

**包过滤防火墙**（作用在网络层和传输层）

包过滤（Packet Filtering）作用在网络层和传输层，根据数据包的包头信息（源和目的IP地址、端口号、标志位等），依据事先设定的过滤规则，决定是否允许数据包通过。包过滤防火墙相当于一个具有包过滤功能的路由器

**包过滤技术的优点：**

用一个放置在重要位置上的包过滤路由器即可保护整个网络，这样，不管内部网的站点规模多大，只要在路由器上设置合适的包过滤，各站点均可获得良好的安全保护；

包过滤工作对用户来说是透明的。包过滤不需用户软件支持，也不要对客户机做特殊设置；

包过滤技术是一种有效而通用的控制网络流量的方法，经常作为不可信网络的第一层防卫；可以有效阻塞公开的恶意站点的信息流。

**包过滤技术的缺点：**

仅依赖网络层和传输层信息，如IP地址、端口号、TCP标志等，只能“就事论事”地进行安全判决。由于缺少信息，一些协议如RPC、UDP难以有效过滤；

支持规则的数量有限，规则过多会降低效率。

正确制定规则并不容易

（1）通常不能对付某些类型的拒绝服务攻击——基于包损坏、SYN Flood或其他基于TCP/IP的异常。

（2）静态包过滤防火墙不能跟踪会话的状态数据。管理员被迫保持所有1024以上的端口。

（3）支持极繁忙网络的包过滤防火墙会引起网络性能降级和更高的CPU负载。

**状态检测防火墙**（网络层防火墙）

状态检测又称动态包过滤，在网络层由一个检查引擎截获数据包，抽取出与应用层状态有关的信息，并以此作为依据决定对该数据包是接受还是拒绝。

检查引擎维护一个动态的状态信息表并对后续的数据包进行检查。一旦发现任何连接的参数有意外变化，该连接就被中止

它在协议底层截取数据包，然后分析这些数据包，并且将当前数据包和状态信息与前一时刻的数据包和状态信息进行比较，从而得到该数据包的控制信息，来达到保护网络安全的目的

优点

状态检测防火墙克服了包过滤防火墙的局限性，能够根据协议、端口及源地址、目的地址的具体情况决定数据包是否可以通过。

对于每个安全策略允许的请求，状态检测防火墙启动相应的进程，可以快速地确认符合授权标准的数据包，这使得本身的运行速度很快。

跟踪通过防火墙的网络连接和包，这样它就可以使用一组附加的标准，以确定是否允许和拒绝通信。

**举例：状态检测防火墙适合过滤SYN+ACK扫描包**

缺点

状态检测防火墙的安全特性是最好的，但其配置非常复杂，会降低网络效率。

**应用网关防火墙**(协议栈到应用层，起到代理服务器作用)

应用代理（应用网关）是代理内部网络用户与外部网络服务器进行信息交换的程序。它将内部用户的请求确认后送达外部服务器，同时将外部服务器的响应再回送给用户。

代理服务是运行在防火墙主机上的特定的应用程序或服务程序。防火墙主机可以是具有一个内部网接口和一个外部网接口的双穴(Dual Homed)主机，也可以是一些可以访问Internet并可被内部主机访问的堡垒主机。（将在体系结构一节中讲解）

