
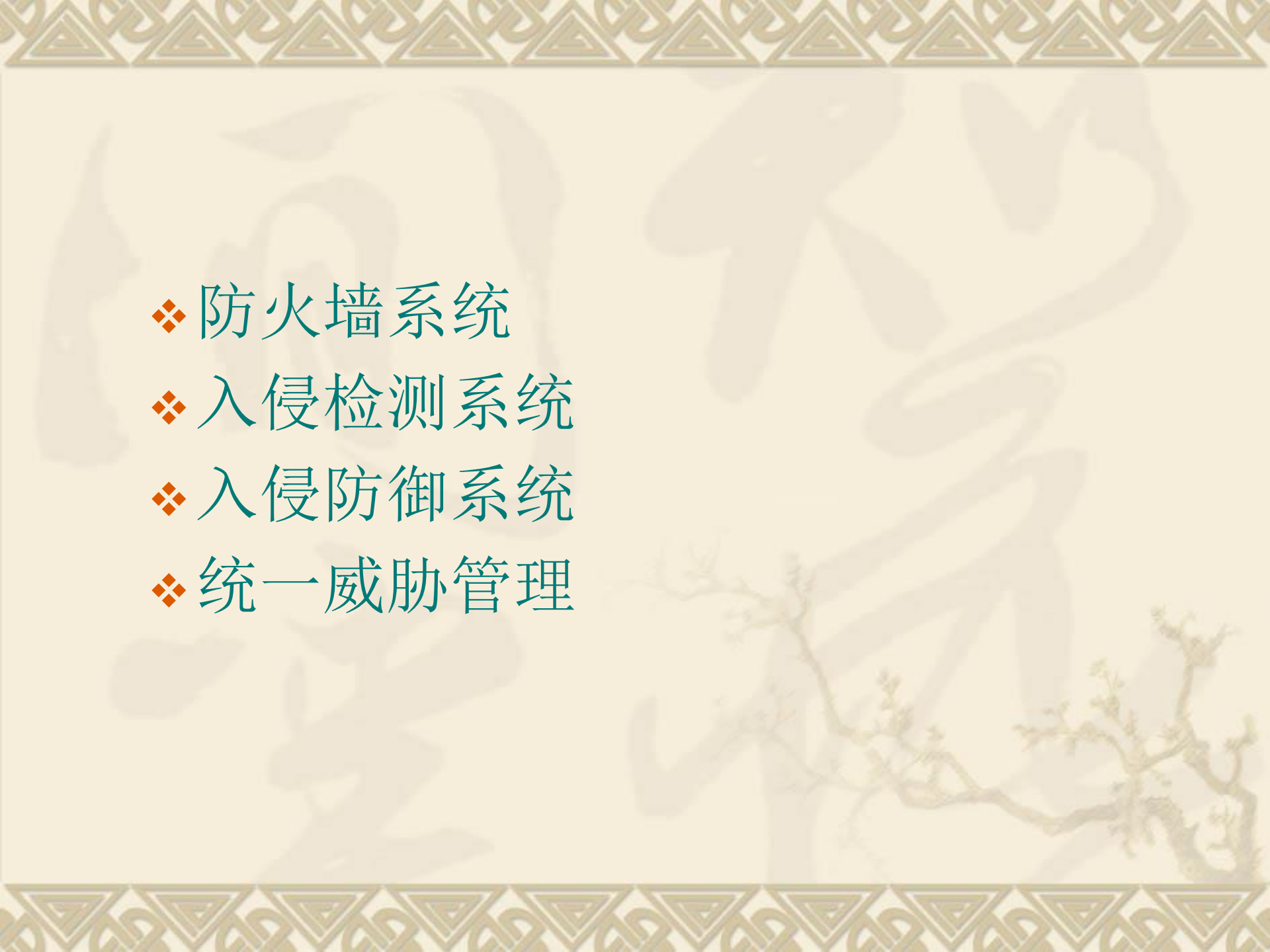


第十章

网络安全防御系统

- 
- 
- ❖ 防火墙系统
 - ❖ 入侵检测系统
 - ❖ 入侵防御系统
 - ❖ 统一威胁管理

CISCO ASA5505-SEC-BUN-K9

防火墙



启明星辰天阕NS100 入侵检测系统



H3C SecPath T200-A

入侵防御系统



SecPath T200-A

H3C SecPath U200-M

统一威胁管理



防火墙系统



❖ 什么是防火墙

❧ 古代修筑在房屋之间的一道墙,用于防止火势蔓延

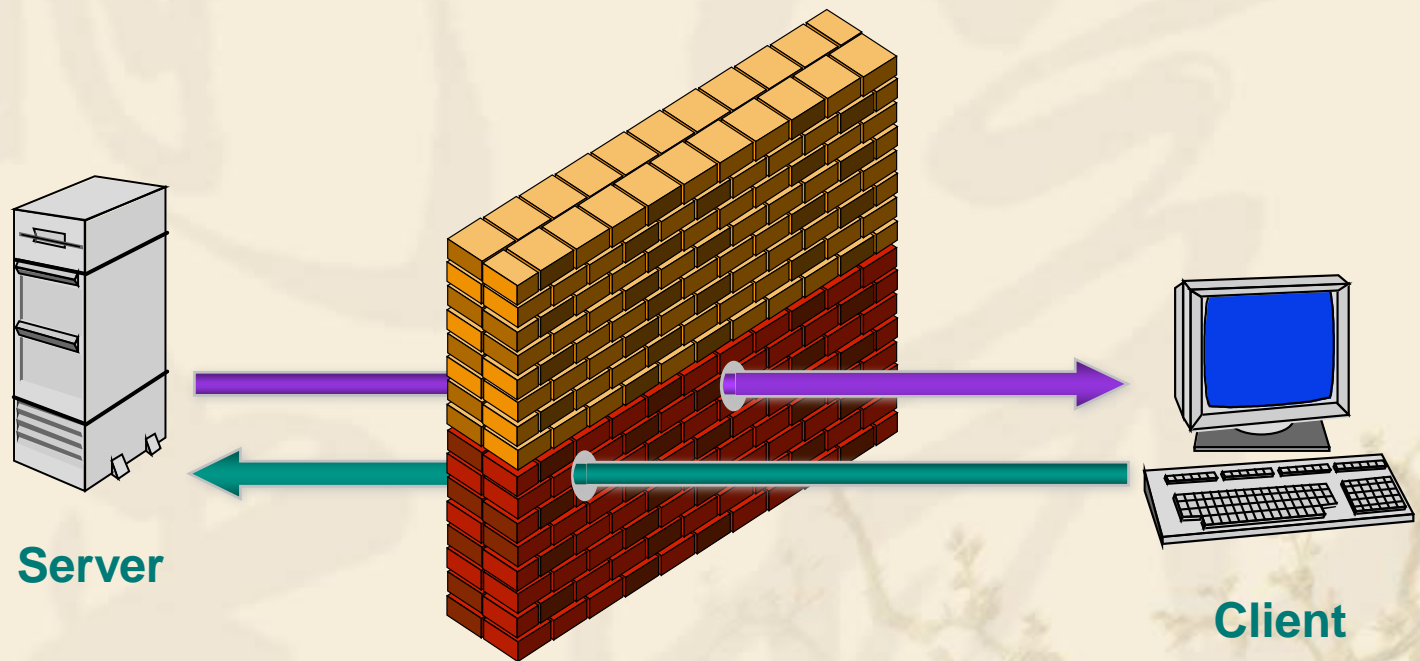
❧ Rich Kosinski(Internet Security公司总裁)：

防火墙是一种访问控制技术，在某个机构的网络和不安全的网络之间设置障碍，阻止对信息资源的非法访问。

防火墙的原理

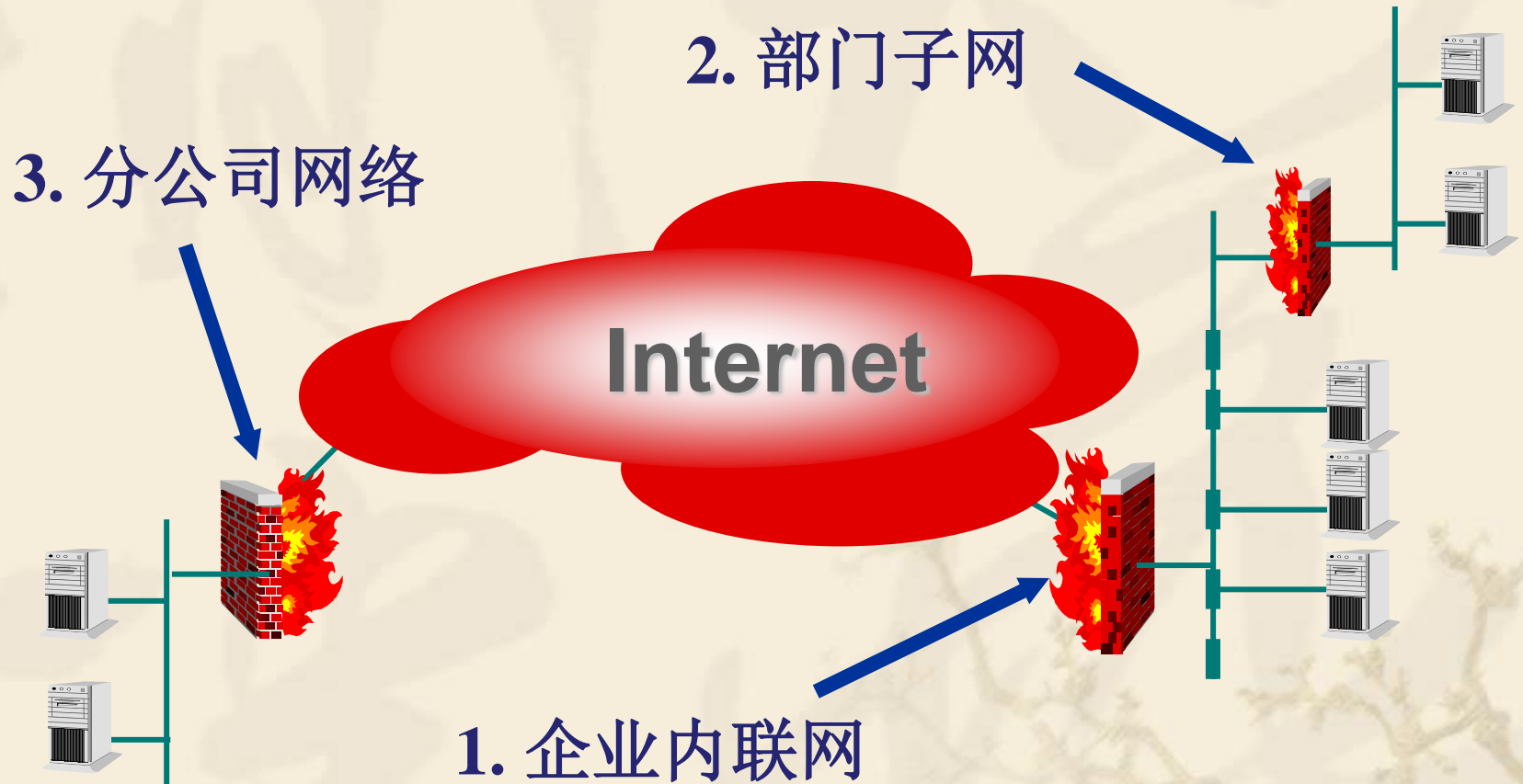
- ❖ Willam Cheswick和 steven Beellovin: 防火墙是位于两个（或多个）网络间，实施网间访问控制的一组组件的集合，它满足以下条件：
 - ∞内部和外部之间的所有网络数据流必须经过防火墙；
 - ∞符合安全政策的数据流才能通过防火墙；
 - ∞防火墙自身能抗攻击。

☀ 防火墙 (Firewall)

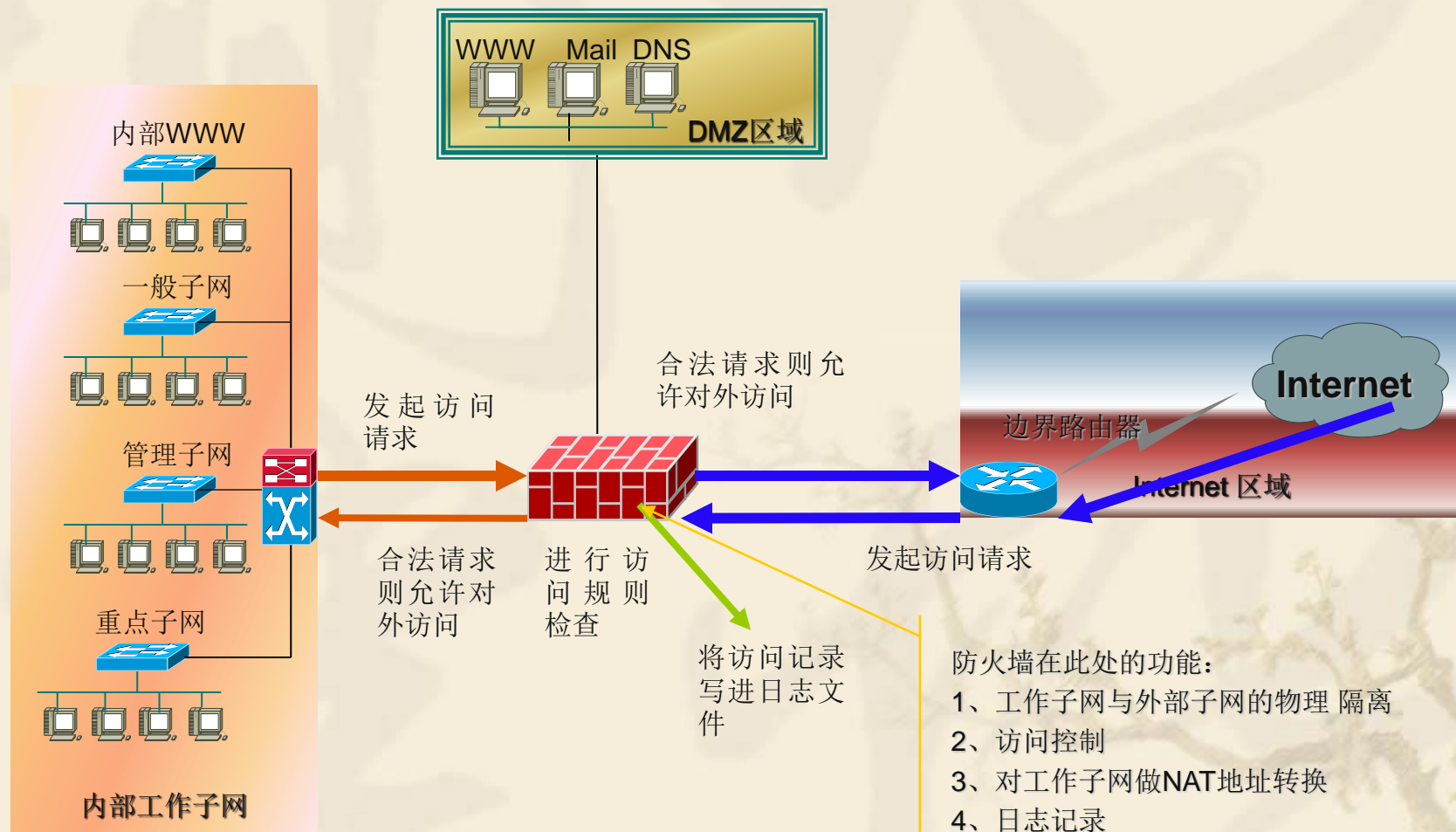


防火墙类似一堵城墙，将服务器与客户主机进行物理隔离，并在此基础上实现服务器与客户主机之间的授权互访、互通等功能。

防火墙示意图



一个典型的防火墙使用形态



防火墙的概念是广义的

- ❖ 在逻辑上，防火墙是分离器，限制器，也是一个分析器，有效地监控了内部网和外部网之间的任何活动，保证了内部网络的安全。
- ❖ 在物理上，防火墙通常是一组硬件设备——路由器、主计算机，或者是路由器、计算机和配有软件的网络的组合。
- ❖ 防火墙一般可分为多个部分，某些部分除了执行防火墙功能外还执行其它功能。如：加密和解密——VPN。

防火墙的作用

- ❖ 确保一个单位内的网络与因特网的通信符合该单位的安全方针，为管理人员提供下列问题的答案：
 - ❧ 谁在使用网络
 - ❧ 他们在网络上做什么
 - ❧ 他们什么时间使用了网络
 - ❧ 他们上网去了何处
 - ❧ 谁要上网没有成功

防火墙的实施策略

- ❖ 一切未被禁止的就是允许的（Yes规则）
 - ❧ 确定那些被认为是不安全的服务，禁止其访问；而其他服务则被认为是安全的，允许访问。
- ❖ 一切未被允许的就是禁止的（No规则）
 - ❧ 确定所有可以被提供的服务以及它们的安全性，然后开放这些服务，并将所有其他未被列入的服务排除在外，禁止访问。

防火墙的分类

- ❖ 根据防火墙形式分类
- ❖ 根据防火墙结构分类
- ❖ 按照防火墙应用部署分类
- ❖ 根据防火墙实现技术分类

根据防火墙形式分类

❖ 软件防火墙

- ❧ 软件防火墙运行于特定的计算机上，它需要客户预先安装好的计算机操作系统的支持，一般来说这台计算机就是整个网络的网关。俗称“个人防火墙”。

❖ 硬件防火墙

- ❧ 基于PC架构，就是说，它们和普通的家庭用的PC没有太大区别。在这些PC架构计算机上运行一些经过裁剪和简化的操作系统，最常用的有老版本的Unix、Linux和FreeBSD系统。由于此类防火墙采用的依然是别人的内核，因此依然会受到OS（操作系统）本身的安全性影响。

❖ 芯片级防火墙

- ❧ 基于专门的硬件平台，速度更快，处理能力更强，性能更高。做这类防火墙最出名的厂商有NetScreen、FortiNet、Cisco等。这类防火墙由于是专用OS（操作系统），因此防火墙本身的漏洞比较少，不过价格相对比较高昂。

