Intrusion Detection and Prevention

Defining Intrusion

The intrusion can be defined as an unauthorized entry into the networked system. Such unauthorized entries are normally malicious and involve a breach of supposed security mechanism of the system. Such unauthorized access is gained generally by exploiting a known system vulnerability or predictable system user behavior observed by the intruder. As a result, an effective detection mechanism for such activities involves extensive behavior analysis and anomaly detection in the system activity.

Intruders

System intruders can be categorized broadly into the following three categories:

1. **Masquerader**: It is an unauthorized user, generally external, that exploits a system weakness to access the system through the account of a legitimate system user.
2. **Misfeasor**: It is a legitimate and generally internal system user that abuses his/her system privileges to access those system functions or data that are not covered by his/her access privileges.
3. **Clandestine user**: A person who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection so that his/her activities are not traceable and difficult to investigate. Such can be both internal and external user.

**Stages of Intrusion**

An unlawful and unauthorized access to a networked system is obtained after a generally predictable sequence of events and activities. The major stages are as follows:

1. First stage is to scan the network to:
   * locate which IP addresses are in use, (e.g. nmap in linux)
   * what operating system is in use,
   * what TCP or UDP ports are “open” (being listened to by Servers).

This stage gives vital information regarding the network and system status for the attacker. Based on the information thus collected, the attacker can plan which service or system is more vulnerable and has exploitable weaknesses. The weak system or service thus identified is used as a gateway to enter the system or network.

The following is a sample output of ‘nmap’ system command in linux that tells about the remote machines and services/ports open on them:

# nmap w.x.y.z

Starting Nmap 5.00 ( http://nmap.org ) at 2012-12-31 15:17 NPT

Interesting ports on server.domain.com (w.x.y.z):

Not shown: 993 filtered ports

PORT STATE SERVICE

25/tcp open smtp

110/tcp open pop3

143/tcp open imap

443/tcp open https

465/tcp open smtps

993/tcp open imaps

995/tcp open pop3s

Nmap done: 1 IP address (1 host up) scanned in 5.21 seconds

1. Run “Exploit” scripts against open ports which are identified in the scanning stage.
2. Get access to Shell program which is “suid” (has “root” privileges). Normally, almost all systems are operated by administrators using the system’s shell interface. So, best way for the attacker to have shell access with desired privilege to start actual damage to the system.
3. Download from Hacker Web site special versions of systems files that will let Cracker have free access in the future without his cpu time or disk storage space being noticed by auditing programs. This is a stage of grooming or preparing the system for further unlawful access but without having to go through the same hassle as in the case of first access.
4. Use IRC (Internet Relay Chat) to invite friends to the feast. This is not the case of every case of intrusion. But for scenarios such as DoS, DDoS and Botnets, the compromised machine is used by the gang of exploiters as a common platform for further attacks to other systems.

Intrusion Detection

Intrusion detection helps to mitigate damage of the current intrusion as well as discourage similar activity in future if such detection can be followed by appropriate legal or administrative action against the identified intruders.

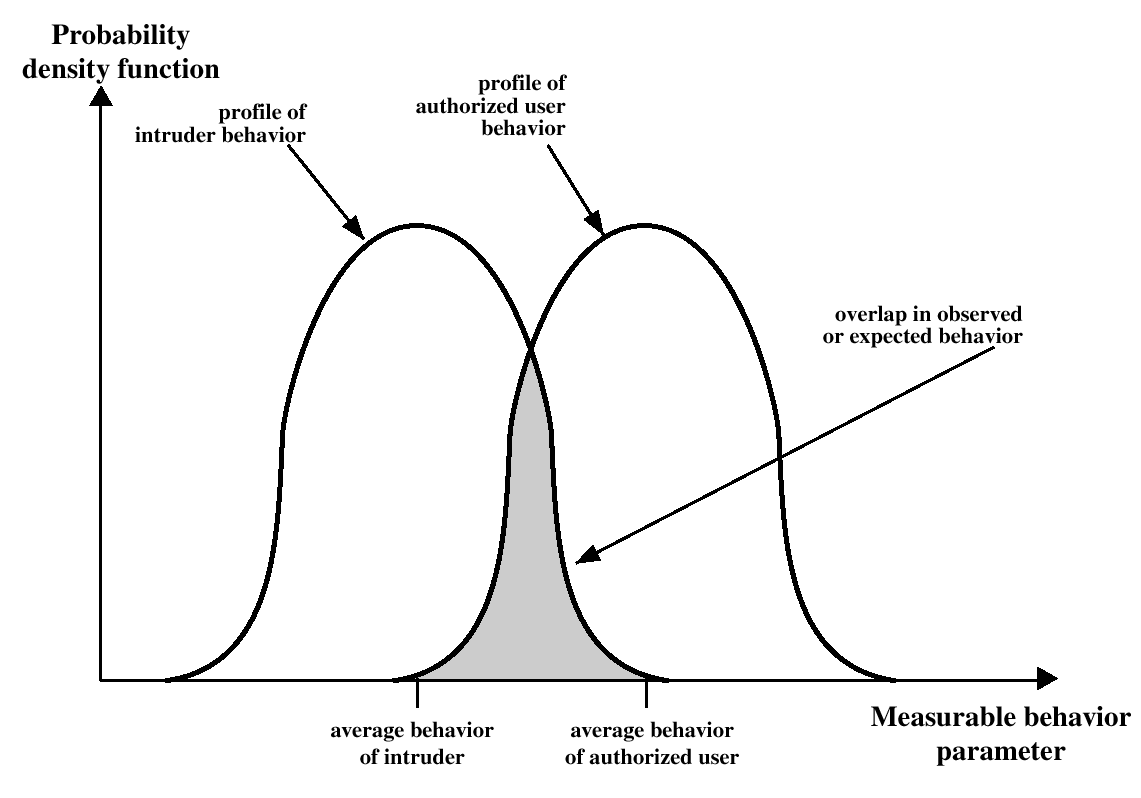
The major approaches of intrusion detection are:

1. Statistical anomaly detection where predictable profiles of legitimate users are prepared by studying their behaviour for a period of time. Then, these profiles are used as the datum for comparing any anamolous behaviour amounting to intrusion. Such anomalies can be detected mainly by:
   * Treshold detection: the activity parameters or statistics exceeding a certain threshold.
   * Profile based: to identify the changes in behaviour of users based on their past activities and current activities.
2. Rule based detection where a set of rules are defined which can be used to decide that a particular behaviour is that of an intruder. Such identification can be done by:
   * Anomaly detection: identification for the anomalous activity in the system.
   * Penetration identification: an intelligent mechanism that keeps on looking for suspicious behaviour in the system.

Measurable Behavior Parameters and Profile of Normal and Intrusion Activities

The common system related parameters that are measured and monitored to identify possible intrusion are enlisted below:

* Login frequency by day and time.
* Frequency of login at different locations.
* Time since last login.
* Password failures at login.
* Execution frequency.
* Execution denials.
* Read, write, create, delete frequency.
* Failure count for read, write, create and delete.

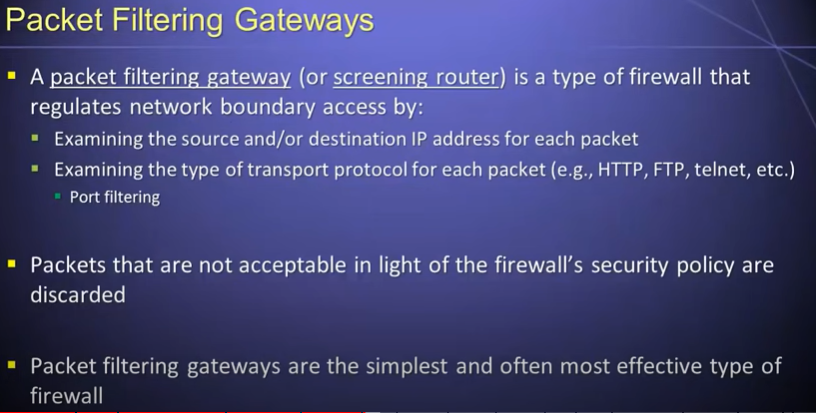
Measurable differences in the normal and abnormal values of these parameters are used as important indicators of system intrusion or similar unwanted activity. The figure 5.5.5.1 shows a graphical view of such differences. Properly defined normal behavior indicators and anomaly thresholds can help better identify anomalous behavior and hence timely detection of intrusion.