优点

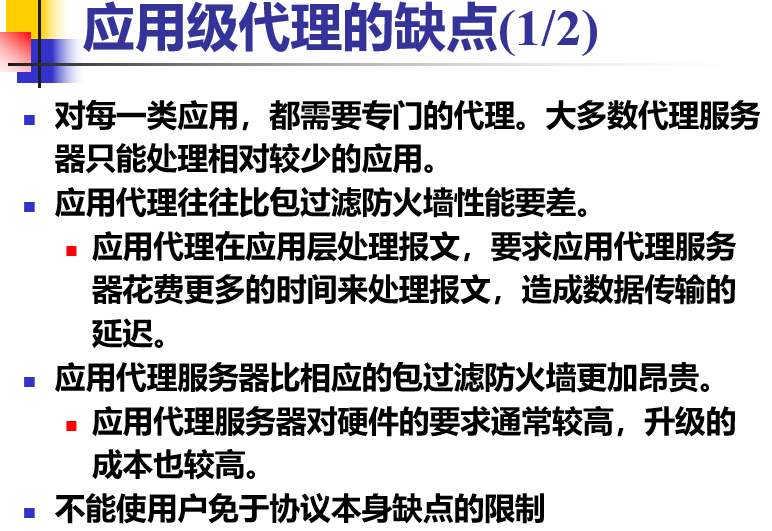
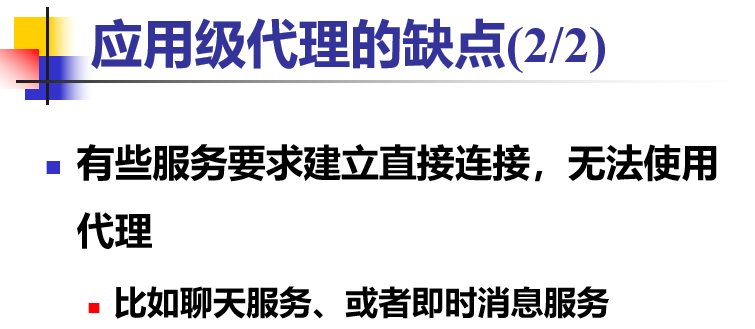
由于代理直接和应用程序交互，它可以根据应用上下文进行决策和判定，而不仅仅依据IP地址和端口号。可以做出更为准确的判定。