根据防火墙结构分类

❖ 单一主机防火墙

- ☞ 最为传统的防火墙，独立于其它网络设备，位于网络边界。一般都集成了两个以上的以太网卡，连接一个以上的内、外部网络。

❖ 路由器集成式防火墙

- ☞ 在许多中、高档路由器中集成了防火墙功能。如Cisco IOS防火墙系列。但这种防火墙通常是较低级的包过滤型。这样企业就不用再同时购买路由器和防火墙

❖ 分布式防火墙

- ☞ 由多个软、硬件组成的系统。渗透于网络的每一台主机，对整个内部网络的主机实施保护。在网络服务器中，通常会安装一个用于防火墙系统管理软件，在服务器及各主机上安装有集成网卡功能的PCI防火墙卡，一块防火墙卡同时兼有网卡和防火墙的双重功能。这样一个防火墙系统就可以彻底保护内部网络。

按照防火墙应用部署分类

❖ 网络防火墙

❧ 位于内、外部网络的边界，所起的作用是对内、外部网络实施隔离

❖ 基于主机的防火墙

❧ 安装于单台主机中，防护的也只是单台主机。这类防火墙应用于广大的个人用户，通常为软件防火墙，价格最便宜，在功能上有很大的限制。

根据实现技术分类

- ❖ 包过滤防火墙
- ❖ 状态防火墙
- ❖ 应用网关防火墙

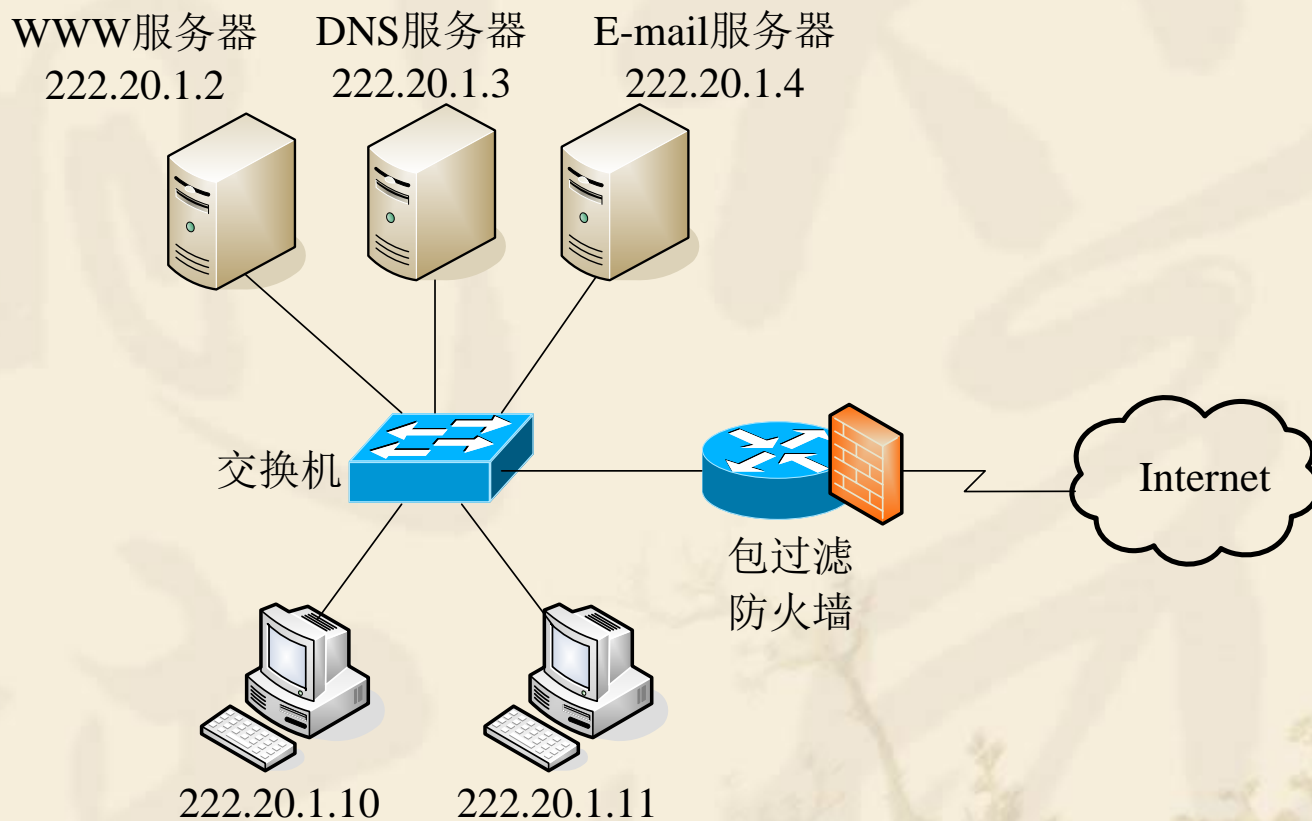
包过滤防火墙

- ❖ 包过滤防火墙是最早出现的、形式最简单的一种防火墙。
- ❖ 通常在路由器上通过访问控制列表来实现，通过检查数据包的报头信息，根据数据包的源地址、目的地址和以上其他的信息组合，按照过滤规则来决定是否允许数据包通过。
- ❖ 包过滤防火墙在根据规则对数据包的相关内容进行匹配时，一般不判断数据包的上下文，只根据当前的数据包内容做决定。

- ❖ 包过滤防火墙通常可以根据源IP地址、目的IP地址、传输层协议、端口号等来进行数据包的过滤

TCP/IP层	过滤依据
网络层	源IP地址、目的IP地址
网络层	IP、ICMP、OSPF、TCP、UDP或其它协议
网络层	IP优先级域（服务类型）
传输层	TCP和UDP端口号
传输层	TCP控制标记（SYN、ACK、FIN、PSH、RST等）

一个包过滤防火墙的应用实例



规则	源 IP 地址	目的 IP 地址	协议	端口号	操作
1	任意	222.20.1.2	TCP	80	允许
2	任意	222.20.1.3	UDP	53	允许
3	任意	222.20.1.4	TCP	25	允许
4	任意	任意	任意	任意	丢弃

包过滤防火墙的优缺点

❖ 优点:

- ❧ 性能优于其他防火墙，因为它执行的计算较少，并且容易用硬件方式实现；
- ❧ 规则设置简单，通过禁止内部计算机和特定Internet资源连接，单一规则即可保护整个网络；
- ❧ 不需要对客户端计算机进行专门配置。

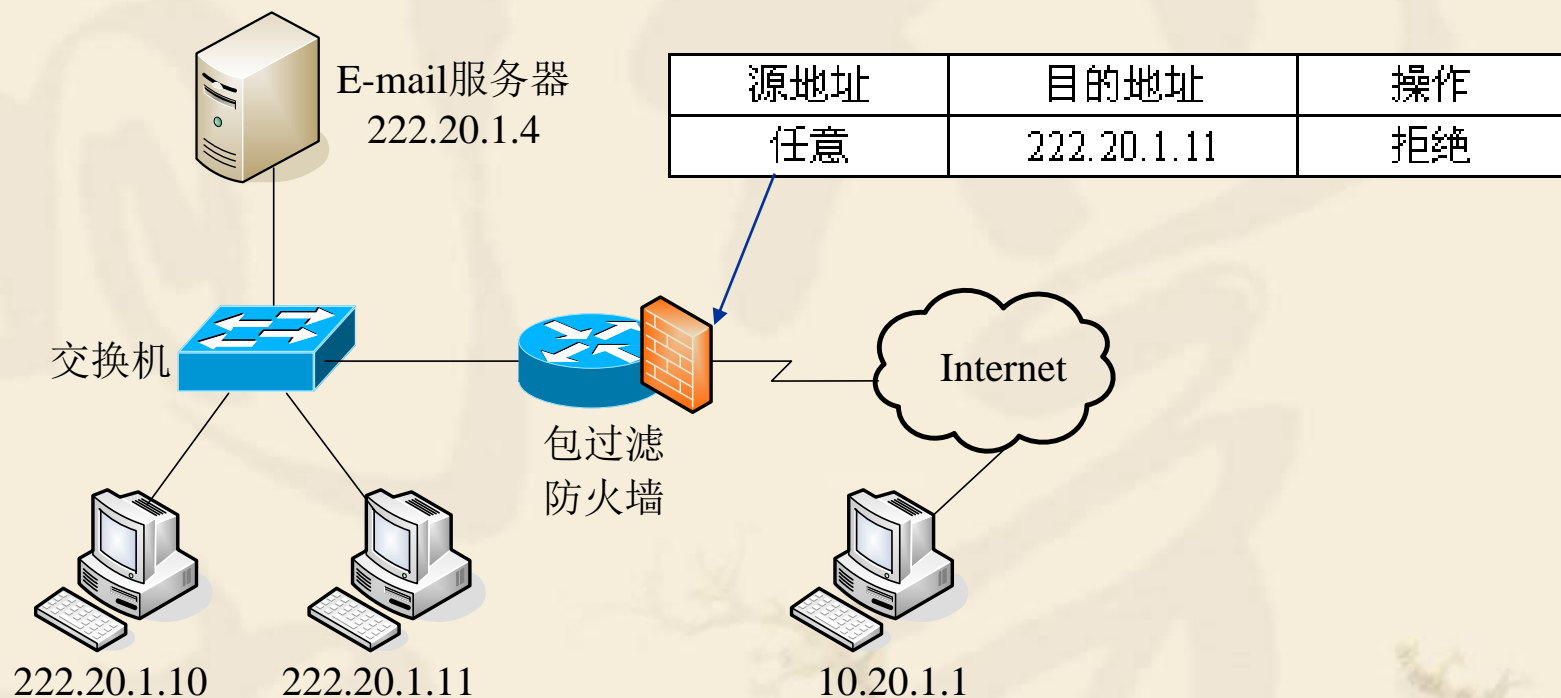
❖ 缺点:

- ❧ 对管理员的知识要求高；
- ❧ 不能阻止应用层的攻击；
- ❧ 只对某些类型的TCP/IP攻击比较敏感；
- ❧ 不支持用户的连接认证；
- ❧ 只有有限的日志功能。

状态防火墙

- ❖ 状态防火墙采用的是状态检测技术，这是由CheckPoint公司最先提出的一项具有突破性的防火墙技术。它把包过滤的快速性和代理的安全性很好地结合在一起，成为防火墙的基本过滤模式。

先分析包过滤防火墙的一个问题



- ❖ 阻止Internet上的任意主机发往内部网络中主机222.20.1.11的数据包。
- ❖ 如果内部主机222.20.1.11要访问Internet上的某台主机？？

尝试下面两种解决办法

❖ 开放端口

∞ 由于客户端在发出请求时，本地端口是临时分配的，也就是说这个端口是不定的，只要是1023以上的端口都有可能，所以如果要开放端口，只有把这些所有端口都开放

源地址	目的地址	目的端口	操作
任意	222.20.1.11	大于 1023	允许
任意	222.20.1.11	其它	拒绝

∞ 显然，这是非常危险的

尝试下面两种解决办法方法

❖ 检查TCP控制位

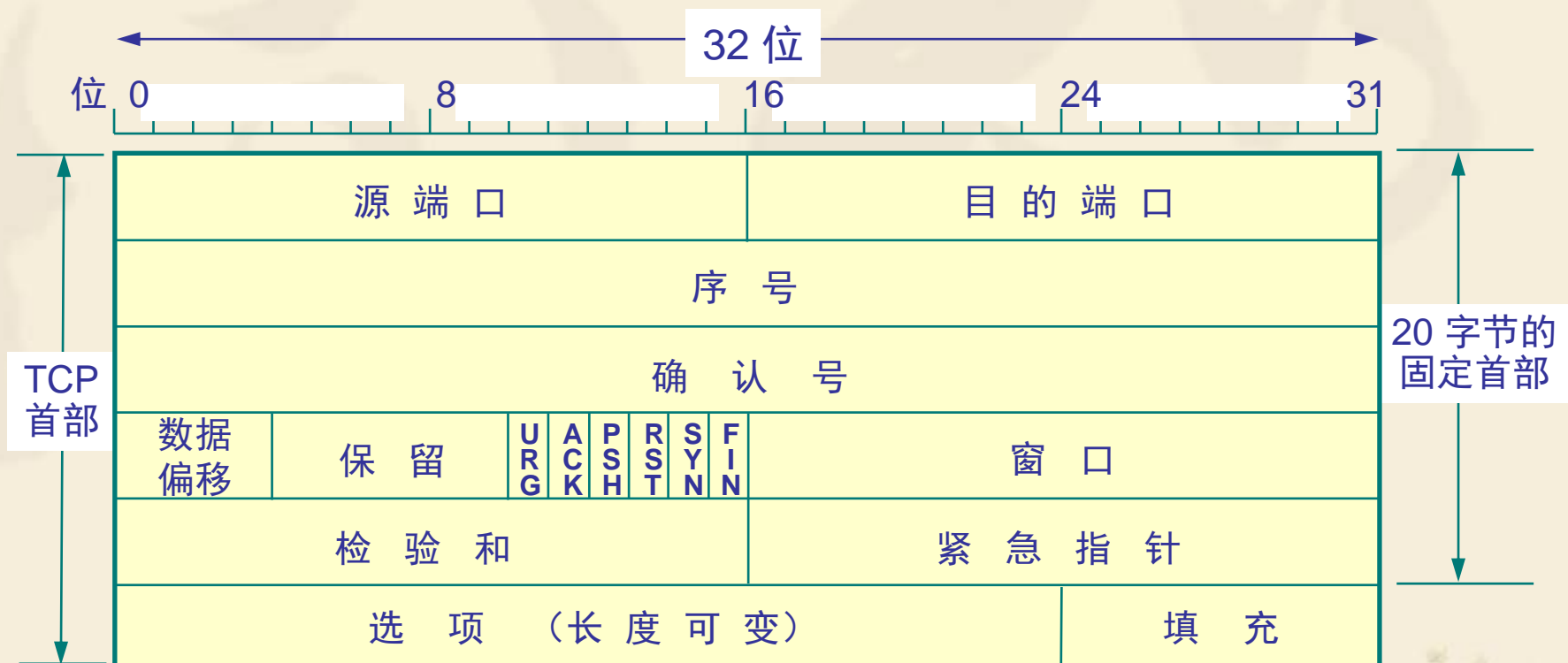
源地址	目的地址	协议信息	操作
任意	222.20.1.11	TCP 控制字段: ACK,RST,SYN/ACK,FIN	允许
任意	222.20.1.11	其它	拒绝

- ❧ 不是所有的传输层协议都支持控制字段
- ❧ 控制字段的值也能被手工操控，根据TCP连接中的ACK位值来决定数据包进出，容易导致DoS攻击。

状态检测

- ❖ **TCP**的连接过程是一个有序过程，新连接一定是通过**SYN**包来开始的，防火墙可以将连接的信息记录到连接状态表中。
- ❖ 数据通信过程是有方向性的，一定是发起方发送**SYN**，接收方发**SYN/ACK**，不是此方向的数据就是非法的。
- ❖ 因此状态检测可以实现“**A**可以访问**B**而**B**却不能访问**A**”的效果。

- ❖ 当222.20.1.11发送一个TCP连接请求SYN，源端口号是一个大于1023的整数（例如端口号为10000），目的端口号为80。
- ❖ 这个数据包在到达状态防火墙后，防火墙会将这个连接信息记录到一个连接状态表中，然后再将这个数据包转发出去。
- ❖ 当防火墙收到来自10.20.1.1的连接响应包时，首先查找连接状态表，就会知道从10.20.1.1的TCP80端口到222.20.1.11的TCP10000端口的响应是已存在的连接的一部分，就会允许数据包通过，从而双方在第三次握手之后建立连接。
- ❖ 之后两者之间的通信由于是属于这个连接的，防火墙都会放行。



包过滤和状态防火墙的比较

- ❖ 当比较包过滤防火墙和状态防火墙时，状态防火墙更智能，因为它能理解连接的状态：初始化连接、传输数据或者释放连接。通常，一个状态防火墙包含了包过滤防火墙的功能。

状态防火墙的优缺点

❖ 优点:

- ❧ 状态防火墙知晓连接的状态;
- ❧ 状态防火墙无须打开很大范围的端口以允许通信;
- ❧ 状态防火墙能比包过滤防火墙阻止更多类型的DoS攻击,并具有更丰富的日志功能。

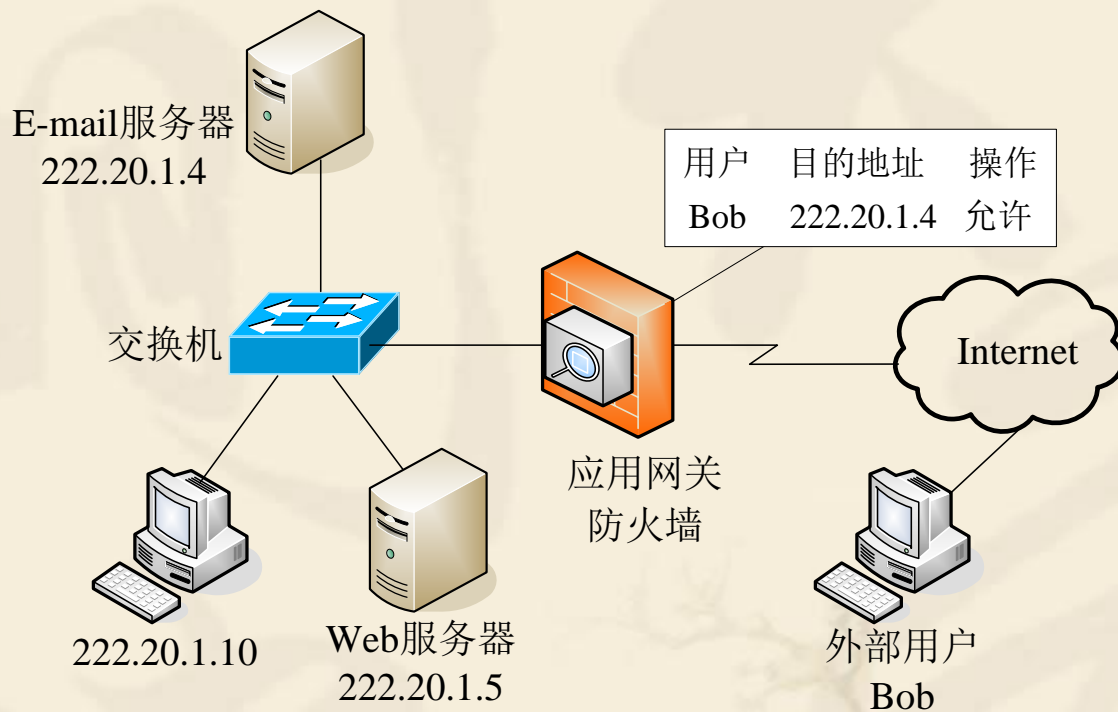
❖ 缺点:

- ❧ 配置防火墙需要管理员对网络层和传输层的信息非常熟悉,配置起来会比较复杂;
- ❧ 由于状态防火墙依然检验的是网络层和传输层的信息而不涉及到应用层,所以它任然不能阻止应用层攻击
- ❧ 不是所有的协议都象TCP协议那样包含有状态信息

应用网关防火墙

- ❖ 应用网关防火墙，也称为代理防火墙，能够根据网络层、传输层和应用层的信息对数据流进行过滤。由于应用网关防火墙要在应用层处理信息，所以绝大多数应用网关防火墙的控制和过滤功能是通过软件来完成的，这能够比包过滤或状态防火墙提供更细粒度的流量控制。

应用网关防火墙的认证功能

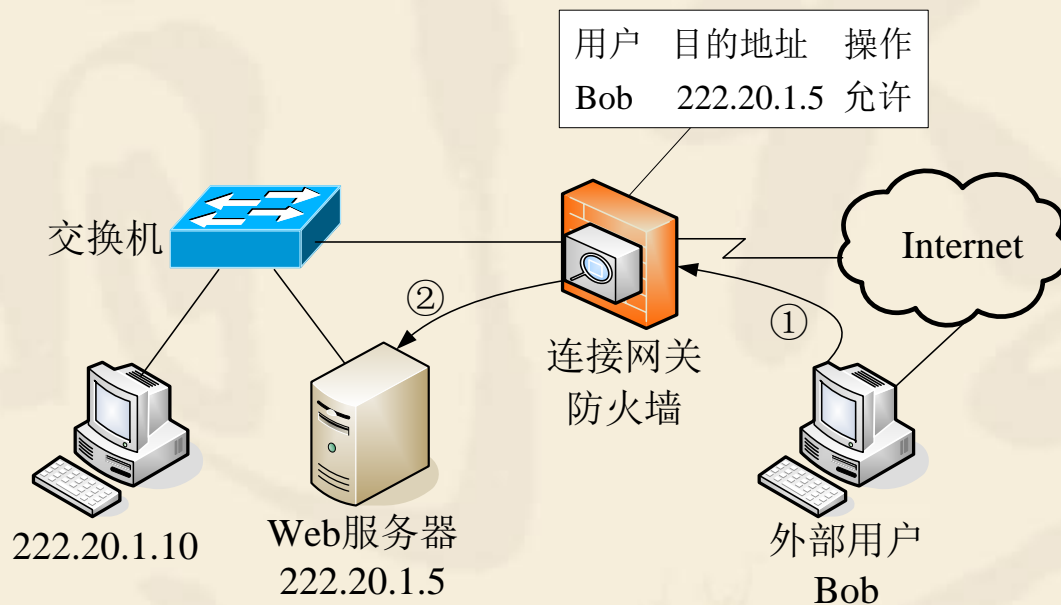


- ❖ 用户主动发送一个连接到应用网关防火墙的Web浏览器，或者应用网关防火墙截获用户到内部服务器的初始化连接请求后，发送给用户一个认证信息的请求（比如Web浏览器的弹出窗口）。然后应用网关防火墙对用户的身份信息认证。

应用网关防火墙的分类

- ❖ 连接网关防火墙
- ❖ 直通代理防火墙

连接网关防火墙



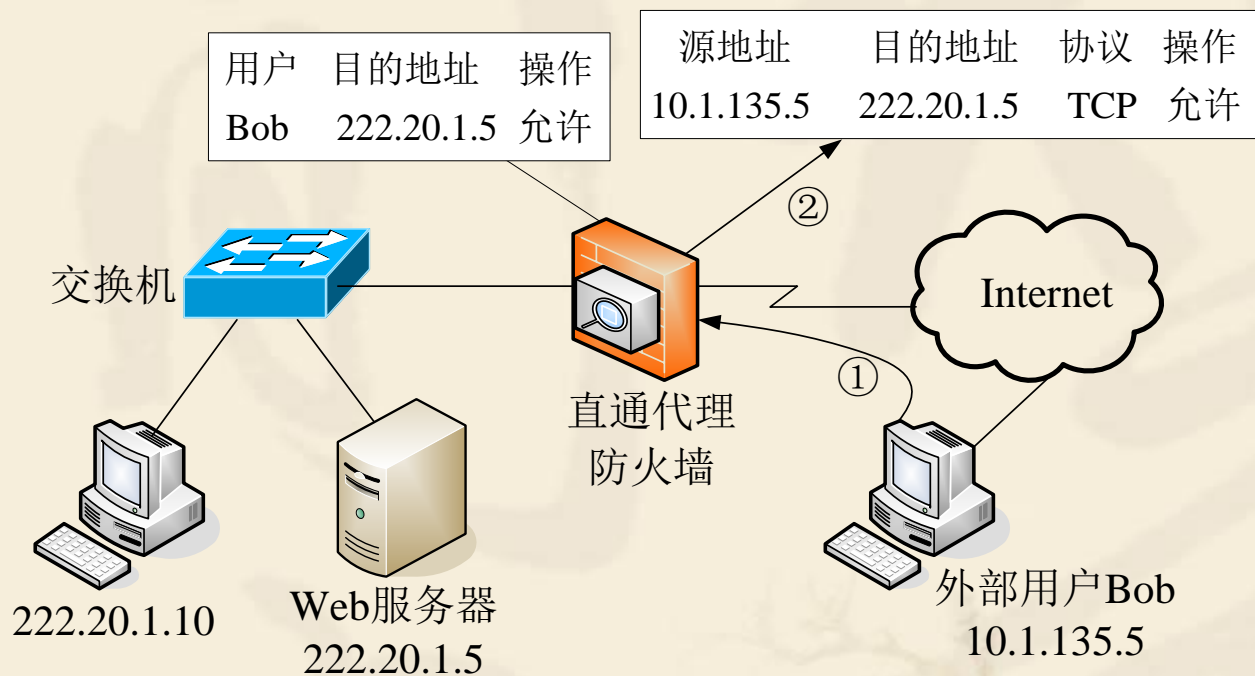
❖ 过程①

☞ 当外部用户**Bob**试图建立一个到内部**Web**服务器的连接时，连接网关防火墙会截获这个连接，并要求对用户进行认证

❖ 过程②

☞ 通过认证后，防火墙会打开一个到内部**Web**服务器的单独连接。

直通代理防火墙



❖ 过程①

☞ 当外部用户**Bob**试图建立一个到内部**Web**服务器的连接时，和连接网关防火墙一样，直通代理会对用户进行认证。

❖ 过程②

☞ 认证通过后，这个连接和任何其它授权连接（网络层和传输层的信息）被添加到过滤规则表中。

应用网关防火墙的优缺点

❖ 优点

- ❧ 能够实现对用户的认证，这能够阻止绝大多数欺骗攻击。
- ❧ 使用连接代理防火墙则能够监控连接上的所有数据，使得我们能够检测到应用层攻击，如不良的URL、缓存溢出企图、未授权的访问和更多类型的攻击，同时生成非常详细的日志。

❖ 缺点

- ❧ 密集性的处理过程要求大量的CPU资源和内存。
- ❧ 详尽的日志能够也会占用大量磁盘空间。
- ❧ 通常不支持所有的应用，它基本上被限制在一种或少数几种连接类型上。
- ❧ 应用网关防火墙有时要求在客户端安装厂商指定的软件，用来处理认证过程和可能的连接重定向

混合防火墙与防火墙系统

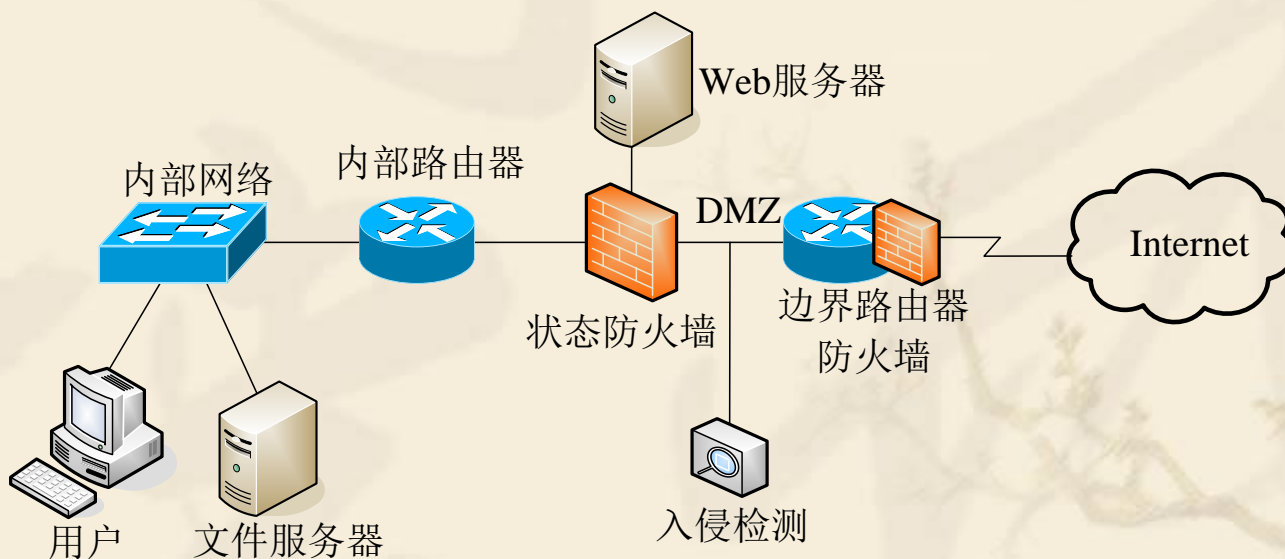
- ❖ 随着Internet的广泛使用和电子商务的蓬勃发展，对网络安全的需求也急剧增加。一个功能单一的防火墙产品往往无法满足越来越复杂的安全形势。
- ❖ 为了提供健壮的安全特性，可以通过两个途径来对已有的防火墙进行改进。
 - ❧ 将前述多种类型的防火墙的功能整合到一个单一的防火墙产品中，这就是**混合防火墙**；
 - ❧ 将多种安全技术应用到各个防火墙组件中，构成**防火墙系统**。

混合防火墙

- ❧ 将多种安全技术集成在一起的单一设备，为网络提供更加综合性的保护。例如**Cisco PIX**防火墙，它支持一个状态防火墙、一个直通代理和最小形式的连接网关防火墙，也具有网络地址转换和很多其它安全特性。

防火墙系统

- ❖ 由多种安全技术、多台安全设备构成的，并且通过合理部署的安全防御系统。
- ❖ 往往包含了边界路由器、防火墙、VPN、入侵检测等组件。



防火墙的体系结构

❖ 堡垒主机（Bastion Host）

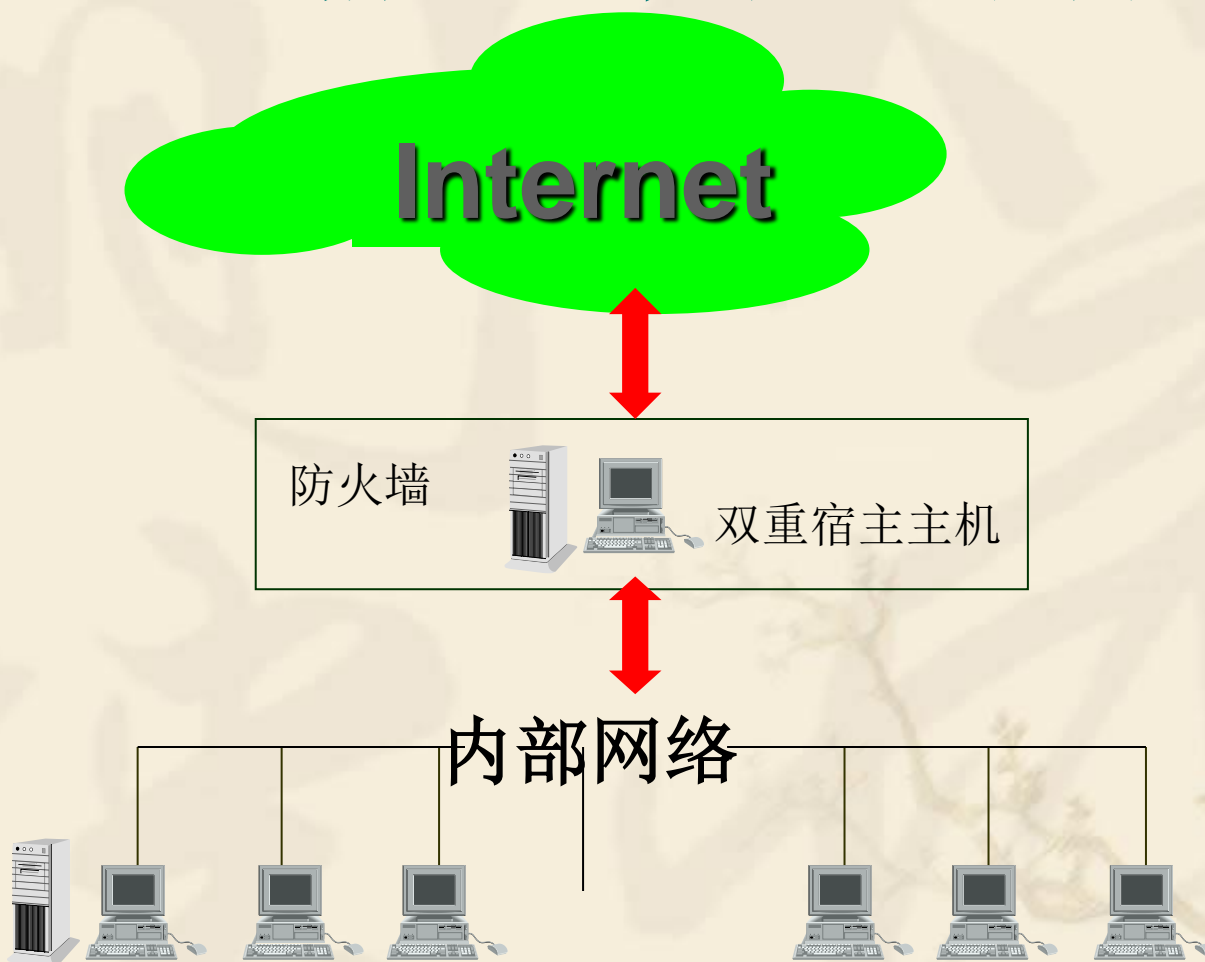
☞ 物理内部网中唯一可供外界访问到的主机，它通常配置了严格的安全防范措施，堡垒主机为内部网和外部网之间的通信提供一个阻塞点。

❖ DMZ

☞ 指供外部网访问的专门区域，用于发布信息、提供服务。通常情况下，外部网和内部网都可以访问这一区域。

❖ 防火墙的体系结构一般有双重宿主主机体系结构、屏蔽主机体系结构和屏蔽子网体系结构。

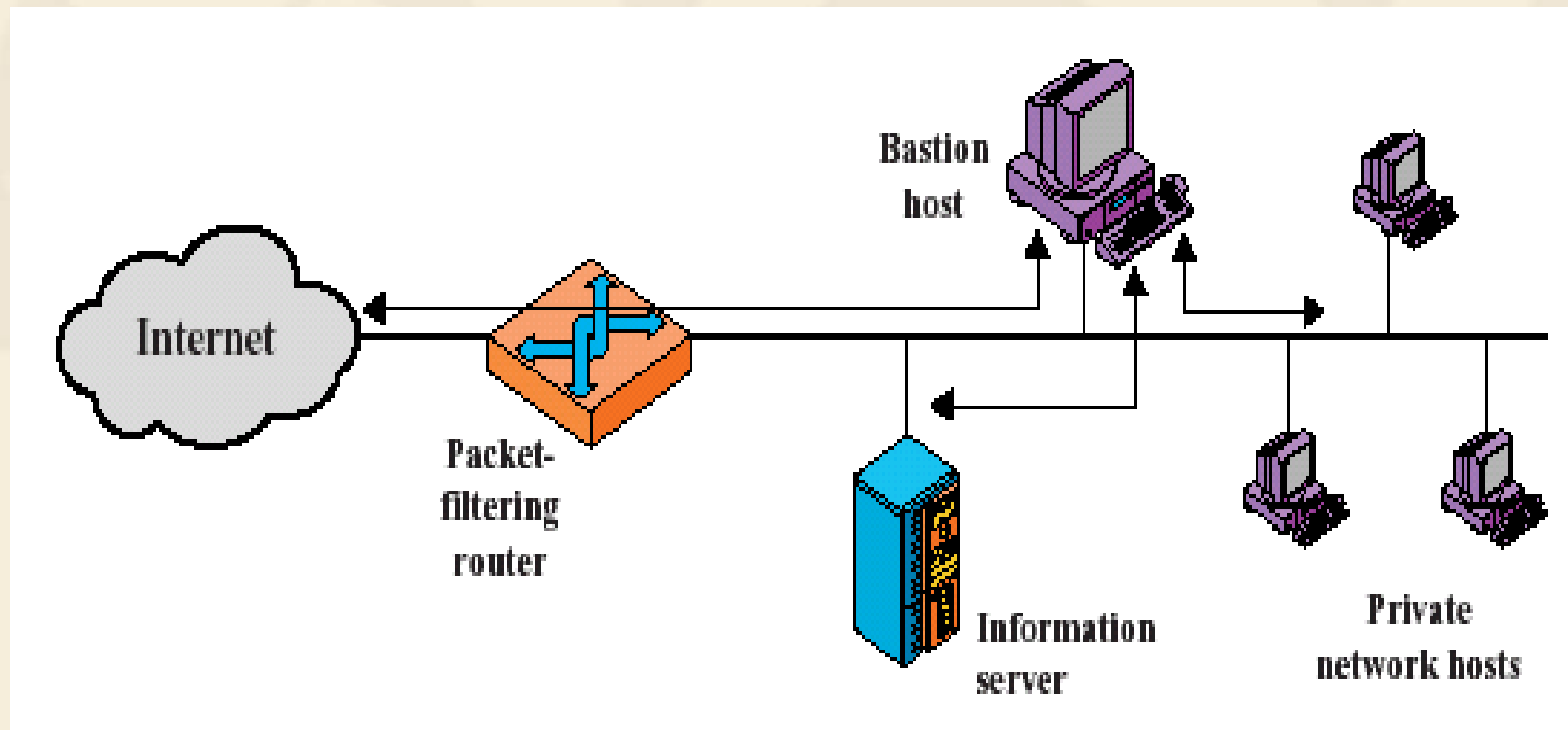
双重宿主主机体系结构



双重宿主主机体系结构

- ❖ 所有的流量都通过堡垒主机（双网卡）
- ❖ 两种方式：
 - ❧ 用户登录
 - ❧ 服务代理
- ❖ 缺点：双重宿主主机是隔开内外网络的唯一屏障，一旦它被入侵，内部网络便向入侵者敞开大门

