
- Designed to
  - Divert an attacker from accessing critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
- Honeypot has no production value
  - Attempts to communicate with honeypots is most likely a probe, scan or attack

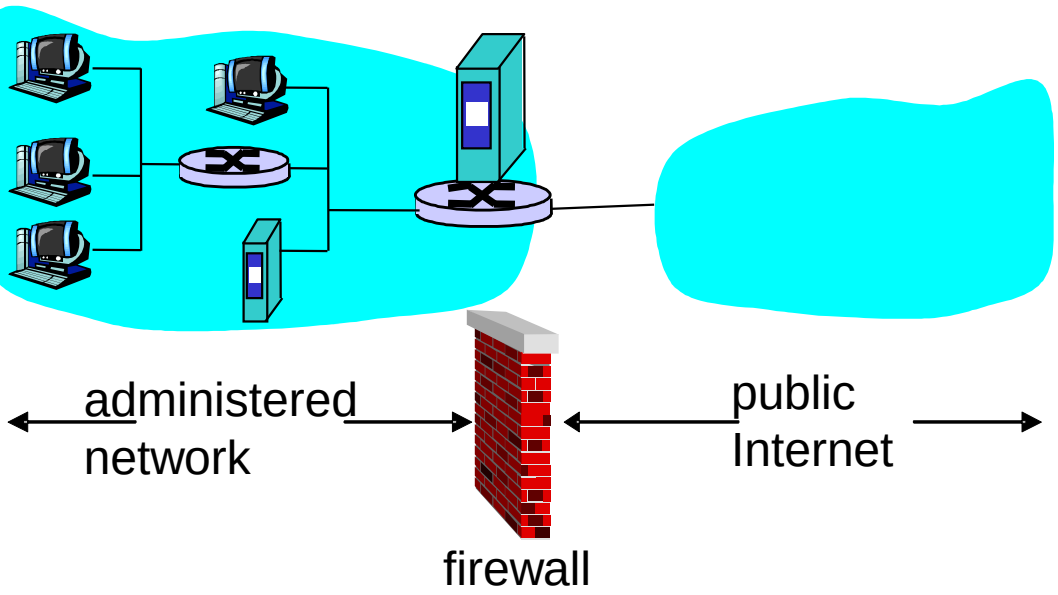
Honeypot Locations



ROYAL INSTITUTE
OF TECHNOLOGY

Firewalls

Firewall Definition



Isolates organization's internal network from larger Internet, allowing some packets to pass and blocking others

Firewalls—General Techniques

- Service control
  - Determines the types of Internet services that can be accessed, inbound or outbound
    - Packet filtering, proxy software, hosting server software
- Direction control
  - Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall
- User control
  - Controls access to a service, can be applied to local users or to external users (requires secure authentication)
- Behavior control
  - Controls how particular services are used
    - E.g., filter email to eliminate spam or enable access to only parts of the information on a local web server

Firewall Capabilities

Defines single choke point where security capabilities are consolidated

Provides location for monitoring security-related events, can implement audits and alarms

Provides convenient platform for several non-security related functions: NAT, logging, etc

Can serve as platform for IPsec, can implement tunnel mode end-point

Firewall Limitations

Cannot protect against attacks bypassing the firewall, e.g., dial-in modem pools

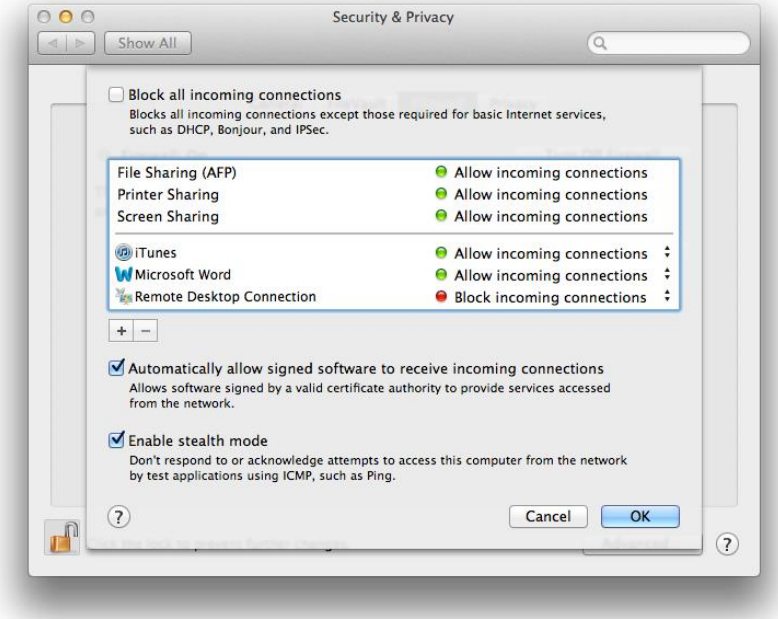
Cannot guard against unprotected wireless LANs

