

CS 6v81 - Network Security

Firewalls and Intrusion Detection Systems

Firewalls

2

(Source: Stallings' book, papers)

What is a *firewall* ?

- ▶ Collection of components between two networks that filter cross traffic based on some security policy
- ▶ Used as a perimeter defense – to block/permit untrusted/trusted access to internal resources protecting networks and hosts
- ▶ Can also be used to block access to certain external Internet sites by internal users
 - ▶ To prevent users from downloading from blacklisted sites
 - ▶ To prevent users from visiting blacklisted sites, etc.
- ▶ **Challenge:** managing a large number of firewalls and ensuring they enforce a consistent policy across the organization's network

3

Firewall capabilities

- ▶ Installed at the boundary, *choke point*, of the nw to
 - ▶ Keep unauthorized users out of the nw
 - ▶ Prohibit potentially vulnerable services from entering/exiting the network
 - ▶ Provides protection from IP spoofing and routing attacks
- ▶ Provides a location for monitoring security-related Internet functions
 - ▶ Can implement audits and alarms
- ▶ Can implement several security-related functions
 - ▶ Network address translation
 - ▶ Network management – auditing and logging of Internet usage
- ▶ Can be an end point for a VPN connection

4

Firewall limitations

- ▶ Cannot protect against attacks that bypass firewall
 - ▶ Dial-out / dial-in systems for commuting employees
- ▶ Cannot protect against internal threats
 - ▶ A disgruntled employee
 - ▶ An unwitting employee cooperating with attacker
- ▶ Cannot protect against the transfer of virus-infected programs or files
- ▶ Need to be customized to specific use scenario
 - ▶ Difficult and error-prone process, requires verification and testing to ensure that it does what it is supposed to do

5

Firewall limitations, cont'd

- ▶ Traffic amount and the need to analyze packet content may cause firewalls to become congestion point in the network
- ▶ Diversity of network access technologies may necessitate use of multiple firewalls for each access point resulting in the need for distributed firewall management
- ▶ End-to-end encryption is an issue for firewall use

6

Types of Firewalls

- ▶ Packet filtering firewalls
- ▶ Stateful inspection firewalls
- ▶ Application level firewalls
- ▶ Circuit level firewalls

7

Types of Firewalls

- ▶ Packet-filtering firewalls
 - ▶ A router with a set of static rules/filters to determine which packets are allowed to cross the inspection point
 - ▶ Filtering is based on info contained in the packet
 - ▶ Source/Dest IP; source/dest port no; IP protocol field; router interface
 - ▶ Limitations due to operation on individual packets
 - ▶ Cannot filter packets that use application layer vulnerabilities
 - ▶ Attacks involving multiple packets
 - ▶ Ex. A hand crafted bogus TCP ACK packet for a non-existent TCP connection
 - ▶ IP address spoofing
 - ▶ Source routing based attacks
 - ▶ Tiny fragmentation attacks

8

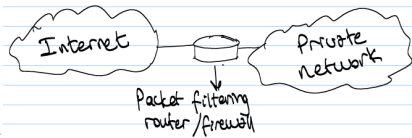
Types of Firewalls

- ▶ Packet-filtering firewalls – Example rules

Action	Ourhost	Port	Theirhost	Port	comment
Block	*	*	SPIGOT	*	We don't trust these people
Allow	OUR-GW	25	*	*	Connection to our SMTP port

Action	Ourhost	Port	Theirhost	Port	comment
Block	*	*	*	*	Default is to block all traffic

Packet Filtering Firewall – Deployment



9

Types of Firewalls

- ▶ Stateful inspection firewalls
 - ▶ Inspects packets in the context of their role in an incipient or ongoing conversation (e.g., TCP connection)
 - ▶ Maintains data about open connections to ensure that the packet is part of a valid connection initiated by an authorized user
 - ▶ Enforces policy on which type of conversation can take place (e.g., TCP connections if opened by local users)
 - ▶ Maintains state for ongoing connections and accepts incoming packets for those connections only if they fit the profile of the connections