以HTTP流量为例：

包过滤技术仅仅知道应该允许或者拒绝HTTP流量；

应用级代理可以配置来过滤具体HTTP流量类型的数据；

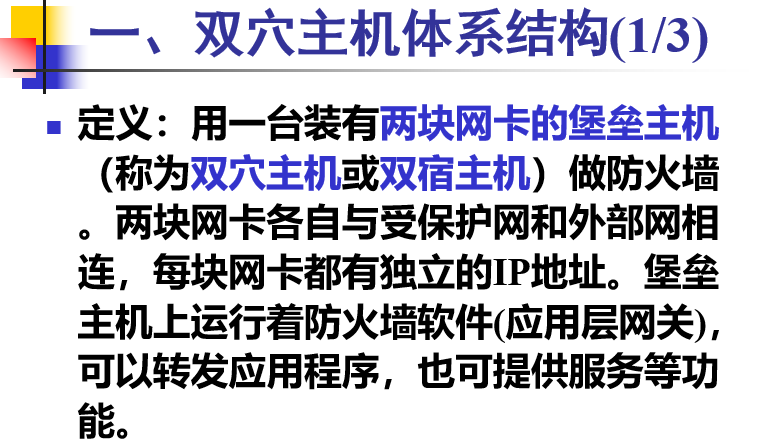
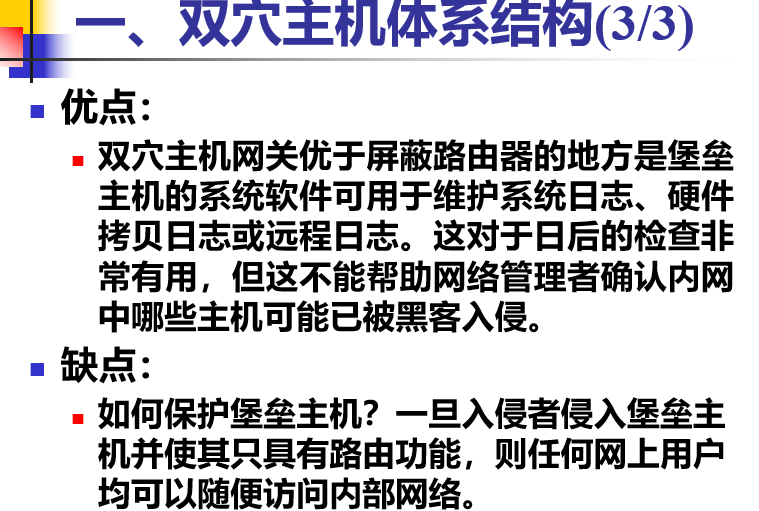
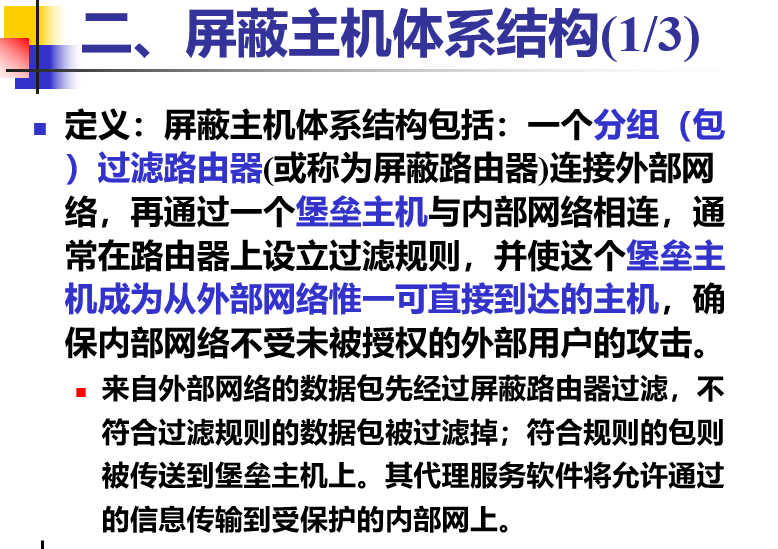
防火墙管理员的管理带来极大的伸缩性，可以严格控制什么流量将会被允许，什么流量将被拒绝。