Cannot protect agains internal threats, e.g., disgruntled employees

A laptop (or other portable device) infected outside firewall can still contaminate the internal network

Firewall Locations in the Network

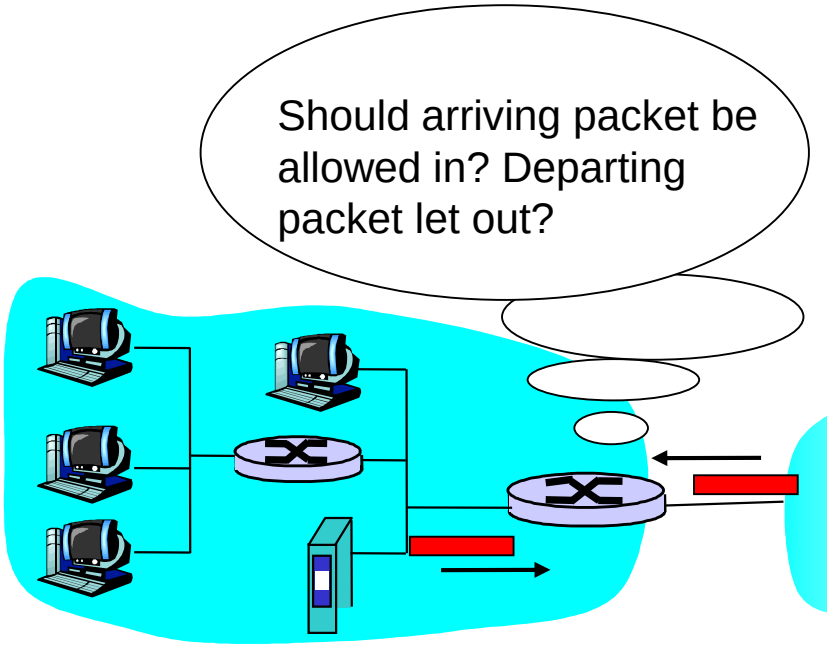
- Between internal LAN and external network
- At the gateways of sensitive subnets within the organizational LAN
  - Payroll's network must be protected separately within the corporate network
- On end-user machines
  - "Personal firewall"
  - Mac OS X, for instance

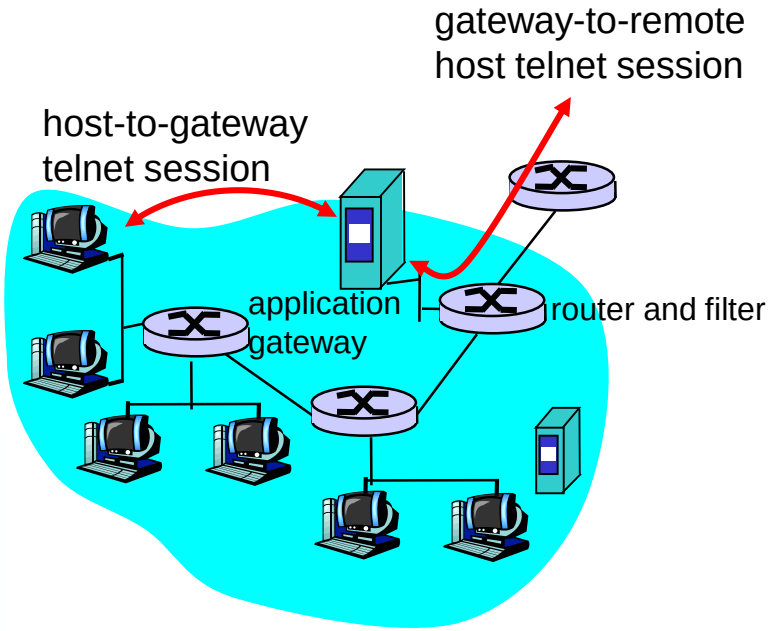


Firewall Types

Packet filter:
internal network connected to Internet via *router firewall*

Application level gateway:
splices and relays two application-specific connections





Packet Filters

- For each packet, firewall decides whether to allow it to proceed
  - Decision must be made on per-packet basis
- To decide, use information available in the packet
  - IP source and destination addresses, ports
  - Protocol identifier (TCP, UDP, ICMP, etc.)
  - TCP flags (SYN, ACK, RST, PSH, FIN)
  - ICMP message type
- Filtering rules are based on pattern-matching
  - Deep packet inspection

Packet Filter Default Policies

Two default policies:

- Default = discard
  - That which is not explicitly permitted is prohibited
- Default = forward
  - That which is not explicitly prohibited is permitted

- Default = discard is more conservative
  - Services added on a case-by-case basis
  - Very visible to users....