10

- ▶ Stateful inspection firewalls

- ▶ Maintain a table for allowed connections
 - ▶ By default, allow connections originated from internal hosts & deny connections originated from external hosts
 - ▶ Accept packets belonging to allowed connections with no/minimal inspection
 - ▶ Only the initial packets are matched against firewall rule db
 - ▶ Other packets are matched with table of allowed connections
 - ▶ Ex. connection table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	192.168.5.12	64333	129.110.44.12	80	OK
UDP	192.168.33.13	60002	129.110.23.5	69	OK

11

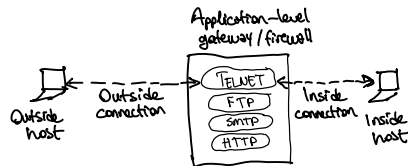
Types of Firewalls

- ▶ Application-level firewall – proxy server
 - ▶ Relays application traffic
 - ▶ Client application contacts the relay to establish a connection and have it relay packets in both directions on its behalf
 - ▶ Adv
 - ▶ More secure than packet filters
 - ▶ User authentication allows for effective blocking of unwanted traffic
 - ▶ Easy to log and audit all incoming traffic at protocol level
 - ▶ Disadv
 - ▶ Requires additional processing overhead for each connection
 - ▶ Effectively two connections between the users
 - ▶ Still susceptible to SYN floods and ping floods

12

Types of Firewalls

- ▶ Application-level firewall – proxy server



13

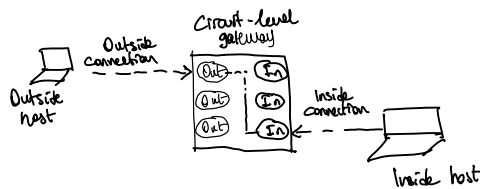
Types of Firewalls

- ▶ Circuit-level firewall
 - ▶ A stand-alone system or a specialized function performed by an application level gateway
 - ▶ Does not permit an end-to-end TCP connection
 - ▶ Gateway sets up two connections – one with inner host, one with outside host
 - ▶ Before the connection is set up, user must authenticate
 - ▶ After authentication, TCP segments are forwarded between the two sides without examining their content
 - ▶ Security provided by determining which connections are allowed
 - ▶ Can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections

14

Types of Firewalls

- ▶ Circuit-level firewall



15

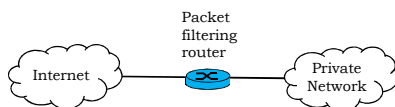
Bastion host

- ▶ A system that hosts application-level or circuit-level gateways in a critical point in the network
 - ▶ Hosts only the required/minimal set of services and shuts down all unnecessary services
 - ▶ May require additional authentication before a user is allowed to access the proxy services
 - ▶ Proxy modules include bare minimum required service functionality for network security

16

Firewall Deployment Topologies

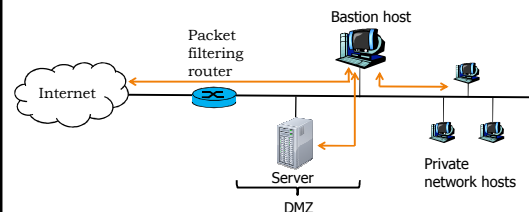
- ▶ Simple packet filtering router



17

Firewall Deployment Topologies

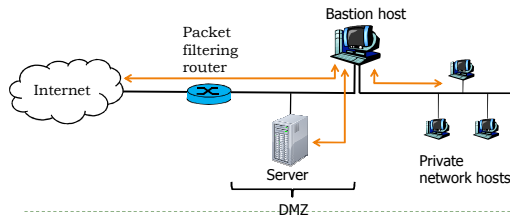
- ▶ Screened host firewall system – single-homed bastion host
 - ▶ Consists of two nodes – packet filtering router and bastion host
 - ▶ Bastion host performs authentication and proxy function
 - ▶ All traffic (internal/external) has to go thru bastion host
 - ▶ Server can be allowed to directly communicate w/ outside