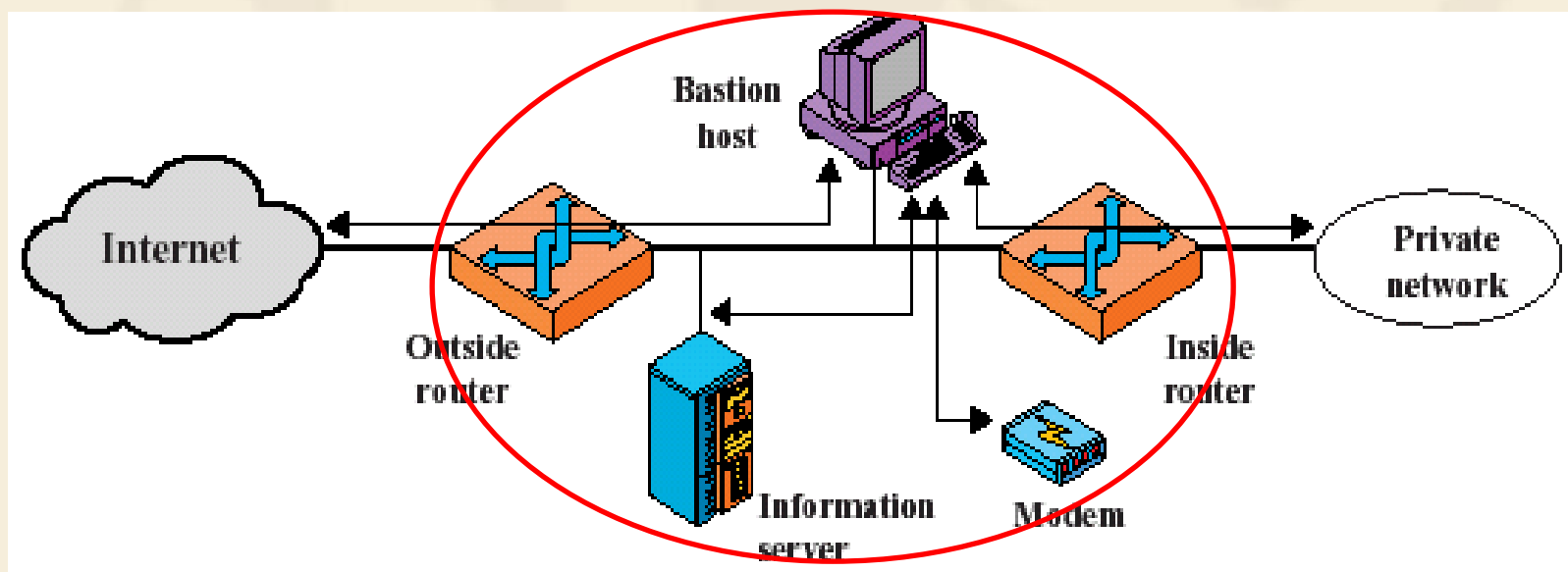
屏蔽主机体系结构



屏蔽主机

- ❖ 屏蔽主机方案：单宿主堡垒主机
- ❖ 典型构成：包过滤路由器+堡垒主机。
 - ❧ 包过滤路由器配置在内部网和外部网之间，保证外部系统对内部网络的操作只能经过堡垒主机。
 - ❧ 堡垒主机配置在内部网络上，是外部网络主机连接到内部网络主机的桥梁，它需要拥有高等级的安全。
- ❖ 只允许堡垒主机可以与外界直接通讯
- ❖ 优点：两层保护：包过滤+应用层网关；灵活配置
- ❖ 缺点：如果路由器被损害，堡垒主机将被穿过，则内部网络被暴露

屏蔽子网体系结构



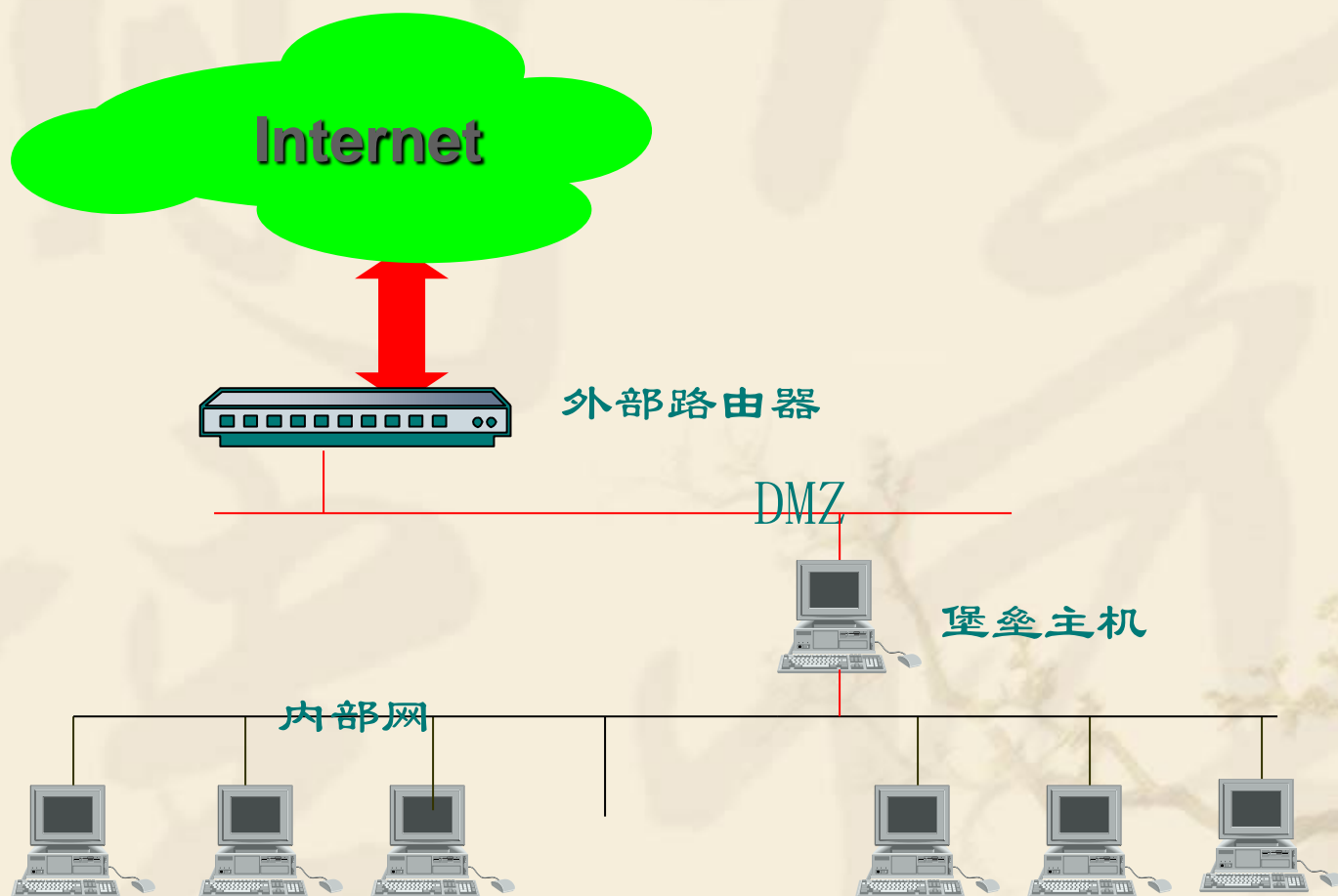
- ◆ 屏蔽子网防火墙
- ◆ 优点：
 - 三层防护，用来阻止入侵者
 - 外面的router只向Internet暴露屏蔽子网中的主机
 - 内部的router只向内部私有网暴露屏蔽子网中的主机

屏蔽子网体系结构

- ❖ 屏蔽子网体系结构在本质上与屏蔽主机体系结构一样，但添加了额外的一层保护体系——周边网络。堡垒主机位于周边网络上，周边网络和内部网络被内部路由器分开。
- ❖ 原因：堡垒主机是用户网络上最容易受侵袭的机器。通过在周边网络上隔离堡垒主机，能减少在堡垒主机被侵入的影响。
- ❖ 周边网络是一个防护层，在其上可放置一些信息服务器，它们是牺牲主机，可能会受到攻击，因此又被称为非军事区（DMZ）。
- ❖ 周边网络的作用：即使堡垒主机被入侵者控制，它仍可消除对内部网的侦听。

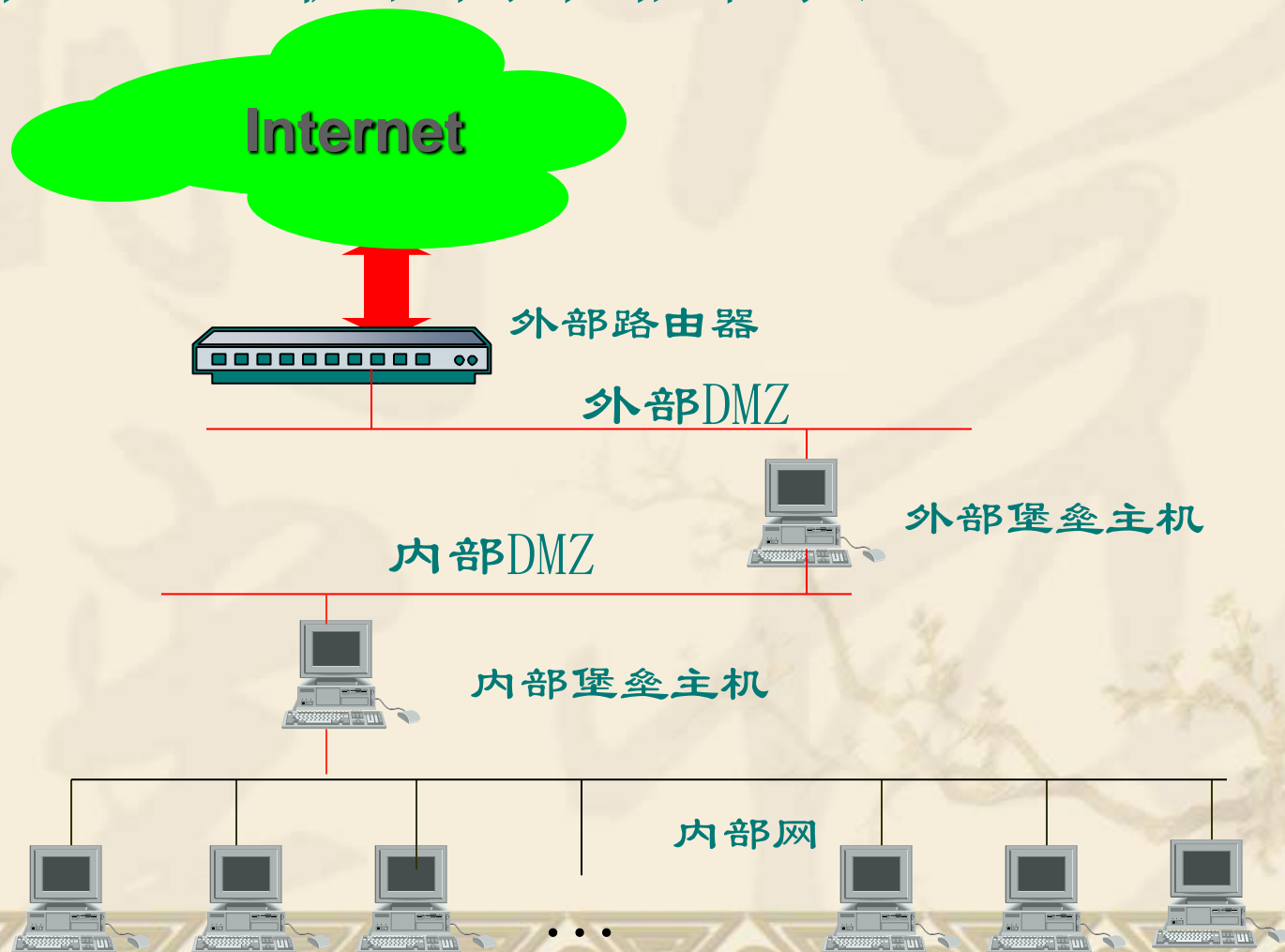
其它的防火墙结构（1）

❖ 一个堡垒主机和一个非军事区示意图



其它的防火墙结构（2）

❖ 两个堡垒主机和两个非军事区



防火墙的功能（总结）

- ❖ 不同厂商的产品功能不尽相同。
- ❖ 相同厂商的产品因不同型号，具有的功能也不尽相同。

防火墙的基本功能模块



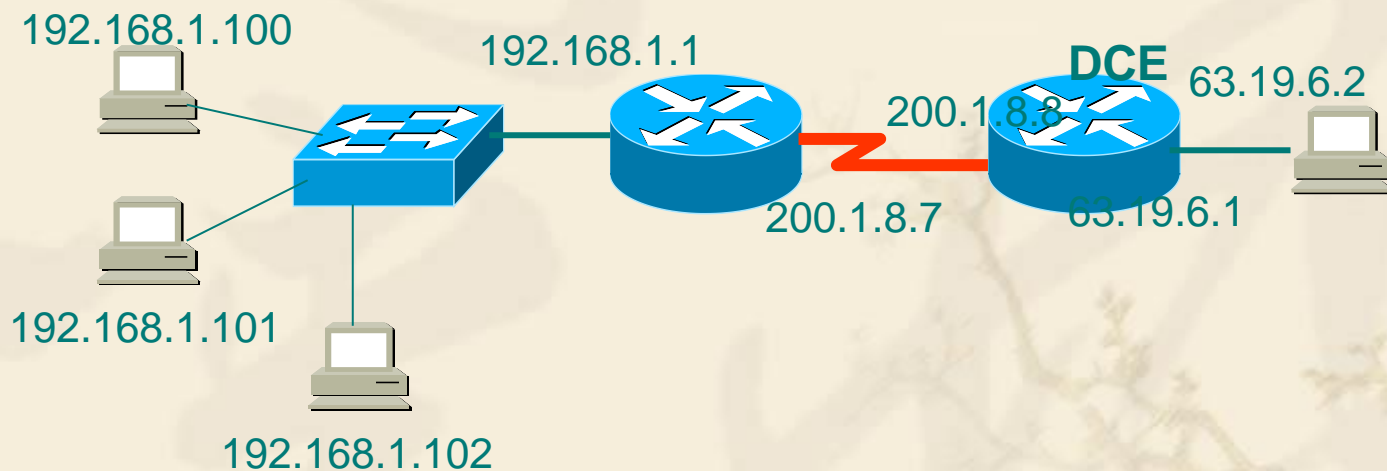
1 访问控制列表

❖ 通过访问控制列表来实现包过滤。

规则	包的方向	源地址	目的地址	协议	源端口	目的端口	ACK	是否通过
A	出	内部	Internet	TCP	>1023	80	any	允许
B	入	Internet	内部	TCP	80	>1023	1	允许