Packet Filtering—Examples

- Example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
  - All incoming and outgoing UDP flows carrying telnet connections are blocked.

- Example 2: Block inbound TCP segments with ACK=0.
  - Prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

TCP has a flag, called ACK, that is set on all but the first packet, the one that establishes the connection. So, if the firewall disallows packets from B without ACK set in the TCP header, then we will have the desired effect, in general.

Packet Filtering—Ruleset Example

Rule	Direction	Src addr	Dst addr	Protocol	Dst port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

A: Inbound mail from external source allowed (port 25 for SMTP)
B: Intended to allow response to an inbound SMTP connection
C: Outbound mail to an external source is allowed
D: Intended to allow response to an outbound SMTP connection
E: Explicit statement of the default policy (all rulesets include this one)

Ruleset Problems

Rule	Direction	Src addr	Dst addr	Protocol	Dst port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Rule D: allows external traffic to any port >1023 → external attacker can open connection from port 5150 to internal web server on port 8080

Solution: add source port 25 for B&D and source port >1023 for A&C

Rule D: attacker could have other application linked to port 25 and send TCP segments to internal machines

Solution: add TCP ACK flag set to rule D

Rule	Direction	Src addr	Dst addr	Protocol	Src port	Dst port	Flag	Action
D	In	External	Internal	TCP	25	>1023	ACK	Permit

Weaknesses of Packet Filters

- Do not prevent application-specific attacks
  - For example, if there is a buffer overflow in URL decoding routine, firewall will not block an attack string
- No user authentication mechanisms
  - … except (spoofable) address-based authentication
  - Firewalls don’t have any upper-level functionality
- Vulnerable to TCP/IP attacks such as spoofing
  - Attacker sends packets with IP src address belonging to the internal network
- Security breaches due to misconfiguration

PF: Attacks and Countermeasures

- IP address spoofing
  - Attacker sends packet with internal src address
  - Countermeasure: discard packets with inside source address arriving on an external interface
- Source routing attacks
  - Use source routing IP option to try to bypass security measures
  - Countermeasure: discard all packets with this IP option
- Tiny fragment attacks
  - Intruder uses IP fragmentation to create very small fragments to circumvent filtering on TCP header information
  - Countermeasure: Discard packets based on protocol type and IP fragment offset (remember first fragment rejected and discard subsequent fragments)

Stateful Inspection Firewalls

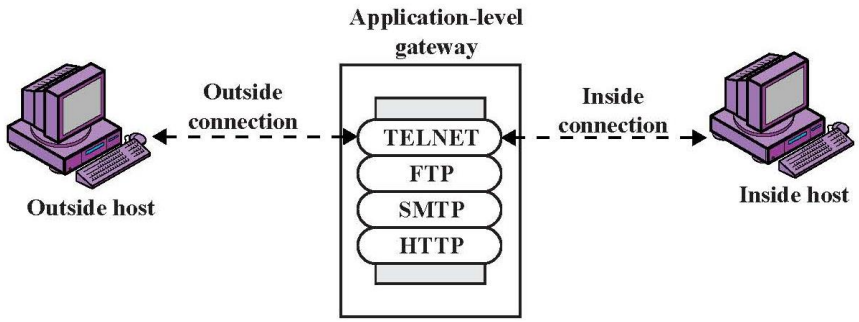
- Simple firewalls permit inbound TCP traffic on all high-numbered ports, >1023
  - Vulnerability that can be exploited
- Stateful inspection firewalls have tighter rules for TCP
  - Create directory of outbound TCP connections
    - One entry per established connection
    - Allow incoming traffic to ports only for those

Src addr	Src port	Dst addr	Dst port	Connection state
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established

Stateful Packet Filters

- Can track related connections for well-known protocols
- There are protocols that require B to make a TCP connection to A, even though A initiated the session
  - FTP (control connection and data connection)
- Stateful packet filter
  - Note that connection was initiated from *s* (internal) to *d*
  - Allow (for some period of time) connections from *d* to *s*