18

Firewall Deployment Topologies

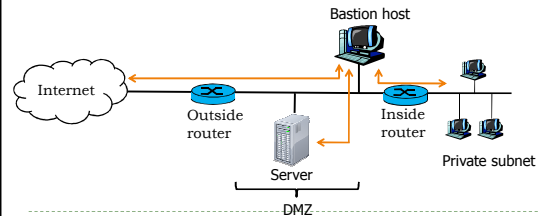
- ▶ Screened host firewall system – dual-homed bastion host
 - ▶ Consists of two nodes – packet filtering router and bastion host
 - ▶ Bastion host physically separates the private network from the public network



19

Firewall Deployment Topologies

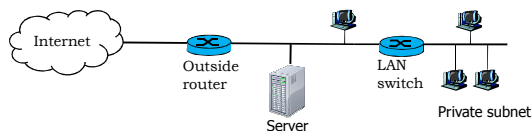
- ▶ Screened subnet firewall
 - ▶ Consists of three nodes – two packet filtering router and bastion host
 - ▶ Outside router only advertizes the screened subnet (not the private subnet) to outside world – private subnet is invisible



20

Firewall Deployment Topologies

- ▶ A bridge (layer 2 LAN switch) firewall case
 - ▶ Allows nw separation at layer 2 so that all the devices can be on the same subnet
 - ▶ Eliminates the need to create multiple subnets to separate private subnet from the screened subnet



21

Firewall platforms (hardware & software)

- ▶ Another classification of firewall types
 - ▶ Screening router firewalls
 - ▶ Computer-based firewalls
 - ▶ Firewall appliances
 - ▶ Host firewalls – on clients and servers

22

Firewall platforms (hardware & software)

- ▶ Screening router firewalls
 - ▶ Add firewall software on a router
 - ▶ Usually provides light filtering only
 - ▶ Expensive for the processing power – usually must upgrade hardware too
 - ▶ Screens out incoming noise of simple scanning attacks to make the detection of serious attacks easier
 - ▶ Good location for egress filtering – can eliminate scanning responses, even from the router

23

Firewall platforms (hardware & software)

- ▶ Computer-based firewalls
 - ▶ Add firewall software to a server running a general purpose OS – MS Windows or UNIX/LINUX
 - ▶ Can be purchased with power to handle any load
 - ▶ Easy to use due to familiarity with the OS
 - ▶ Vendor may bundle software w/ hardened hw/OS
 - ▶ General purpose OS results in slower processing
 - ▶ Security – can be a hacked in
 - ▶ Attacker can change filtering rules to allow attack packets in
 - ▶ Attacker can change filtering rules to filter legitimate traffic

24

Firewall platforms (hardware & software)

- ▶ Firewall appliances
 - ▶ Boxes with minimal OS – difficult to hack
 - ▶ Setup is minimal
 - ▶ Not customized to specific application scenario
 - ▶ Must be able to update for continual use/utility

25

Firewall platforms (hardware & software)

- ▶ Host firewalls
 - ▶ Installed on hosts – servers and/or clients
 - ▶ Enhanced security due to host-specific knowledge
 - ▶ Eg. Filter out everything but Web traffic to webserver
 - ▶ Defense in depth
 - ▶ Normally used in conjunction with other firewalls
 - ▶ Configuration may be difficult by ordinary users
 - ▶ May require maintenance by a specialist for effectiveness/consistence with security policy

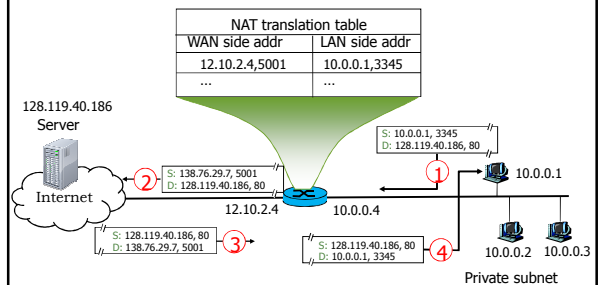
26

Additional Services

- ▶ Network Address Translation – NAT
 - ▶ A technology that allows one to use as few as one single IP address for hosts in a private network
 - ▶ Nodes in the private network are by default inaccessible from outside
 - ▶ Network translation helps local clients to communicate with external servers