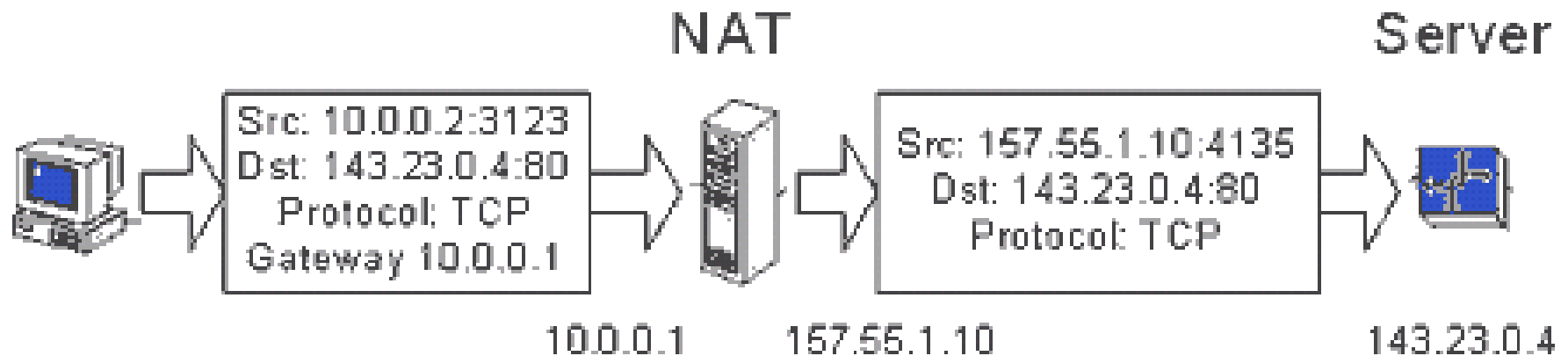
2 网络地址转换

- ❖ 通过NAT技术，隐藏内部主机，限制外部网络对内部主机的访问。



3 端口映射

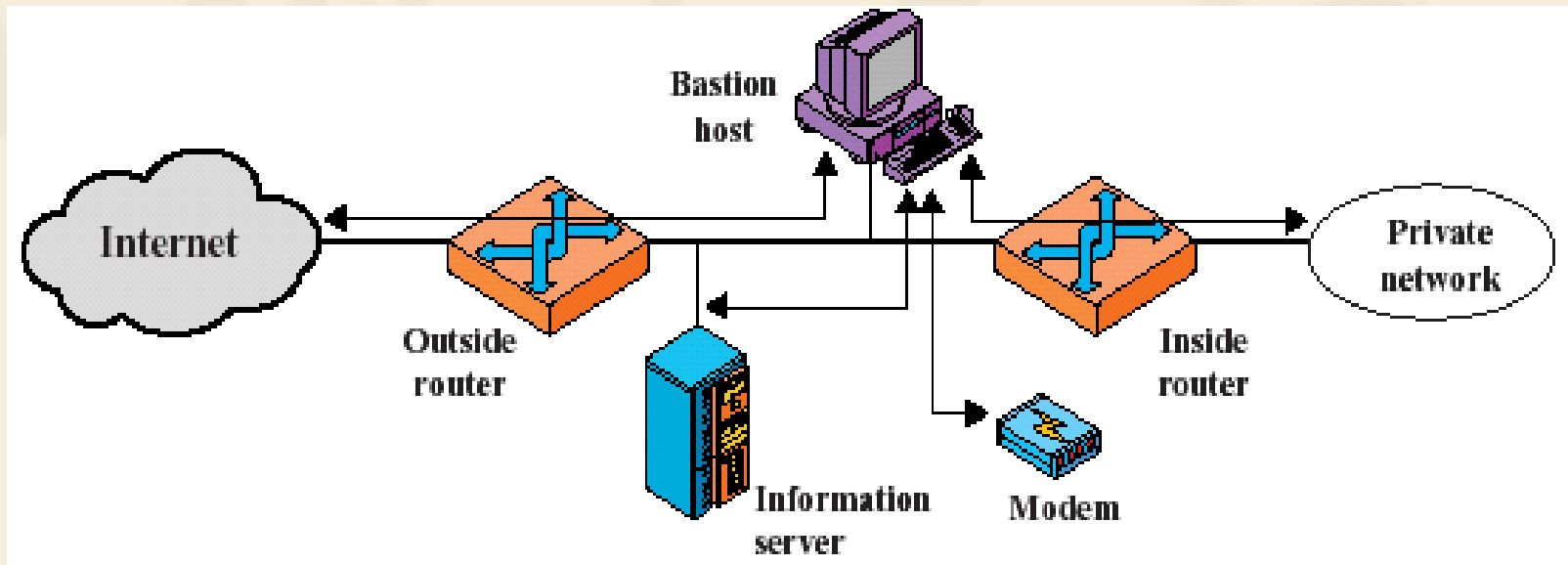
❖ 即NAPT



Port Mapping	
Internal IP	10.0.0.2
Internal port	3123
External IP	157.55.1.10
External port	4135
Remote host	143.23.0.4
Remote port	80

4 路由

- ❖ 防火墙具有简单的路由功能，如静态路由。



5 入侵检测

- ❖ 许多防火墙集成了一些简单的入侵检测功能。
 - ❧ 滥用检测（Misuse Detection）
 - ❧ 异常检测（Anomaly Detection）
 - ❧ 基于主机的入侵检测
 - ❧ 基于网络的入侵检测
 - ❧ 入侵响应

防火墙的参数--并发连接数

- ❧ 防火墙所能处理的最大会话数量，就是“并发连接数”。
- ❧ 并发连接数是指防火墙或代理服务器对其业务信息流的处理能力，是防火墙能够同时处理的点对点连接的最大数目。这个参数的大小直接影响到防火墙所能支持的最大信息点数。

并发连接数并非越大越好

- ❖ 并发连接数的增大意味着对系统内存资源的消耗。
- ❖ 并发连接表，是防火墙用以存放并发连接信息的地方，它可在防火墙系统启动后动态分配进程的内存空间，其大小也就是防火墙所能支持的最大并发连接数。
- ❖ 以每个并发连接表项占用300B计算，实现1000000个并发连接的话那么，这个产品就需要提供2.24Gb内存空间。
- ❖ 并发连接数的增大应当充分考虑CPU的处理能力
- ❖ 应当根据网络环境的具体情况和个人不同的上网习惯来选择适当规模的并发连接表。

防火墙的参数-- --吞吐量

- ❖ 吞吐量是指在不丢包的情况下单位时间内通过防火墙的数据包数量。
- ❖ 防火墙作为内外网之间的唯一数据通道，如果吞吐量太小，就会成为网络瓶颈，给整个网络的传输效率带来负面影响。
- ❖ 大多数防火墙虽号称100M防火墙，由于其算法依靠软件实现，通信量远远没有达到100M,实际只有10M-20M。纯硬件防火墙，由于采用硬件进行运算，因此吞吐量可以达到线性90-95M,是真正的100M防火墙。

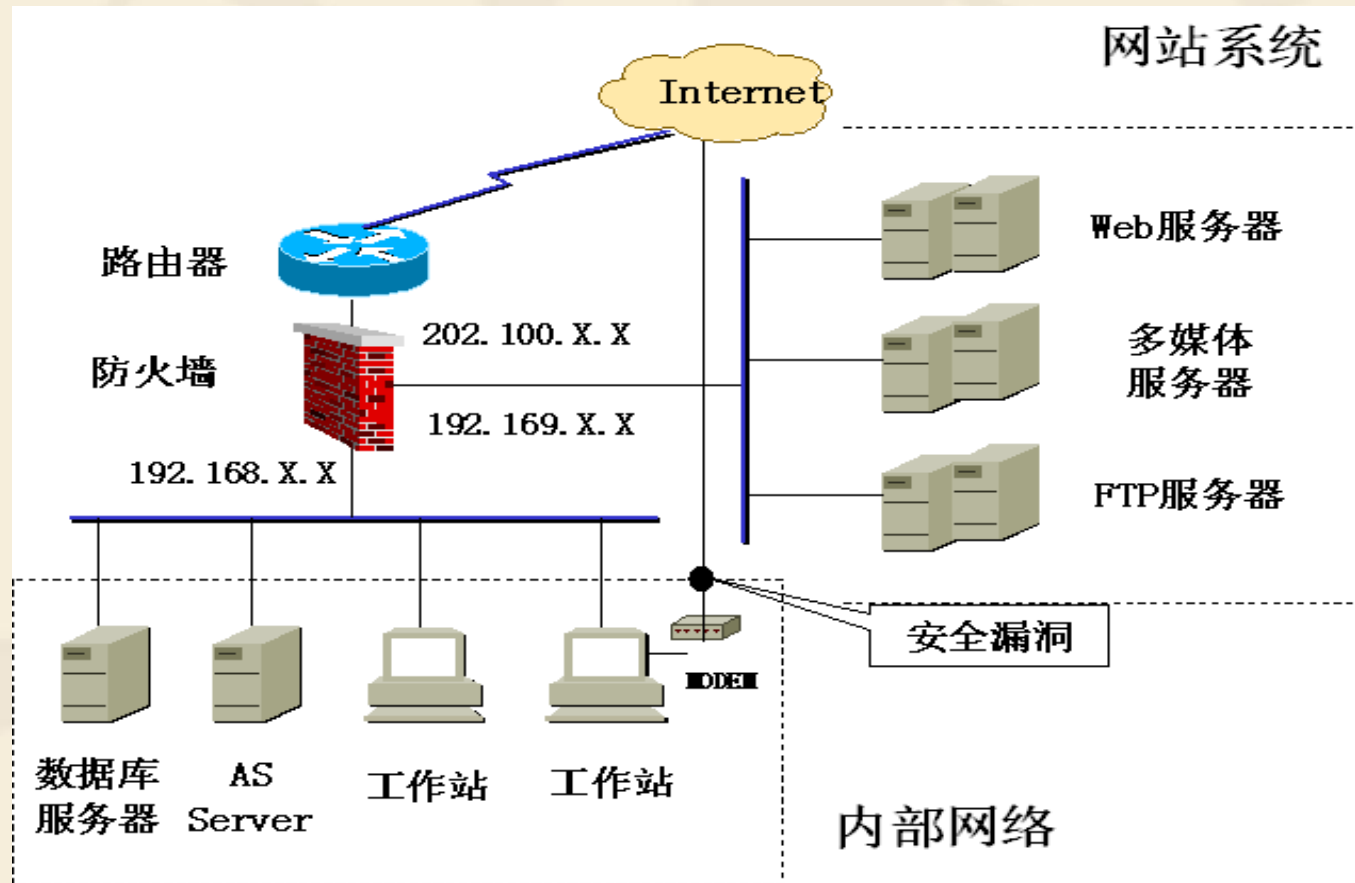
防火墙的参数--用户数

- ❖ 防火墙的用户数限制分为固定限制用户数和无用户数限制两种。固定限制用户数防火墙一般支持几十到几百个用户不等，而无用户数限制大多用于大的部门或公司。
- ❖ 注意，用户数和并发连接数是完全不同的两个概念，并发连接数是指防火墙的最大会话数（或进程），每个用户可以在一个时间里产生很多的连接

防火墙的局限性

- ❖ 防火墙无法防范来自网络内部的攻击，而通过调查发现，有将近一半以上的攻击都来自网络内部
- ❖ 防火墙无法对绕过它的通信进行限制。
- ❖ 防火墙不能堵住来自外部网络的病毒。

防火墙不可以防范什么



内部提供拨号服务绕过防火墙

防火墙的局限性(2)

- ❖ 为了提高安全性，限制或关闭了一些有用但存在安全缺陷的网络服务，给用户带来使用的不便。
- ❖ 防火墙对用户不完全透明，可能带来传输延迟、瓶颈。
- ❖ 作为一种被动的防护手段，防火墙不能防范因特网上不断出现的新的威胁和攻击。

发展趋势

❖ 高性能的防火墙

- ❧ 在今后网络安全防护的路途上，防火墙采用**ASIC**芯片技术将要成为主导地位。

❖ 管理接口和**SOC**的整合，联动功能

- ❧ **SOC——Security Operation Center** 安全管理中心

❖ 抗**DoS**能力

- ❧ 有待于新技术的出现。

❖ 减慢蠕虫和垃圾邮件的传播速度的功能

- ❧ 加强防火墙对数据处理中的粒度和力度，已经成为未来防火墙对数据检测高粒度的发展趋势。

回顾：防火墙的缺点

- ❖ 不能防止来自内部网络的攻击
- ❖ 防火墙不能防范不经过防火墙的攻击，如内部网用户通过拨号直接进入**Internet**。
- ❖ 作为一种被动的防护手段，防火墙不能防范因特网上不断出现的新的威胁和攻击。
- ❖

回顾:安全模型



入侵检测系统在模型中的地位

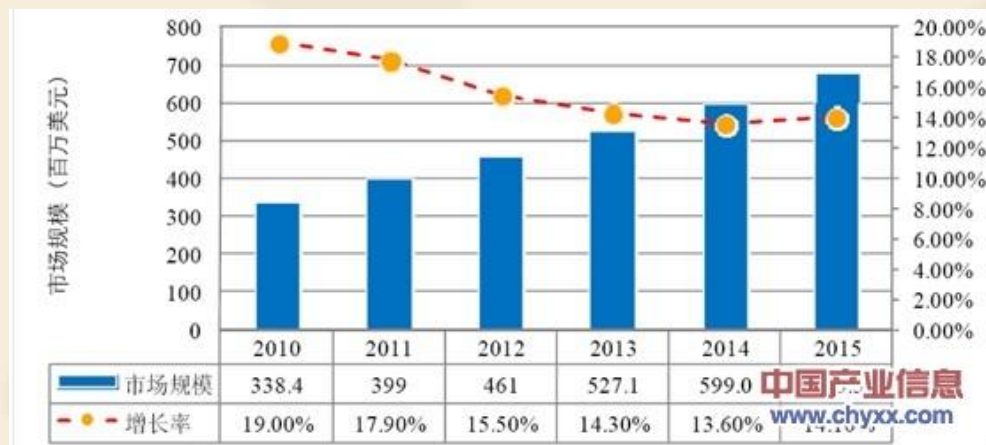


部分由入侵检测系统完成

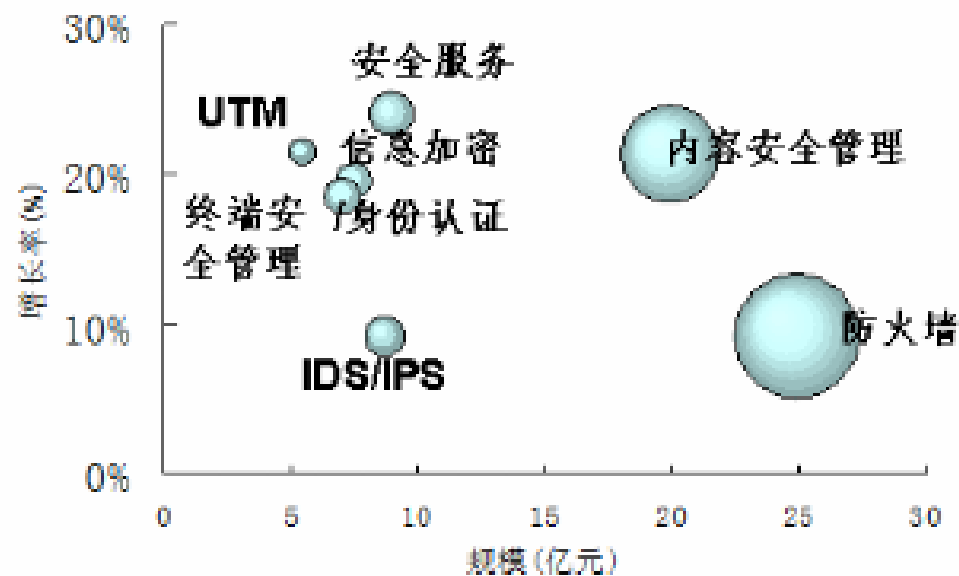
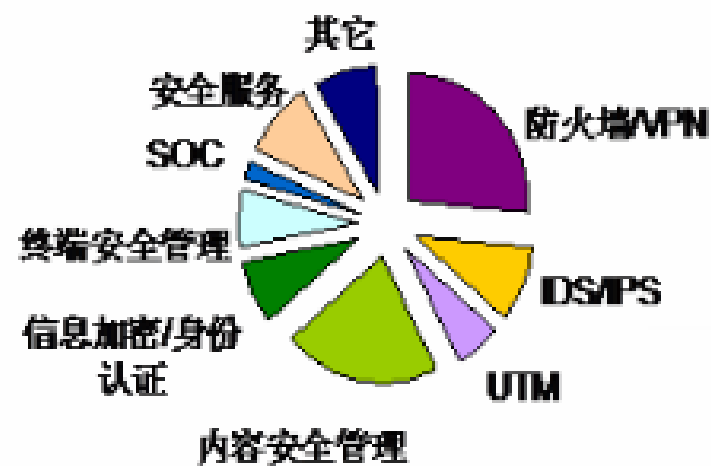
主要由入侵检测系统完成



国内信息安全产品市场规模 (2010-2015年)



国内信息安全服务市场规模 (2010-2015年)



入侵检测定义

❖ 入侵

- ❧ 指一系列试图破坏信息资源机密性、完整性和可用性的行为。
- ❧ 对信息系统的非授权访问及（或）未经许可在信息系统中进行操作。

❖ 入侵检测

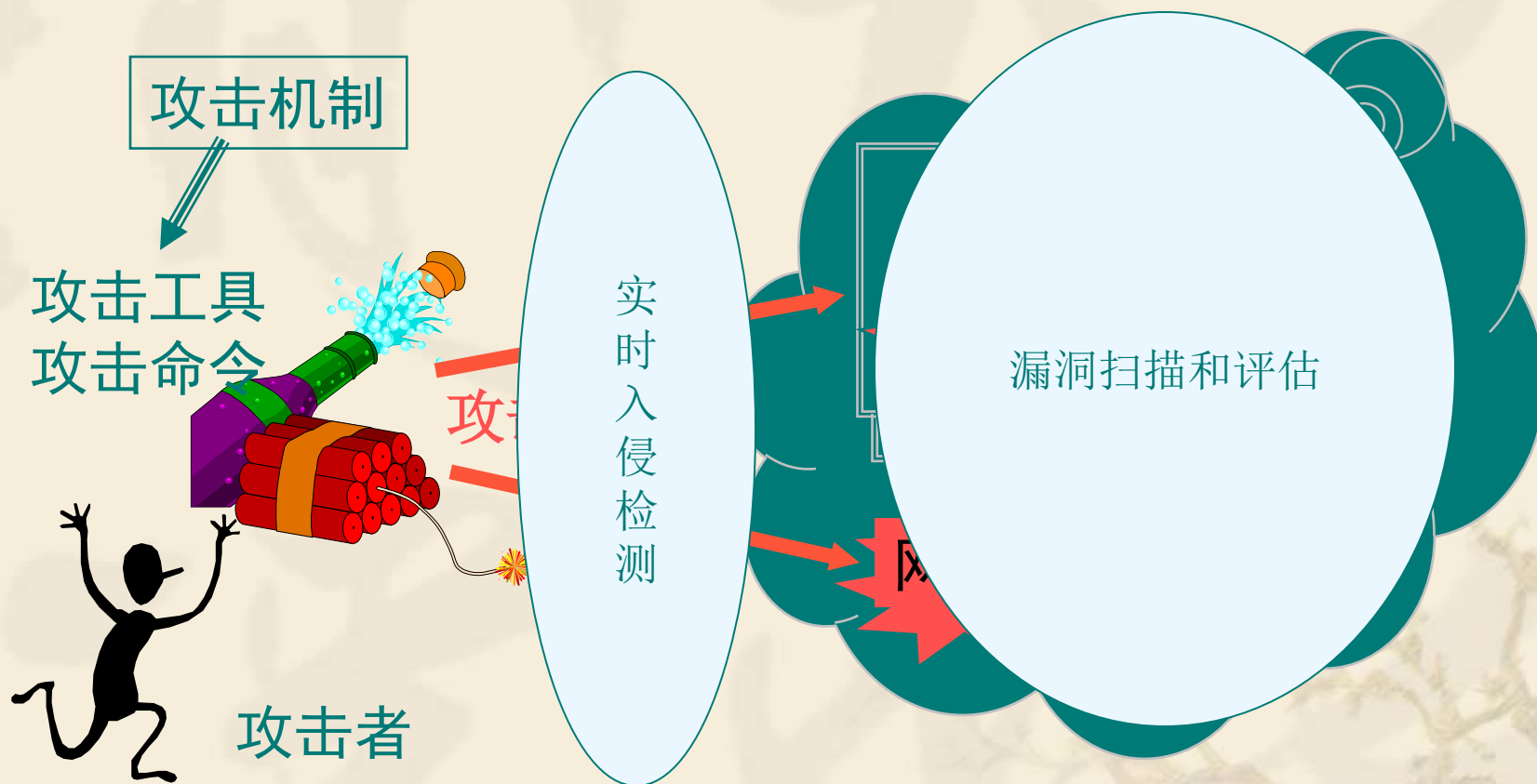
- ❧ 是通过从计算机网络系统中的若干关键节点收集信息，并分析这些信息，监控网络中是否有违反安全策略的行为或者是否存在入侵行为，是对指向计算和网络资源的恶意行为的识别和响应过程。