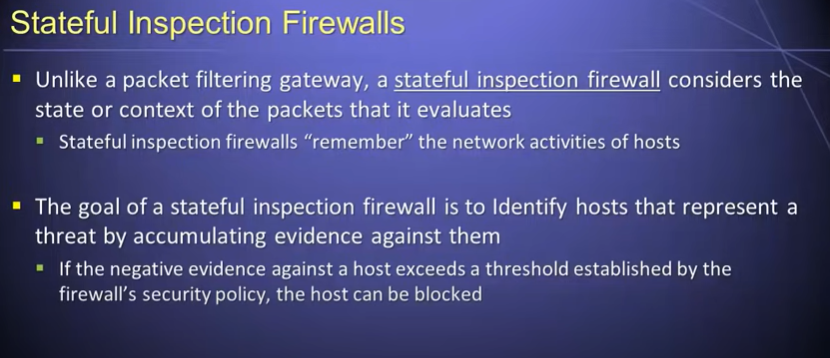
*Figure 5.5.5.1: Differences in normal and anomalous behavior*

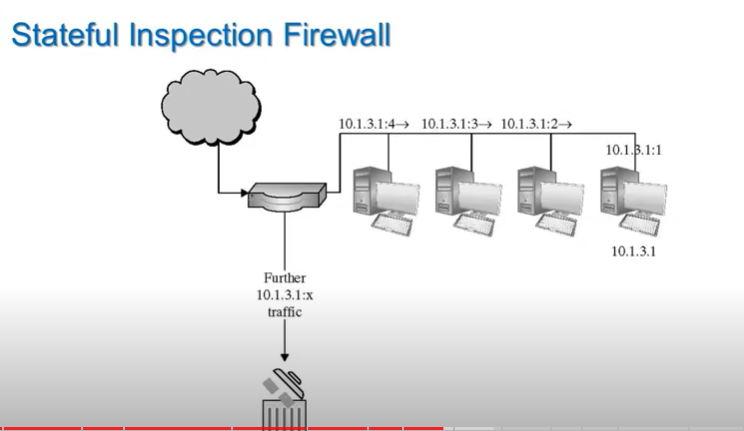
Intrusion Prevention

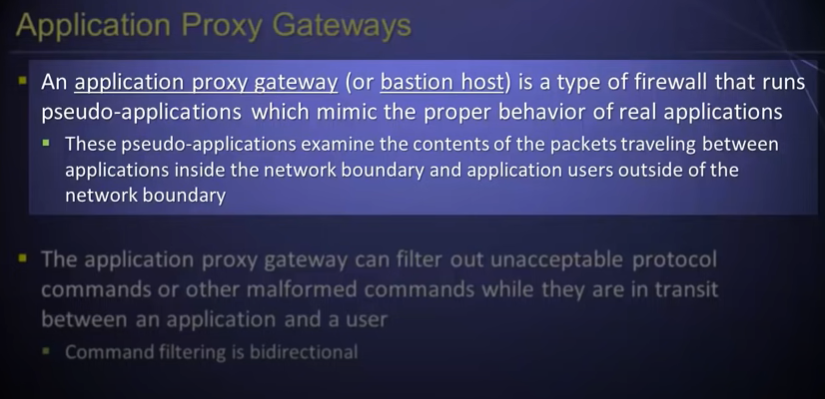
Intrusion prevention needs an integrated approach of system hardening and proper detection and investigation mechanisms. Some of the useful steps for intrusion prevention are:

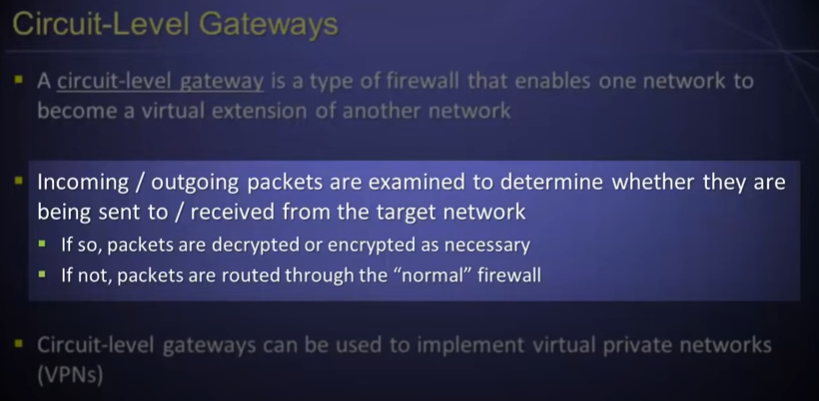
1. Hardening of the systems and their services by using proper configurations.
2. Hardening of system accounts and passwords. Make passwords difficult to guess and maintain practice of routinely changing critical passwords.
3. Have a well-defined intrusion detection guideline based on the major measurable behavior parameters outlined earlier.
4. Regular monitoring and audit of the system, its services, logs, user activity etc.