27

NAT functionality



28

Split-Horizon DNS

- ▶ DNS – Domain Name Service
 - ▶ Provides hostname-to-IP address mapping
 - ▶ DNS info may be used by attackers to identify target machines within the internal network
 - ▶ Use two DNS servers
 - ▶ One to serve external queries – includes DNS info for publicly accessible servers only
 - ▶ Another to serve internal queries – may include DNS info for all systems including the ones in the private network

29

Mitigating host fingerprinting

- ▶ Fingerprinting – the task of inferring information about a system
 - ▶ Its OS, type of services and their particular implementation
 - ▶ Used to learn info about systems for attacking purposes
- ▶ Many packet filtering firewalls include a “scrub” function to normalize and defragment incoming packets to protect internal systems from leaking info about their configurations

30

Virtual Private Networks (VPNs)

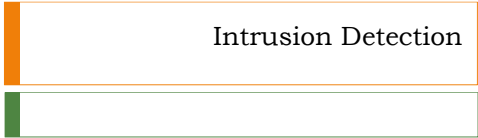
- ▶ Firewalls can support VPN functionality
- ▶ A VPN allows a remote user to be seen as local to the protected network via a secure tunnel ending at the firewall
- ▶ Used to allow remote connection to secured network and use services within the network
 - ▶ E.g., use VPNs to connect UTD network and download your e-mails to your local PC or to map your home directory to your PC while working at home
- ▶ VPNs typically use IPsec to secure communication between your PC and the firewall

31

Linux Firewalls

- ▶ Firewalls lab and related discussion

32



Intrusion Detection

33

(Slides by Lawrie Brown)

Intruders

- ▶ Significant issue hostile/unwanted trespass
 - ▶ From benign to serious
- ▶ User trespass
 - ▶ Unauthorized logon, privilege abuse
- ▶ Software trespass
 - ▶ Virus, worm, or trojan horse
- ▶ Classes of intruders:
 - ▶ Masquerader, misfeasor, clandestine user

Examples of Intrusion

- ▶ Remote root compromise
- ▶ Web server defacement
- ▶ Guessing / cracking passwords
- ▶ Copying viewing sensitive data / databases
- ▶ Running a packet sniffer
- ▶ Distributing pirated software
- ▶ Using an unsecured modem to access net
- ▶ Impersonating a user to reset password
- ▶ Using an unattended workstation

Security Intrusion & Detection

Security Intrusion

A security event, or combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

Intrusion Detection

A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

Hackers

- ▶ Motivated by thrill of access and status
 - ▶ Hacking community a strong meritocracy
 - ▶ Status is determined by level of competence
- ▶ Benign intruders might be tolerable
 - ▶ Do consume resources and may slow performance
 - ▶ Can't know in advance whether benign or malign
- ▶ IDS / IPS / VPNs can help counter
- ▶ Awareness led to establishment of CERTs
 - ▶ Collect/disseminate vulnerability info/responses

Hacker Behavior Example

1. Select target using IP lookup tools
2. Map network for accessible services
3. Identify potentially vulnerable services
4. Brute force (guess) passwords
5. Install remote administration tool
6. Wait for admin to log on and capture password
7. Use password to access remainder of network

Insider Attacks

- ▶ Among most difficult to detect and prevent
- ▶ Employees have access & systems knowledge
- ▶ May be motivated by revenge / entitlement
 - ▶ When employment terminated
 - ▶ Taking customer data when move to competitor
- ▶ IDS / IPS may help but also need:
 - ▶ Least privilege, monitor logs, strong authentication, termination process to block access & mirror data