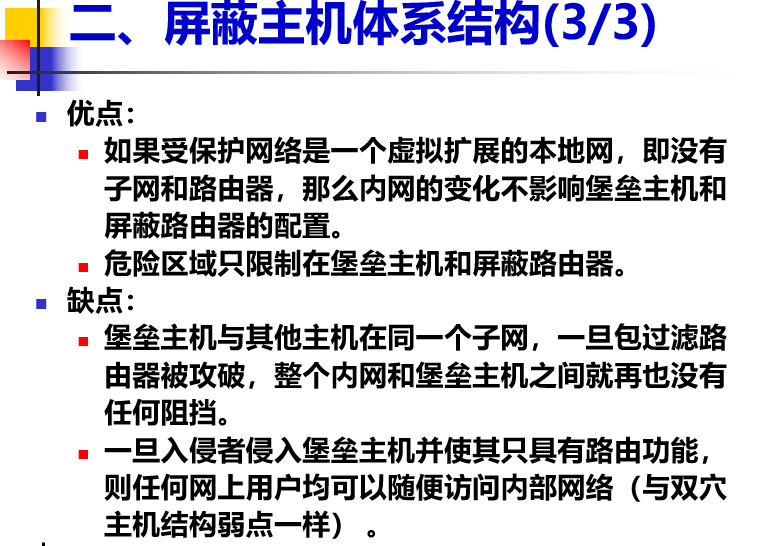


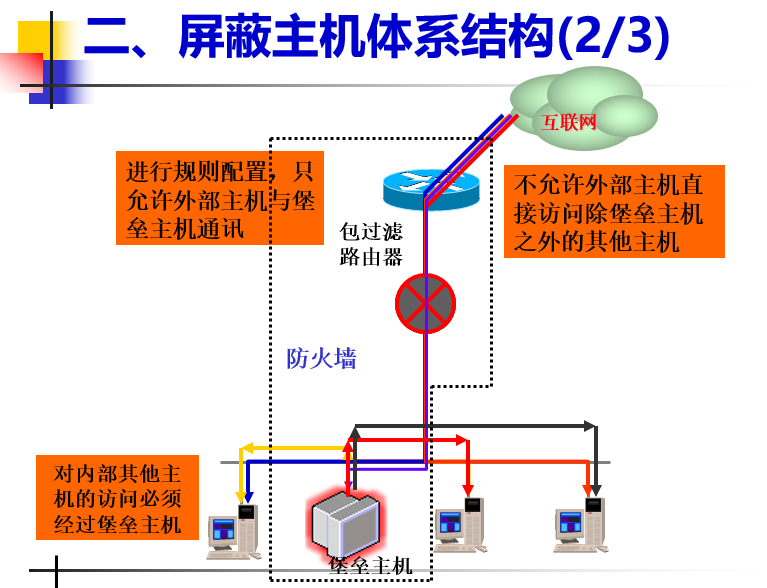
**防火墙体系结构一般有三种：**

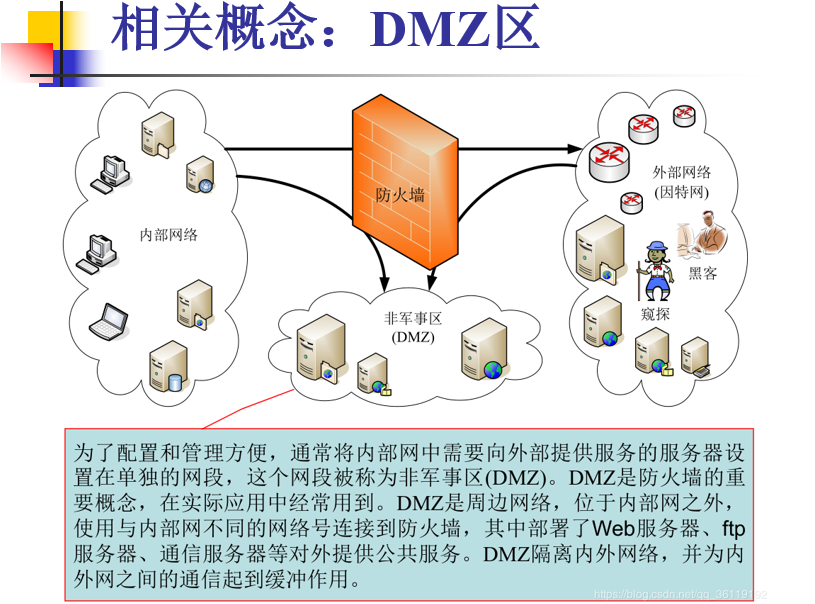
* + **双穴主机或双宿主机结构 (Dual Homed Gateway)**
  + **屏蔽主机或主机过滤结构(Screened Host Gateway)**
  + **过滤子网或屏蔽子网结构(Screened Subnet)**