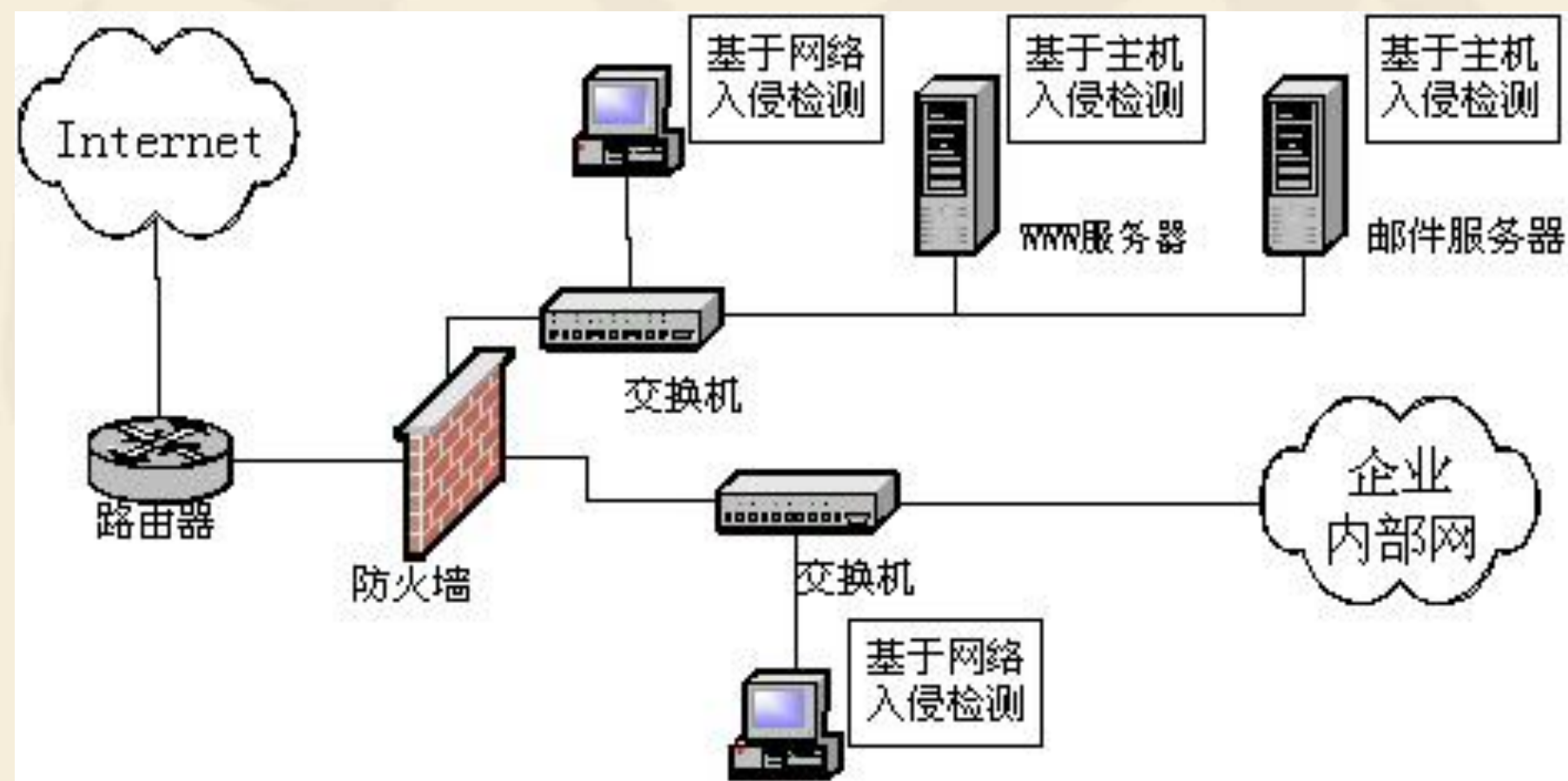
入侵检测系统

（Intrusion Detection System, IDS）

- ❧ 入侵检测系统通过监视受保护系统的状态和活动，采用异常检测或滥用检测的方式，发现非授权的或恶意的系统及网络行为，为防范入侵行为提供有效的手段，是一个完备的网络安全体系的重要组成部分。
- ❧ 入侵检测的软件与硬件的组合，是防火墙的合理补充，是防火墙之后的第二道安全闸门。
- ❖ 入侵检测的内容：试图闯入、成功闯入、冒充其他用户、违反安全策略、合法用户的泄漏、独占资源以及恶意使用。
- ❖ 防火墙是城门守卫，入侵检测系统是城内巡警

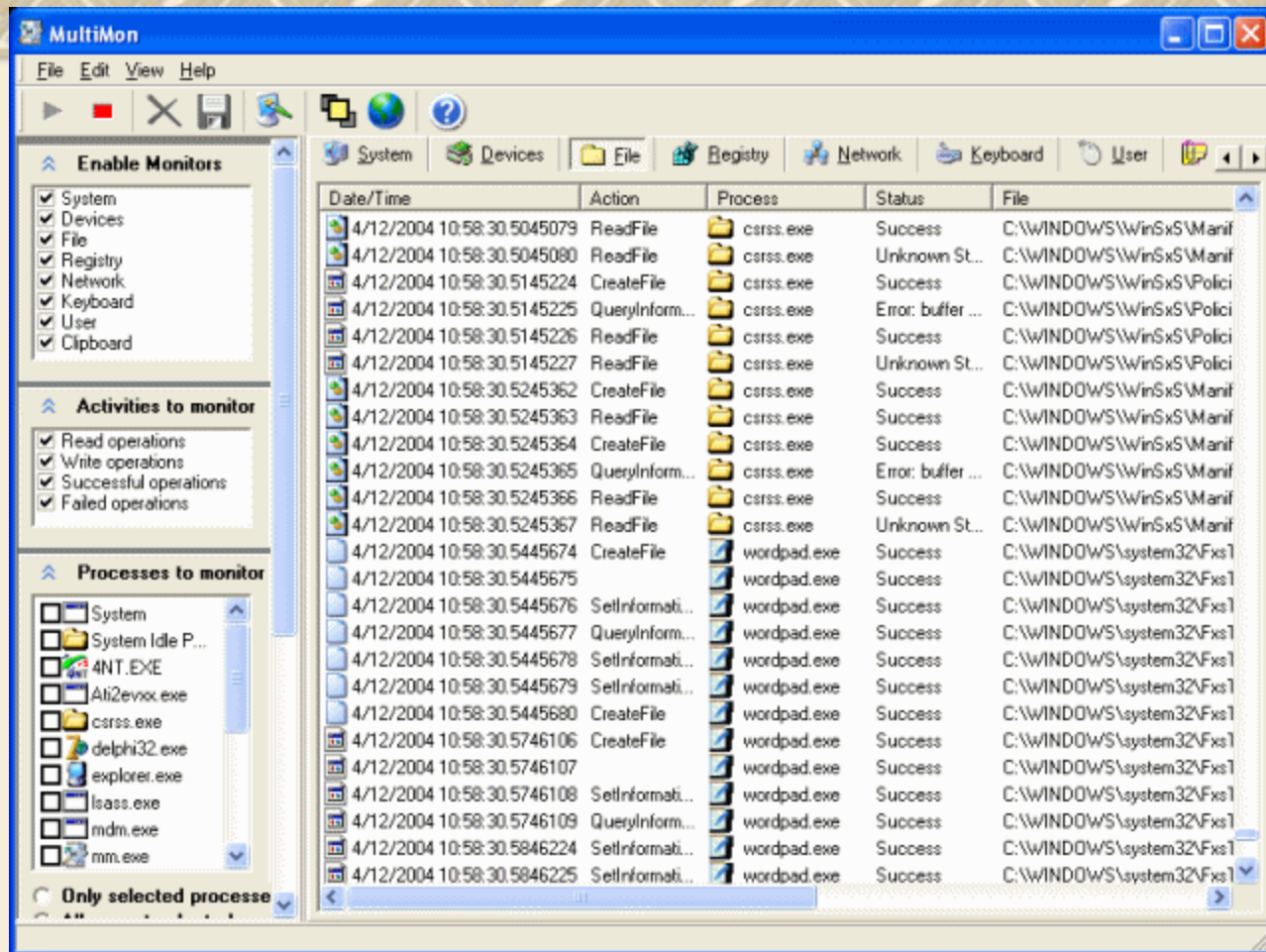
典型的IDS技术





IDS起源与发展

- ❖ 审计技术：产生、记录并检查按时间顺序排列的系统事件记录的过程。
- ❖ 审计的目标：
 - ❧— 确定和保持系统活动中每个人的责任
 - ❧— 重建事件
 - ❧— 评估损失
 - ❧— 监测系统的问题区
 - ❧— 提供有效的灾难恢复
 - ❧— 阻止系统的不正当使用
- ❖ 通常用审计日志的形式记录



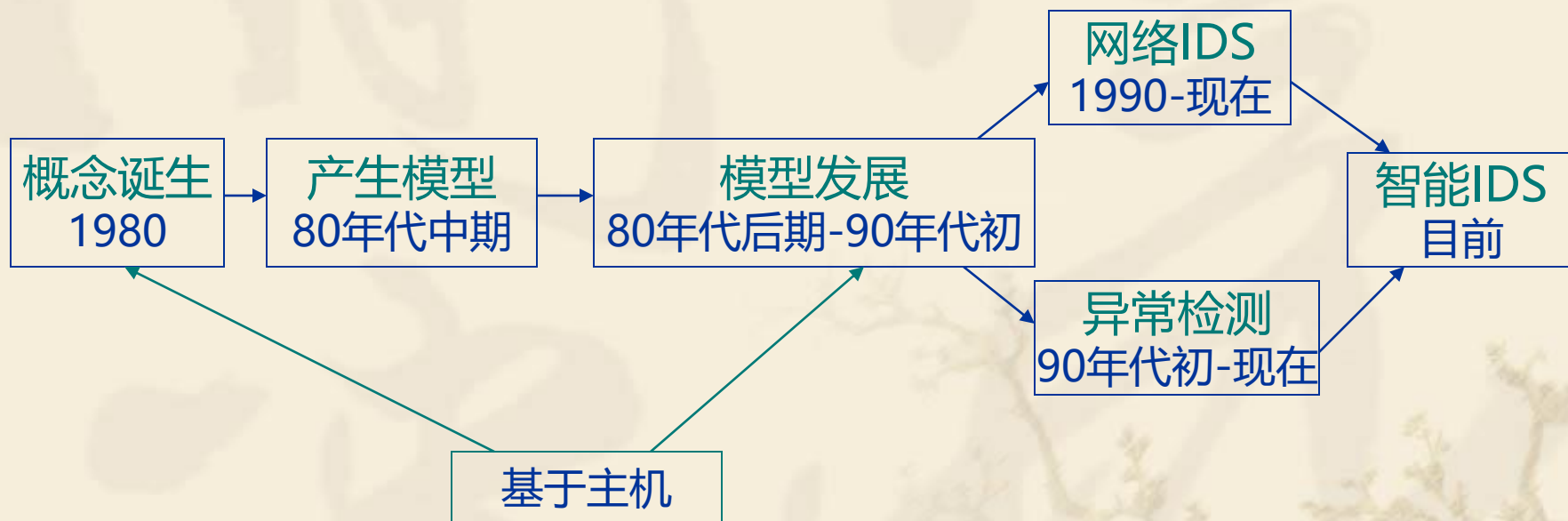
典型的日志

但是大量的日志让管理员无所适从，从中找出需要的信息和安全时间是一件非常繁琐的事情。而且需要管理员有大量的经验

IDS起源与发展

- ❖ **1980年Anderson**提出：提出了精简审计的概念，风险和威胁分类方法
- ❖ **1987年Denning**研究发展了实时入侵检测系统模型
- ❖ **IDES**入侵检测专家系统：**IDES**提出了反常活动与计算机不正当使用之间的相关性。
- ❖ **80年代**，基于主机的入侵检测
- ❖ **90年代**，基于主机和基于网络入侵检测的集成

发展历史



入侵检测流程

❖ 简单地说，入侵检测系统包括三个步骤

❧ (1) 信息收集

❧ (2) 信息分析

❧ (3) 结果处理



信息收集

- ❖ 入侵检测的效率很大程度上依赖于收集信息的可靠性和正确性。
- ❖ 入侵检测的第一步是信息收集，数据的来源可以是主机上的日志信息、变动信息，也可以是网络上的数据信息、网络流量的变化特征、用户活动的状态和行为等。
- ❖ 需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息，
 - ❧ 尽可能扩大检测范围
 - ❧ 从一个源来的信息有可能看不出疑点

信息分析

- ❖ 模式匹配
- ❖ 统计分析
- ❖ 完整性分析，往往用于事后分析

模式匹配

- ❖ 模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。

统计分析

- ❖ 统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。
- ❖ 测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生

完整性分析

- ❖ 完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性，它在发现被更改的、被安装木马的应用程序方面特别有效。

事件响应

❖ 被动的

- ☞ 给管理员发email
- ☞ 对所检测到的入侵产生报警或者文档，提醒管理员注意。

❖ 积极的

- ☞ 切断连接
- ☞ 收集入侵者的额外信息
- ☞ 对入侵者采取反击行为

10.2 入侵检测系统分类

- ❖ 基于主机的入侵检测系统
- ❖ 基于网络的入侵检测系统
- ❖ 分布式入侵检测系统

基于主机的入侵检测系统 (Host-based IDS, HIDS)

- ❖ 基于主机的入侵检测系统通常被安装在被保护的主机上，对该主机的网络实时连接以及系统审计日志进行分析和检查，当发现可疑行为和安全违规事件时，系统就会向管理员报警，以便采取措施。这些受保护的主机可以是Web服务器、邮件服务器、DNS服务器等关键主机设备。

主机的数据源

❖ 操作系统事件日志

❖ 应用程序日志

∞— 系统日志

∞— 关系数据库

∞— **Web**服务器

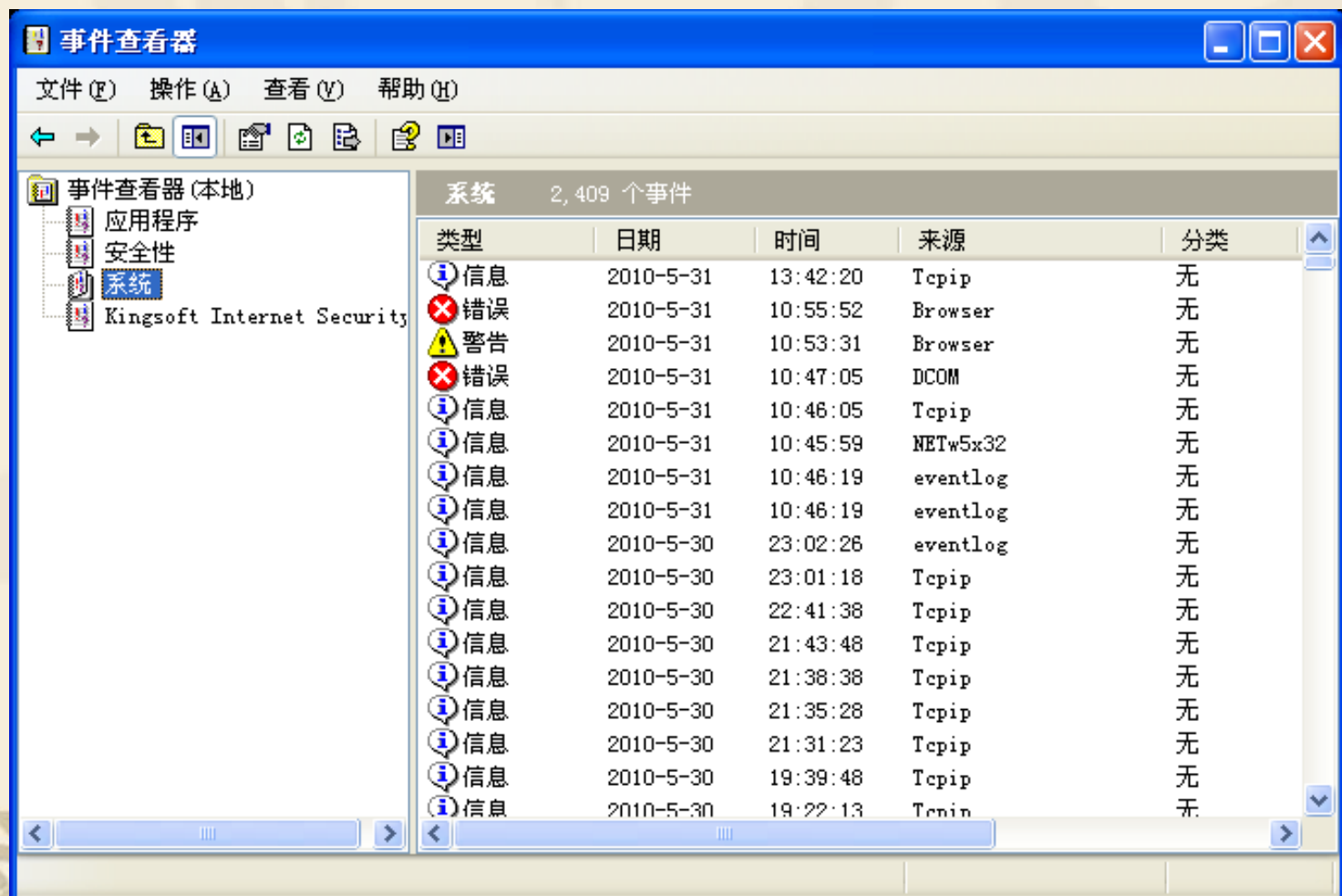
Linux的日志文件:

- /var/log/wtmp: 用户登录历史
- /var/run/utmp: 当前用户登录日志。
- /var/log/messages: 内核消息日志
- /var/log/pacct: 进程审计日志。
- ...还有其他一些日志文件, 位于var/log目录下

Windows的日志文件:

- Sysevent.evt
- Secevent.evt
- Appevent.evt
- ...