Intrusion Techniques

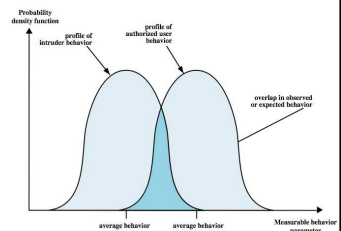
- ▶ Objective to gain access or increase privileges
- ▶ Initial attacks often exploit system or software vulnerabilities to execute code to get backdoor
 - ▶ E.g. buffer overflow
- ▶ Or to gain protected information
 - ▶ E.g. password guessing or acquisition

Intrusion Detection Systems

- ▶ Classify intrusion detection systems (IDSs) as:
 - ▶ **Host-based IDS**: monitor single host activity
 - ▶ **Network-based IDS**: monitor network traffic
- ▶ Logical components:
 - ▶ **Sensors** - collect data
 - ▶ **Analyzers** - determine if intrusion has occurred
 - ▶ **User interface** - manage / direct / view IDS

IDS Principles

- ▶ Assume intruder behavior differs from legitimate users
- ▶ Expect overlap as shown
- ▶ Observe deviations from past history
- ▶ Problems of:
 - ▶ False positives
 - ▶ False negatives
 - ▶ Must compromise



IDS Requirements

- ▶ Run continually
- ▶ Be fault tolerant
- ▶ Resist subversion
- ▶ Impose a minimal overhead on system
- ▶ Configured according to system security policies
- ▶ Adapt to changes in systems and users
- ▶ Scale to monitor large numbers of systems
- ▶ Provide graceful degradation of service
- ▶ Allow dynamic reconfiguration

Host-Based IDS

- ▶ Specialized software to monitor system activity to detect suspicious behavior
 - ▶ Primary purpose is to detect intrusions, log suspicious events, and send alerts
 - ▶ Can detect both external and internal intrusions
- ▶ Two approaches, often used in combination:
 - ▶ Anomaly detection - defines normal/expected behavior
 - ▶ Threshold detection
 - ▶ Profile based
 - ▶ Signature detection - defines proper behavior

Audit Records

- ▶ A fundamental tool for intrusion detection
- ▶ Two variants:
 - ▶ Native audit records - provided by O/S
 - ▶ Always available but may not be optimum
 - ▶ Detection-specific audit records - IDS specific
 - ▶ Additional overhead but specific to IDS task
 - ▶ Often log individual elementary actions
 - ▶ E.g. may contain fields for: subject, action, object, exception-condition, resource-usage, time-stamp

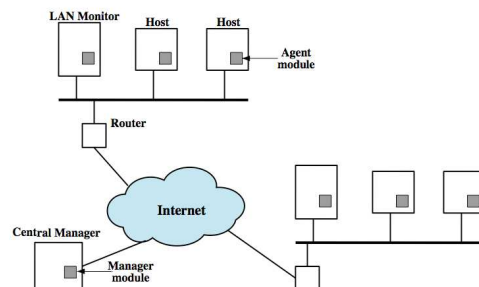
Anomaly Detection

- ▶ Threshold detection
 - ▶ Checks excessive event occurrences over time
 - ▶ Alone a crude and ineffective intruder detector
 - ▶ Must determine both thresholds and time intervals
- ▶ Profile based
 - ▶ Characterize past behavior of users / groups
 - ▶ Then detect significant deviations
 - ▶ Based on analysis of audit records
 - ▶ Gather metrics: counter, gauge, interval timer, resource utilization
 - ▶ Analyze: mean and standard deviation, multivariate, Markov process, time series, operational model