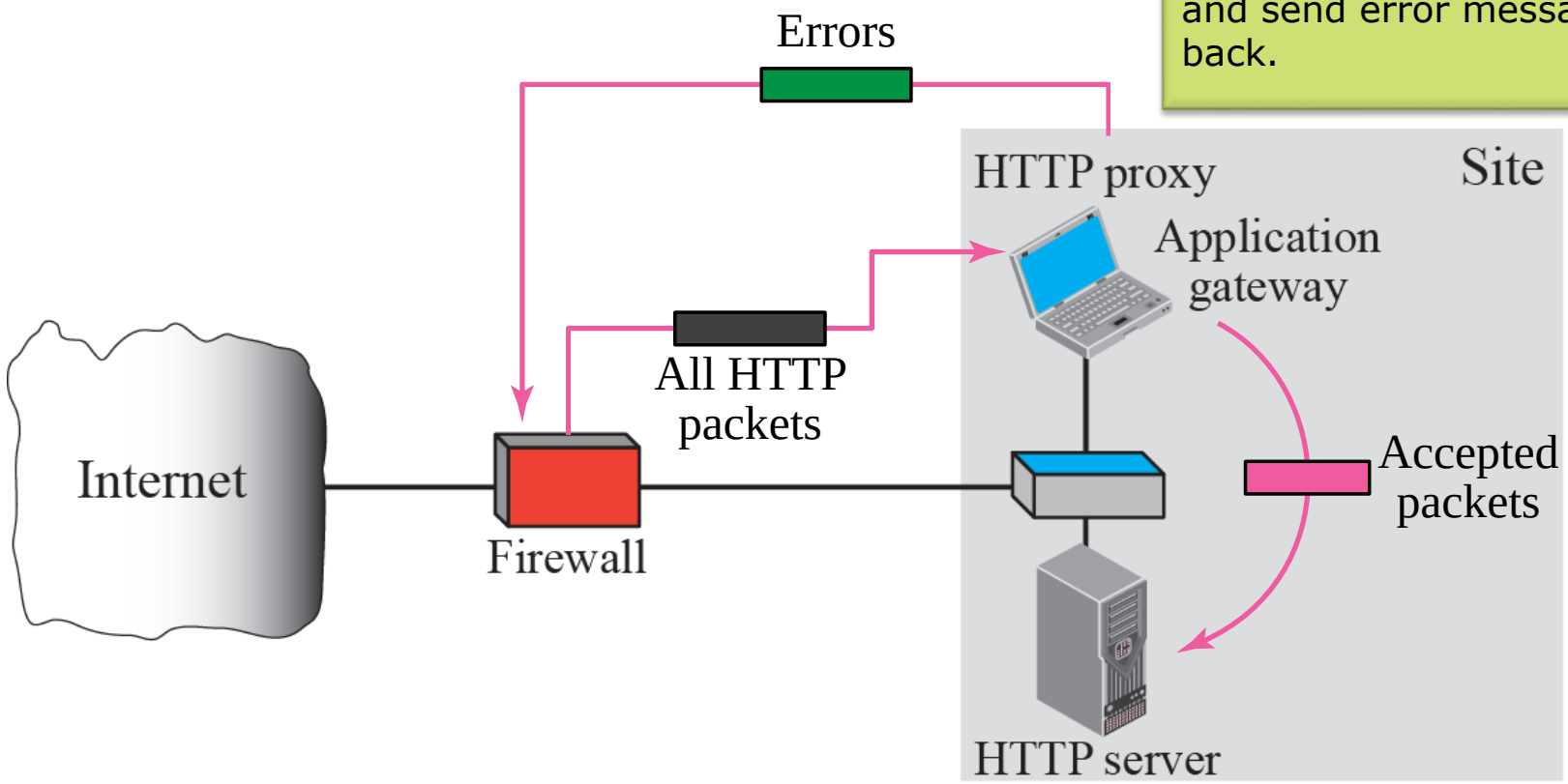
Application-Level Gateway



- Also referred to as *application proxy*
- Splices and relays two application-specific connections
  - Common example: HTTP gateway (proxy server)
- Can support high-level user-to-gateway authentication
  - Log into the proxy server with your name and password
- Simpler filtering rules than for arbitrary TCP/IP traffic
- Each application requires implementing its own proxy
  - Proxy might be a performance bottleneck

Proxy Firewall (same thing as application-level gateway)

If packet is legitimate, act as client and send packet to server. If not legitimate, drop and send error message back.



©The McGraw-Hill Companies, Inc., 2000

Some Comparisons

- Packet filter can do its job without requiring software changes in the communicating nodes
  - Allowed conversations proceed normally (in most cases)
- An application level gateway is visible to the users
  - Need to connect to the gateway
- Application level gateway can be more powerful than packet filters—e.g., look at data inside email messages
  - Gateway is application-aware

General Problems with Firewalls

- Interfere with networked applications
  - Can make it difficult for legitimate user to get the work done
- Many problems not solved with firewalls
  - Buggy software (like buffer overflow exploits)
  - Firewall friendly protocols
    - Run IP over HTTP.....
- Don’t prevent insider attacks
- Increasing complexity and potential for misconfiguration

ROYAL INSTITUTE
OF TECHNOLOGY

Thanks for listening