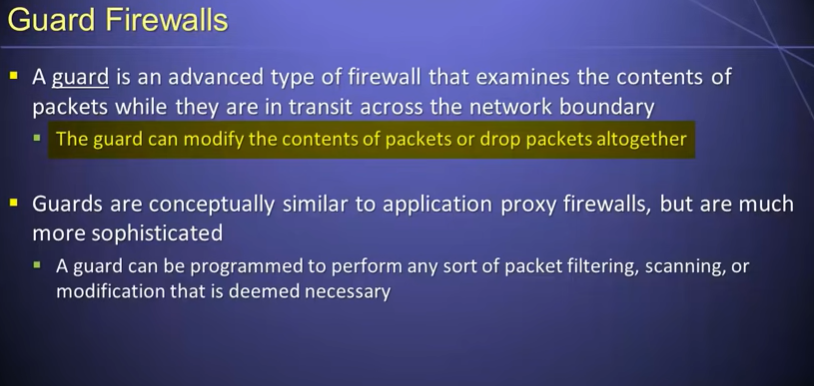


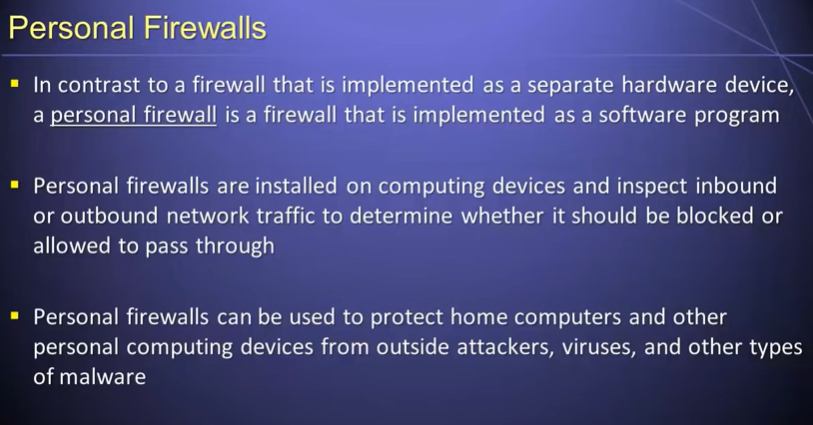








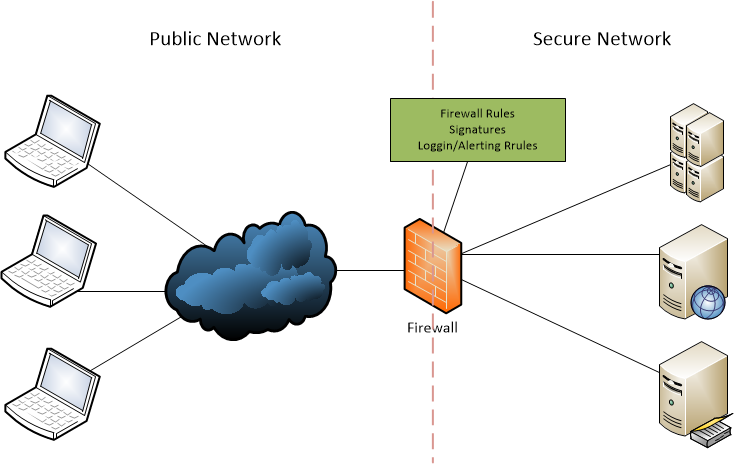




Firewalls

Firewalls are advanced network protection mechanism that can be taken as complicated packet filtering rules at the IP packet layer or at higher layers also. It combines such filtering rules with stateful inspection, reporting, alerting and rule-engine functionalities.

Firewalls are generally used to secure critical network or system resources from unwanted access or attack. Figure illustrates a typical deployment of firewall.



*Figure A typical deployment of a firewall*

As depicted in the figure a firewall isolates the protected/private network from public network with each packet going into or out of the protected network subject to the firewall rules or policy. Firewall decides to allow or deny such packets based on those policies.

### 5.4.1 Multi-dimensional control

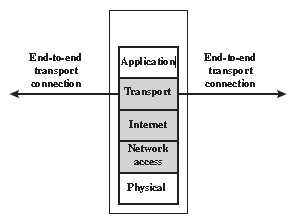
A good firewall system provides control of network access in several dimensions. These are:

1. Service control: defines the types of services that can be accessed both inbound and outbound. Includes packet filter rules based on addresses, ports etc, and other roles such as application gateway, proxies etc.
2. Direction control: can decide to control packets at the ingress, egress or both.
3. User control: defines rules for user access. It is normally used for users inside the secure network. However, in VPN scenarios, it can involve users outside the protected network as well.
4. Behavior control: defines more complicated activities such as redirection of services, allowing some services while blocking others, allowing access to only part of a service or network etc.