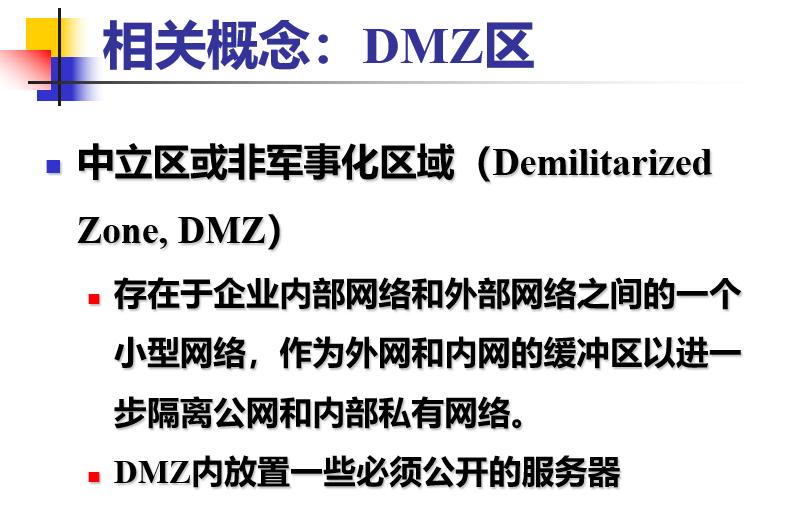
堡垒主机定义见书218。一般作为应用网关或代理服务











在外界网络和内部网络之间建立一个双方都可以访问的独立网络（过滤子网），用两台分组过滤（包过滤）路由器将这一子网分别与内部网络和外部网络分开：

过滤子网也常常被称为DMZ（Demilitarized Zone）区或参数网络或周边网络或屏蔽网络，它可以只包含堡垒主机，也可以增加需要对外提供服务的Web服务器。

过滤子网不提供外部网络和内部网络之间的通路。它是在内/外部网之间另加的一个安全保护层，相当于一个应用网关。如果入侵者成功地闯过外层保护网到达防火墙，参数网络就能在入侵者与内部网之间再提供一层保护。

如果入侵者仅仅侵入到过滤子网中的的堡垒主机，他只能偷看到过滤子网的信息流而看不到内部网的信息，过滤子网的信息流仅往来于外部网到堡垒主机。没有内部网主机间的信息流(重要和敏感的信息)在过滤子网中流动，所以堡垒主机受到损害也不会破坏内部网的信息流

**增加了一个隔离内部网络与Internet的周边网络（DMZ），DMZ中的堡垒主机运行可向Internet开放的各种网络应用（如Web、SMTP、FTP、外部DNS服务）。**

* **堡垒主机**
  + **在过滤子网结构中，堡垒主机与过滤子网相连，而该主机是外部网服务于内部网的主节点。**
  + **在内、外部路由器上建立包过滤，以便内部网的用户可直接操作外部服务器；**
  + **在主机上建立代理服务，在内部网用户与外部服务器之间建立间接的连接，例如：**
    - **接收外来电子邮件并分发给相应站点；**
    - **接收外来FTP并连到内部网的匿名FTP服务器；**
    - **接收外来的有关内部网站点的域名服务。**
* **内部屏蔽路由器**
  + **主要功能是保护内部网免受来自外部网与过滤子网的攻击。**
  + **可以使过滤子网上的堡垒主机与内部网之间传递的各种服务和内部网与外部网之间传递的各种服务不完全相同。**
  + **完成防火墙的大部分包过滤工作，它允许某些站点的包过滤系统认为符合安全规则的服务在内/外部网之间互传。**
* **外部屏蔽路由器**
  + **既可保护过滤子网又保护内部网。实际上，在外部屏蔽路由器上仅做一小部分包过滤，它几乎让所有过滤子网的外向请求通过。与内部路由器的包过滤规则基本相同。**
  + **主要任务是阻隔来自外部网上伪造源地址进来的任何数据包。这些数据包自称来自内部网，其实它是来自外部网**