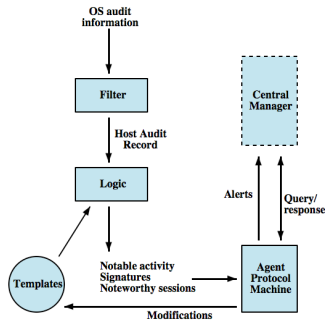
Signature Detection

- ▶ Observe events on system and applying a set of rules to decide if intruder
- ▶ Approaches:
 - ▶ Rule-based anomaly detection
 - ▶ Analyze historical audit records for expected behavior, then match with current behavior
 - ▶ Rule-based penetration identification
 - ▶ Rules identify known penetrations / weaknesses
 - ▶ Often by analyzing attack scripts from Internet
 - ▶ Supplemented with rules from security experts

Distributed Host-Based IDS



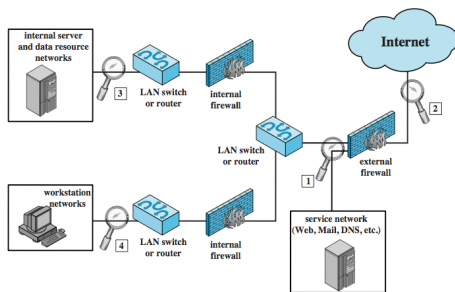
Distributed Host-Based IDS



Network-Based IDS

- ▶ Network-based IDS (NIDS)
 - ▶ Monitor traffic at selected points on a network
 - ▶ In (near) real time to detect intrusion patterns
 - ▶ May examine network, transport and/or application level protocol activity directed toward systems
- ▶ Comprises a number of sensors
 - ▶ Inline (possibly as part of other net device)
 - ▶ Passive (monitors copy of traffic)

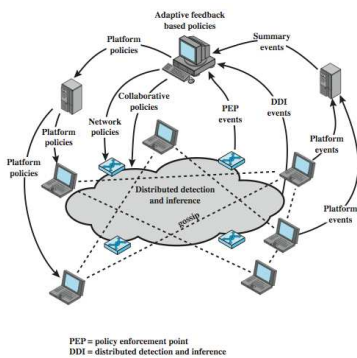
NIDS Sensor Deployment



Intrusion Detection Techniques

- ▶ Signature detection
 - ▶ At application, transport, network layers; unexpected application services, policy violations
- ▶ Anomaly detection
 - ▶ Of denial of service attacks, scanning, worms
- ▶ When potential violation detected sensor sends an alert and logs information
 - ▶ Used by analysis module to refine intrusion detection parameters and algorithms
 - ▶ By security admin to improve protection

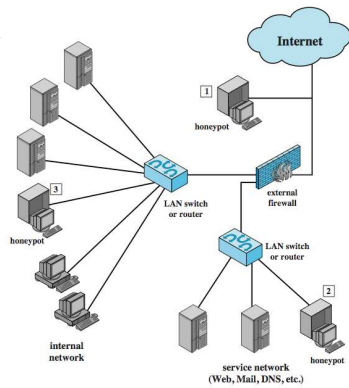
Distributed Adaptive Intrusion Detection



Honeypots

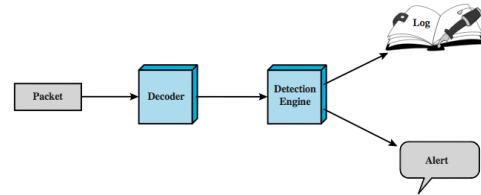
- ▶ Are decoy systems
 - ▶ Filled with fabricated info
 - ▶ Instrumented with monitors / event loggers
 - ▶ Divert and hold attacker to collect activity info
 - ▶ Without exposing production systems
- ▶ Initially were single systems
- ▶ More recently are/emulate entire networks

Honeypot Deployment



SNORT

- ▶ Lightweight IDS
 - ▶ Real-time packet capture and rule analysis
 - ▶ Passive or inline



SNORT Rules

- ▶ Use a simple, flexible rule definition language
- ▶ With fixed header and zero or more options
- ▶ Header includes: action, protocol, source IP, source port, direction, dest IP, dest port
- ▶ Many options
- ▶ Example rule to detect TCP SYN-FIN attack:

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET any \  
(msg: "SCAN SYN FIN"; flags: SF, 12; \  
reference: arachnids, 198; classtype: attempted-recon;)
```