Types of Firewall

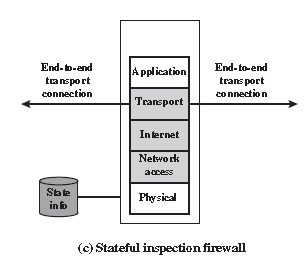
The major types of firewall are:

1. **Packet filtering firewall**: define allow/disallow rules for packets based on the specific content of each packet such as addresses, ports (protocols), interfaces etc. The rules and functional architecture are similar to that of the packet filter lists or access lists. Figure 5.4.2.1 shows the schematic of the packet filtering firewall.



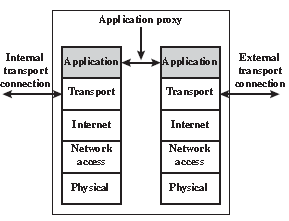
*Figure 5.4.2.1: Packet filtering firewall*

**Stateful inspection firewall**: simple packet filtering firewall decides to allow/block a packet entirely based on the content of that same packet. It does not look at the context of that packet. However, a stateful mechanism can keep track of connections, data sessions and other parameters and uses them to decide on each packet. It can keep track of individual TCP sessions and even their sequence numbers to be able to make packet decisions based more on the previous record, overall behavior and context rather than the content of individual packet only. Figure 5.4.2.2 shows schematic of stateful inspection firewall.



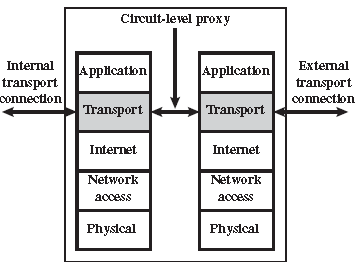
*Figure 5.4.2.2: Stateful inspection firewall*

**Application level gateway**: an application level gateway or application proxy can be used to hide the real application server and forward the packets between the clients and the real server. The clients access certain predefined port or service of the application gateway and based on the authentication parameters and credentials of the client, the relay is done to the real application server. Such application proxy allows end to end connection between client and server by transparently relaying the packets from client to server and vice versa. Such gateway can control which applications are allowed to pass through and which are not. Figure 5.4.2.3 shows the scheme of the application proxy.



*Figure 5.4.2.3: Application proxy (gateway)*

**Circuit level gateway**: this is special kind of application gateway where only one specific type of application is relayed. Moreover, there is no end-to-end direct connection between the client and server. The gateway establishes separate connection with client and servers and relays the application requests and response between the two. Figure 5.4.2.4 shows schematic of the circuit level gateway firewall.

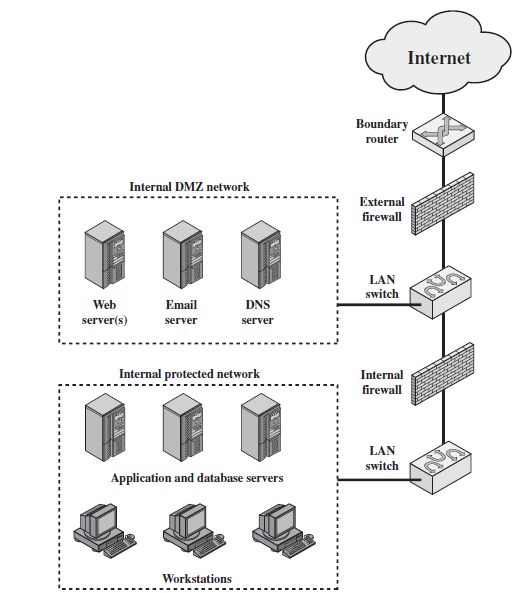


*Figure 5.4.2.4: Circuit level gateway*

Positioning of the Firewalls

Positioning and the number of firewalls to be deployed in a network depends upon the type of the network, level of risk and level of protection being desired. The major types of firewall positioning are as follows:

1. **DMZ Networks:** multiple layers of firewall are used for protecting high-risk systems such as enterprise servers, customer databases etc and the publicly accessible systems such as web, DNS servers. The mid-security region where the publicly accessible systems such as web and DNS are located have moderate security ensured by external layers of firewalls. Such moderate-security region is called de-militarized zone (DMZ). There is an internal layer of high-security firewalls between the DMZ and the internal servers. Fig. 5.4.3.1.

****

*Fig. DMZ Firewall Scenario*