**防火墙部署方式**

* 透明模式
  + 也称为“桥接模式”或“透明桥接模式”。当防火墙处于“透明”模式时，防火墙只过滤通过的数据包，但不会修改数据包包头中的任何信息，其作用更像是处于同一VLAN的二层交换机或者桥接器，防火墙对于用户来说是透明的
  + 透明模式适用于原网络中已部署好路由器和交换机，用户不希望更改原有的网络配置，只需要一个防火墙进行安全防护的场景。
  + 一般情况下，透明模式的防火墙部署在原有网络的路由器和交换机之间，或者部署在互联网和路由器之间，内网通过原有的路由器上网，防火墙只做安全控制用。
* 网关模式
  + 也称为“路由模式”。防火墙所有网络接口都处于不同的子网中，不仅要过滤通过的数据包，还需根据数据包中的IP地址执行路由功能。防火墙在不同安全区（可信区/不可信区/DMZ区）间转发数据包时，一般不会改变IP包头中的源地址和端口号（除非明确采用了NAT）
  + 网关模式适用于内外网不在同一网段的情况，防火墙一般部署在内网，设置网关地址实现路由器的功能，为不同网段进行路由转发。网关模式相比透明模式具备更高的安全性，在进行访问控制的同时实现了安全隔离，具备了一定的机密性。
* NAT模式
  + 不仅对通过的数据包进行安全检查，还需执行网络地址转换（Network Address Translation）功能：使用防火墙的IP地址替换内部网络的源地址向外部网络发送数据；当外部网络的响应数据流量返回到防火墙后，防火墙再将目的地址替换为内部网络的源地址。
  + NAT模式使用地址转换功能可确保外部网络不能直接看到内部网络的IP地址，进一步增强了对内部网络的安全防护。同时，也解决了IP地址数量不足的问题。
  + 与透明模式和网关模式相比，NAT模式可以适用于所有网络环境，为被保护网络提供的安全保障能力也最强。

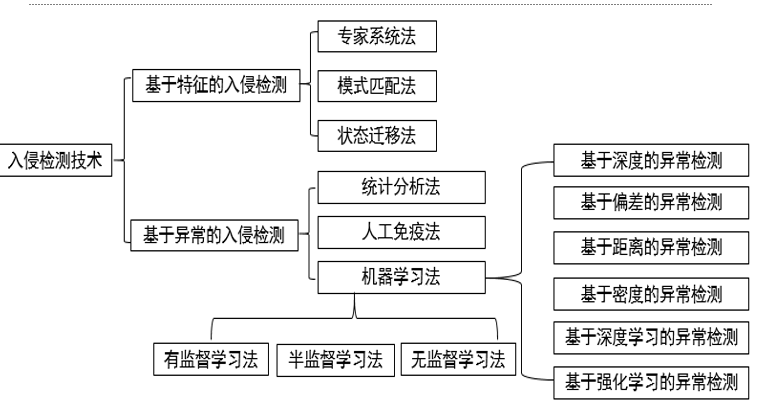
堡垒主机，是否就是应用网关防火墙？

堡垒主机是一个硬件，软件主要配置的是应用网关代理协议，作为内部网络外部唯一可以访问的点，中继网络流量（非转发）。

过滤路由器在网络层，堡垒主机主要在应用层。

**入侵检测分类**

* 根据检测方法来分：
  + 基于特征的入侵检测
  + 基于异常的入侵检测
  + 混合的入侵检测
* 根据数据源来分：
  + 基于应用的入侵检测系统(Application-based IDS, AIDS)
  + 基于主机的入侵检测系统(Host-based IDS, HIDS)
  + 基于网络的入侵检测系统(Network-based IDS, NIDS)
  + 混合的入侵检测系统(Hybrid IDS)



一、特征检测

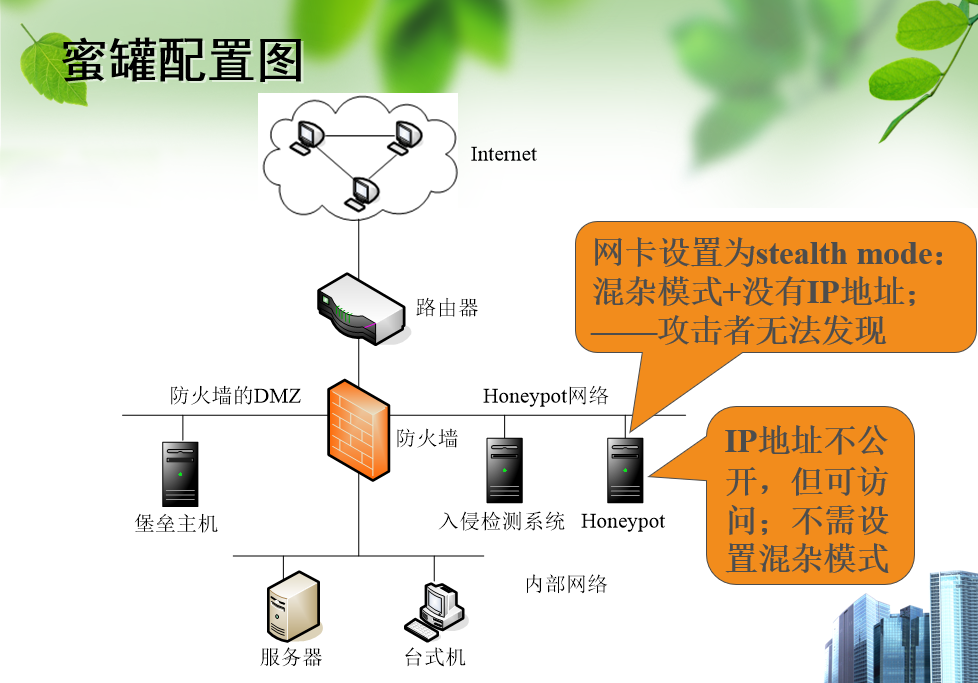
* 1. 模式匹配法
  + 将收集到的入侵特征转换成模式，存放在模式数据库中。检测过程中将收集到的数据信息与模式数据库进行匹配，从而发现攻击行为。
  + 模式匹配的具体实现手段多种多样，可以是通过字符串匹配寻找特定的指令数据，也可以是采用正规的数学表达式描述数据负载内容。技术成熟，检测的准确率和效率都很高
* 2. 专家系统法
  + 入侵活动被编码成专家系统的规则：“If 条件 Then 动作”的形式。入侵检测系统根据收集到的数据，通过条件匹配判断是否出现了入侵并采取相应动作
  + 实现上较为简单，其缺点主要是处理速度比较慢，原因在于专家系统采用的是说明性的表达方式，要求用解释系统来实现，而解释器比编译器的处理速度慢。另外，维护规则库也需要大量的人力精力，由于规则之间具有联系性，更改任何一个规则都要考虑对其他规则的影响。
* 3. 状态迁移法
  + 利用状态转换图描述并检测已知的入侵模式。入侵检测系统保存入侵相关的状态转换图表，并对系统的状态信息进行监控，当用户动作驱动系统状态向入侵状态迁移时触发入侵警告。
  + 状态迁移法能够检测出多方协同的慢速攻击，但是如果攻击场景复杂的话，要精确描述系统状态非常困难。因此，状态迁移法通常与其他的入侵检测法结合使用。

二、异常检测

* **该技术首先假设网络攻击行为是不常见的或是异常的，区别于所有正常行为。**
* **入侵行为偏离了正常的行为轨迹，就可以被检测出来。**
  + 若发现有用户在晚八点到早六点之间（如凌晨一点）登录公司服务器，则把该行为标识为异常行为。

HIDS和NIDS

* **按照信息源的来源**
  + 基于主机的IDS(Host-based Intrusion Detection System, HIDS)：通过监视和分析所在主机的审计记录检测入侵。
  + 基于网络的IDS(Network-based Intrusion Detection System, NIDS)：通过在共享网段上对主机之间的通信数据进行侦听，分析可疑现象。



**1）将蜜罐与任何真实产品系统隔离，一般将它放在离Internet最近的位置（如DMZ上）。**

**2）蜜罐不公开自己的IP地址和端口，对蜜罐的所有访问都可能是攻击。**

**3）蜜罐所捕获数据的针对性强，所以在一定程序上克服IDS的不足：误报率高及漏报新的攻击。**