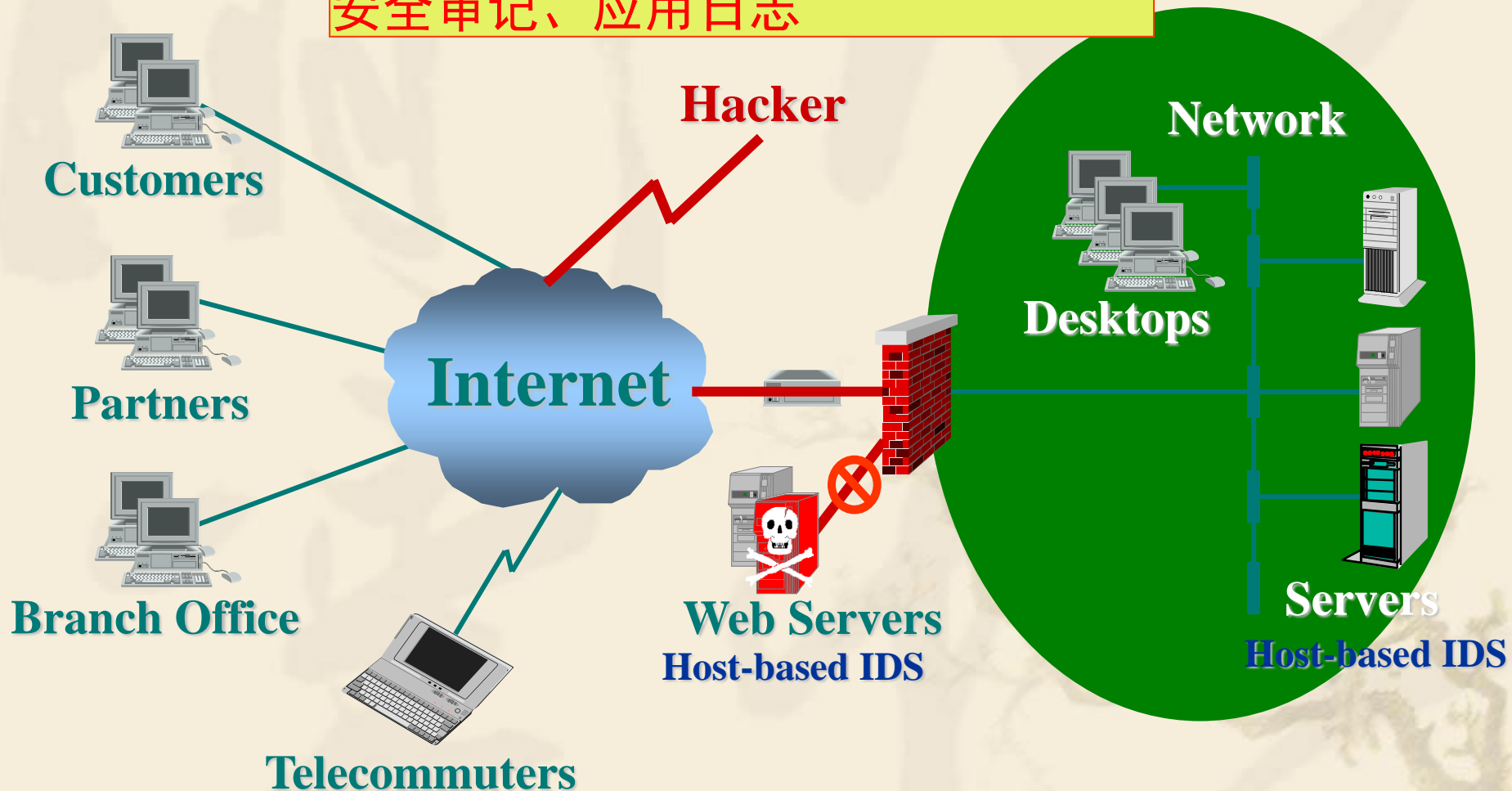
- ❖ Windows有自带的日志系统，可以通过“事件查看器”来进行查阅。
- ❖ 开始—设置—控制面板—管理工具—事件查看器



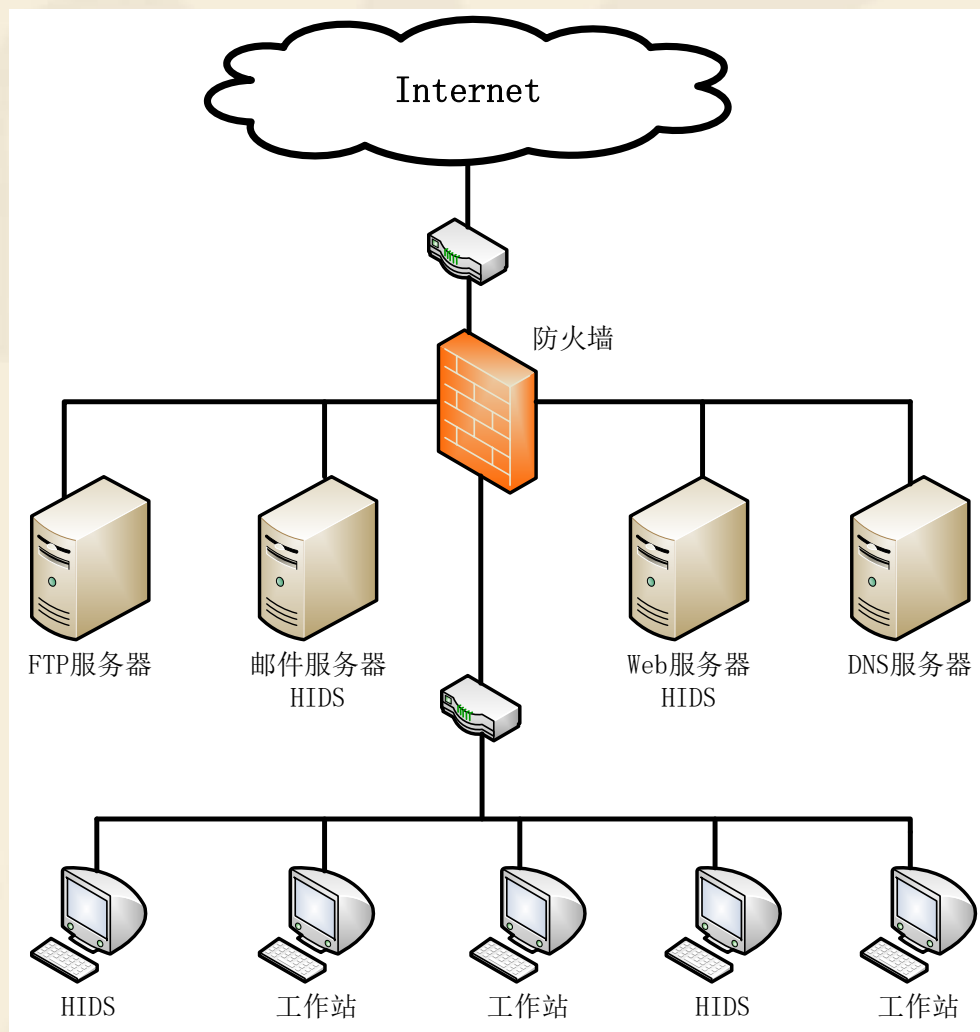
Host-based 入侵检测

检测内容：

系统调用、端口调用、系统日志、
安全审记、应用日志



HIDS在网络中的部署



基于主机的技术面临的问题

- ❖ 性能：降低是不可避免的
- ❖ 糟糕的审计源

基于网络的入侵检测系统

- ❖ 安装在需要保护的网段中，实时监视网段中传输的各种数据包，并对这些数据包进行分析和检测。如果发现入侵行为或可疑事件，入侵检测系统就会发出警报甚至切断网络连接。

网络监听

- ❖ 在一个共享式网络，可以听取所有的流量是一把双刃剑
 - ❧ 管理员可以用来监听网络的流量情况
 - ❧ 开发网络应用的程序员可以监视程序的网络情况
 - ❧ 黑客可以用来刺探网络情报
- ❖ 目前有大量商业的、免费的监听工具，俗称嗅探器(**sniffer**)

Sniffem

File View Capture Tools Mode Filter Help

Filename: C:\My Documents\Bufferdecoding.sem

Capturing

Packet Decoding

MAC Header

IPv4 Header

Version = 4

Header Length = 20 bytes

Type Of Service (0x00)

Total Length = 69

Identification = 16389

Flags (0x0000)

Time To Live = 64

Protocol = 6 (TCP)

Header Checksum = 65053

IP Src = 212.24.193.84

IP Dest = 212.24.211.10

TCP Header

Port Src = 1038

Port Dest = 119 (nntp)

Seq number = 0x0011B7F3

Ack number = 0x11B37680

Header Length = 5

Flags (0x018)

Windows Size = 8192

Checksum = 53781

Urgent Pointer = 0

Data = 29 bytes

Nr.:	IP Adr.: src	IP Adr.: dest	Fr...	Protocol	MAC Adr.: dest	MAC Adr.:
1	-	-	ARP	ARP->request	FF-FF-FF-FF-FF-FF	44-45-53-5
2	212.24.193.84	212.24.211.10	IP	TCP	20-53-52-43-00-00	44-45-53-5
3	212.24.211.10	212.24.193.84	IP	TCP	44-45-53-54-00-00	20-53-52-4
4	212.24.193.84	212.24.211.10	IP	TCP	20-53-52-43-00-00	44-45-53-5
5	212.24.193.84	212.24.211.10	IP	TCP	20-53-52-43-00-00	44-45-53-5
6	212.24.211.10	212.24.193.84	IP	TCP	44-45-53-54-00-00	20-53-52-4
7	212.24.193.84	212.24.211.10	IP	TCP	20-53-52-43-00-00	44-45-53-5
8	212.24.211.10	212.24.193.84	IP	TCP	44-45-53-54-00-00	20-53-52-4
9	212.24.211.10	212.24.193.84	IP	TCP	44-45-53-54-00-00	20-53-52-4
10	212.24.193.84	212.24.211.10	IP	TCP	20-53-52-43-00-00	44-45-53-5
11	212.24.211.10	212.24.193.84	IP	TCP	44-45-53-54-00-00	20-53-52-4

Packet View

0001

20 53 52 43 00 00 44 45 53 54 00 00 08 00 45 00

0002

00 45 40 05 00 00 40 06 FE 1D D4 18 C1 54 D4 18

0003

D3 0A 04 0E 00 77 00 11 B7 F3 11 B3 76 80 50 18

0004

20 00 D2 15 00 00 47 52 4F 55 50 20 61 6C 74 2E

0005

66 61 6E 2E 63 75 6C 74 2D 64 65 61 64 2D 63 6F

0006

77 0D 0A

668 / 2000

Sniff-em

Dial-Up Adapter

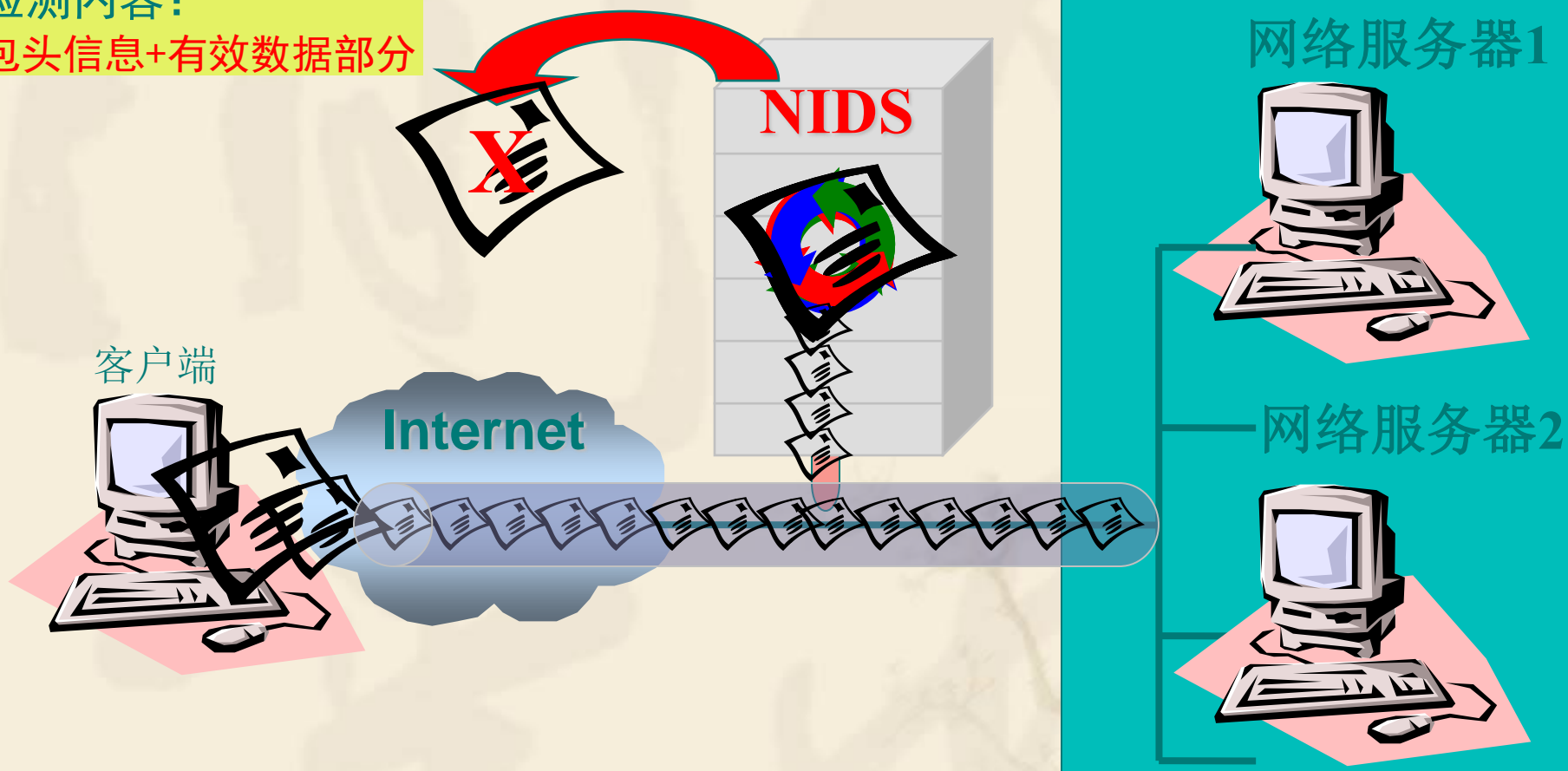
Filter: OFF

Process Priority : Normal

基于网络入侵检测系统工作原理

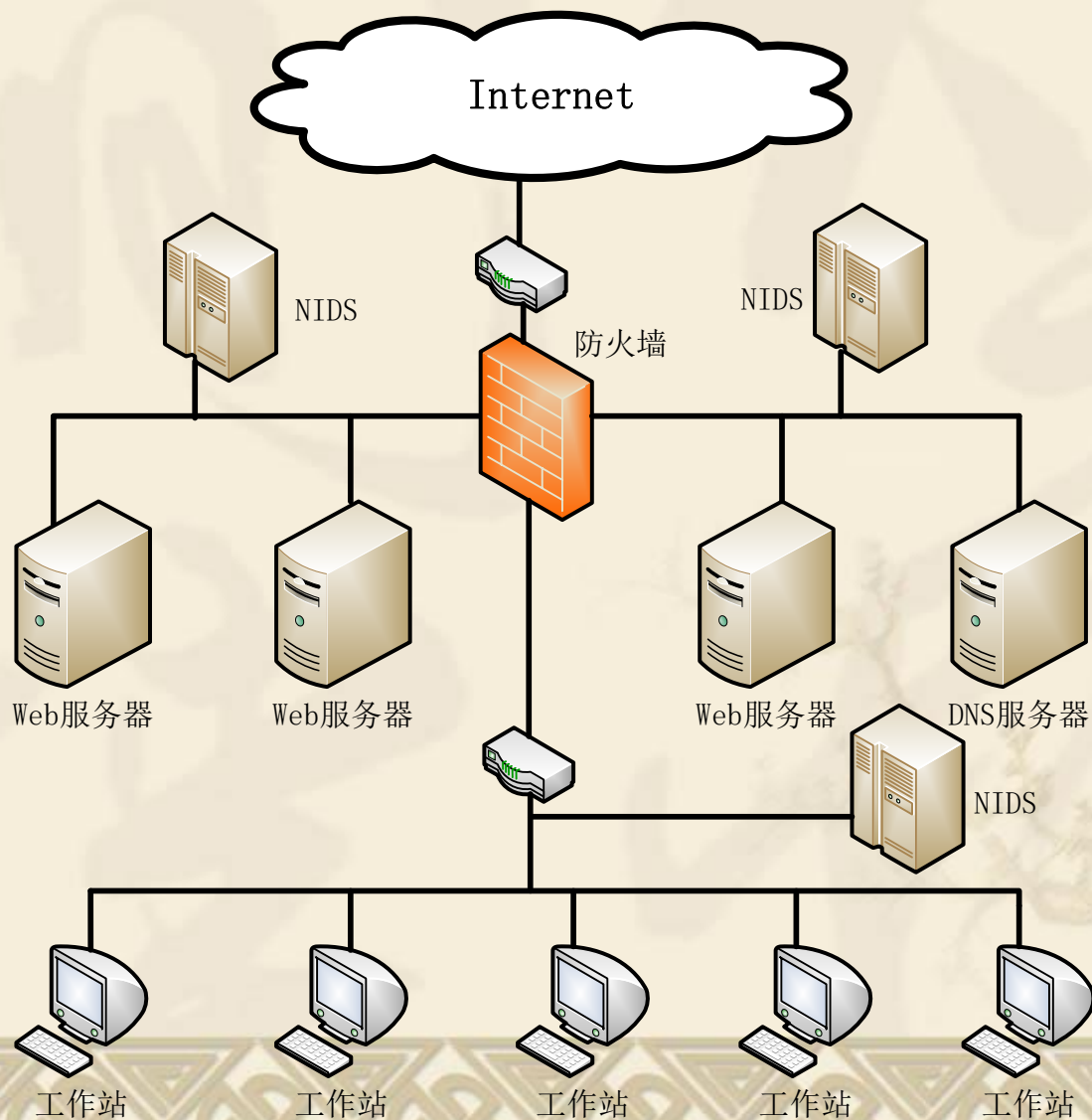
检测内容:

包头信息+有效数据部分

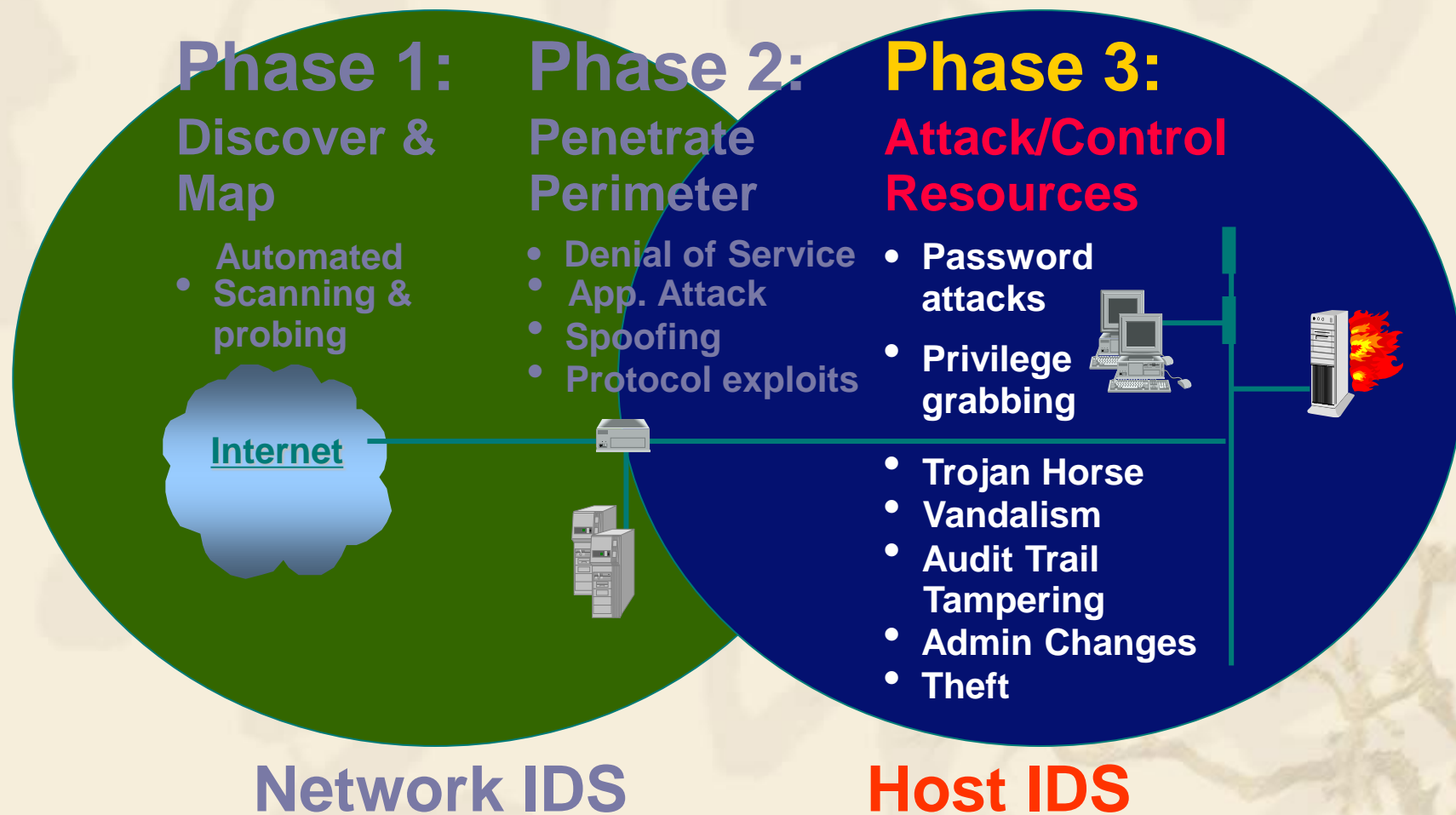


数据包=包头信息+有效数据部分

NIDS在网络中的部署



黑客入侵的过程和阶段



基于主机与基于网络IDS

Top 10 Attack Families	Example	Network	Host
Denial of Service	SynFlood Attack	Best solution	<i>Poor Strategy</i>
Scanning and Probing	Satan	Best solution	Good solution
Password Attacks	L0phtCrack	<i>Poor Strategy</i>	Good solution
Privilege Grabbing	Buffer Overflow		Best solution
Hostile Code Insertion	Malformed URL	<i>Poor Strategy</i>	Best solution
Vandalism	Melissa Virus	<i>Poor Strategy</i>	Best solution
Proprietary Data Theft	Targeting Key Sources		Good solution
Fraud, Waste, & Abuse	BO2K	<i>Poor Strategy</i>	Good solution
Audit Trail Tampering	Covering a Trail		Best solution
Security Admin. Attacks	Backdoor insert		Best solution

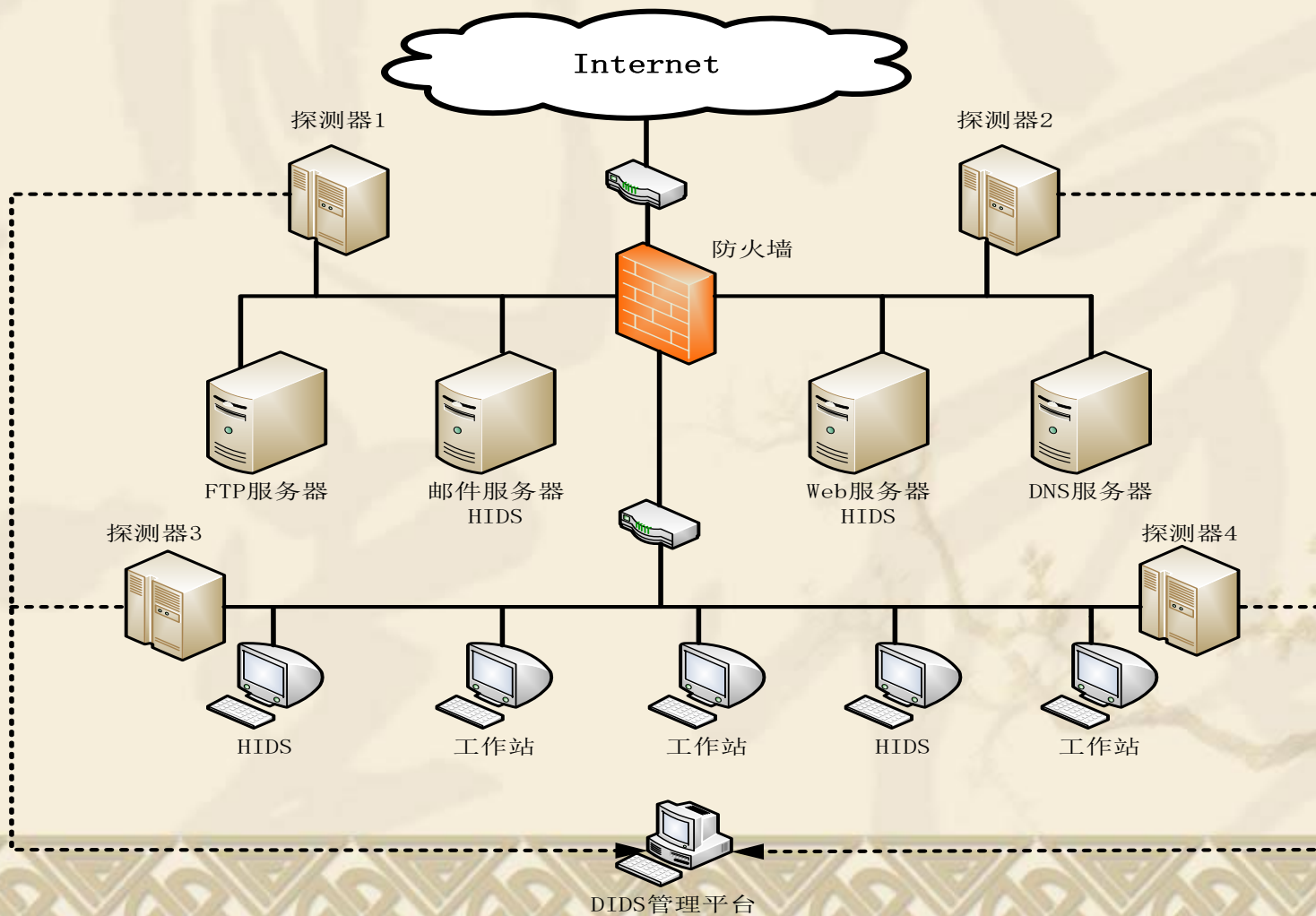
分布式入侵检测系统

❖ 网络系统结构的复杂化和大型化，使得：

- ❧ 系统的弱点或漏洞分散在网络中的各个主机上，这些弱点有可能被入侵者用来攻击网络，而仅依靠一个主机或网络的入侵检测系统很难发现入侵行为
- ❧ 入侵行为不再是单一的行为，而是表现出相互协作入侵的特点，例如分布式拒绝服务攻击
- ❧ 入侵检测所依靠的数据来源分散化，使得收集原始的检测数据变得比较困难

DIDS在网络中的部署

- ❖ 分布式入侵检测系统（DIDS）的目标是既能检测网络入侵行为，又能检测主机的入侵行为。



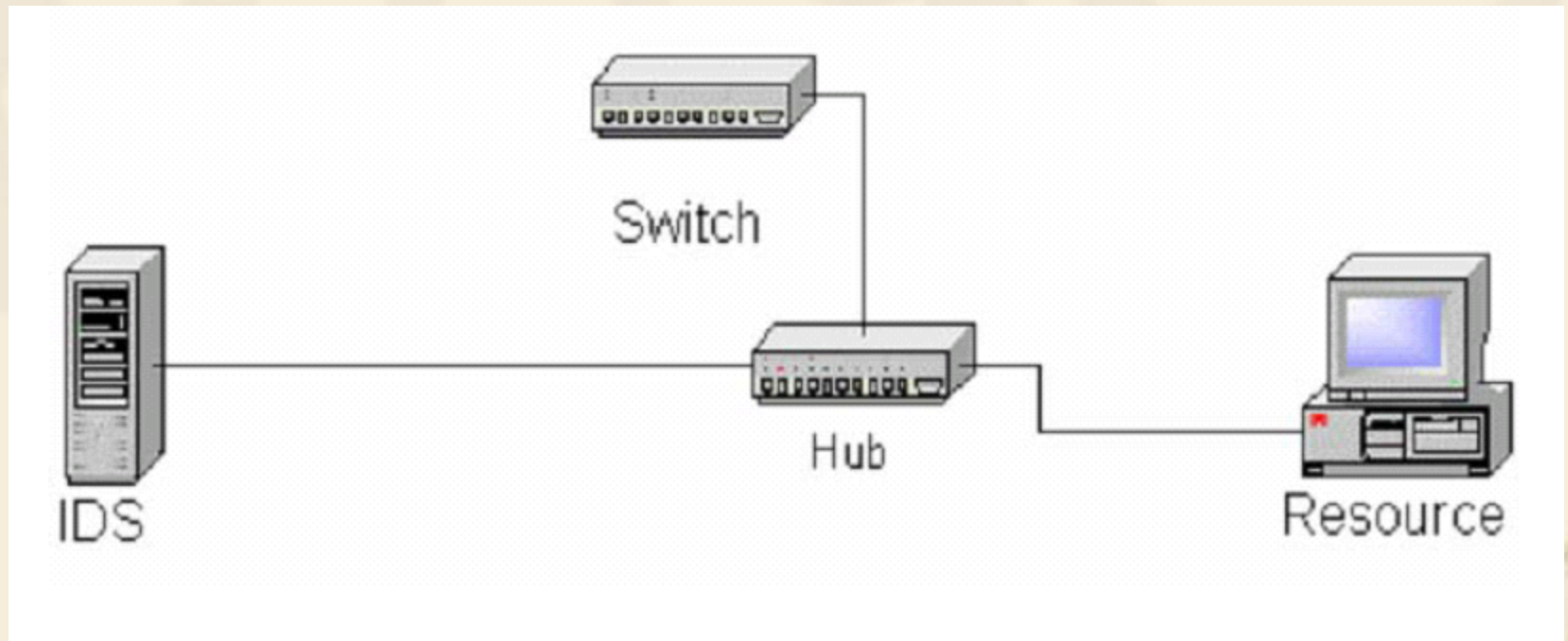
检测器的位置

- ❖ 放在防火墙之外
 - ❧ 无法检测到某些攻击，但可以看到自己的站点和防火墙暴露在多少种攻击之下
- ❖ 检测器在防火墙内
 - ❧ 少一些干扰，减少误报警；减少对检测器的攻击；
- ❖ 防火墙内外都有检测器
 - ❧ 各有优势
- ❖ 检测器的其他位置
 - ❧ 高价值的地方
 - ❧ 有大量不稳定雇员的地方
 - ❧ 已被当作攻击目标的子网

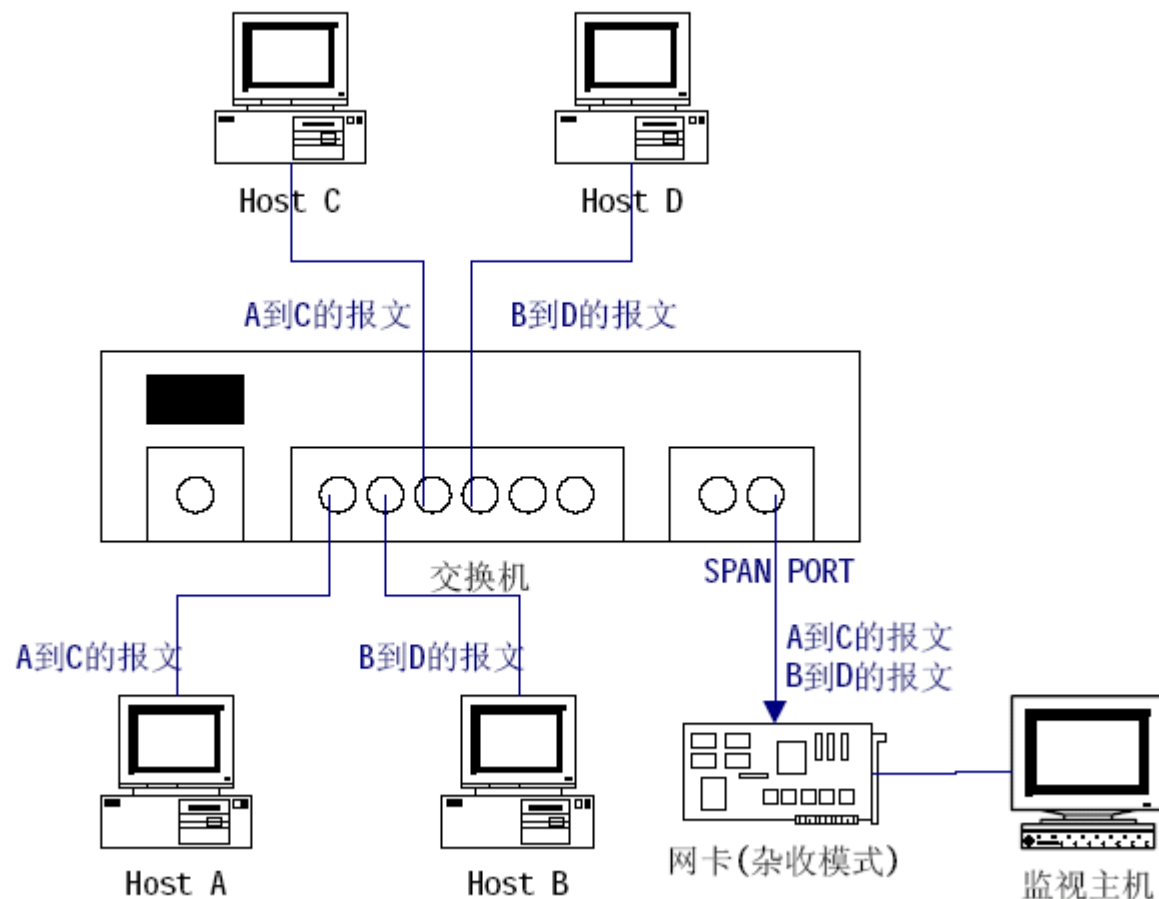
基于网络的技术面临的问题

- ❖ 在某些采用交换技术的网络环境中，交换机使得网络报文不能在子网内任意广播，只能在设定的虚网（VLAN）内广播，这就使得进行网络监听的主机只能提取到本虚网内的数据，监视范围大为减少，监视的能力也受到削弱。

使用HUB



使用交换机的镜像端口

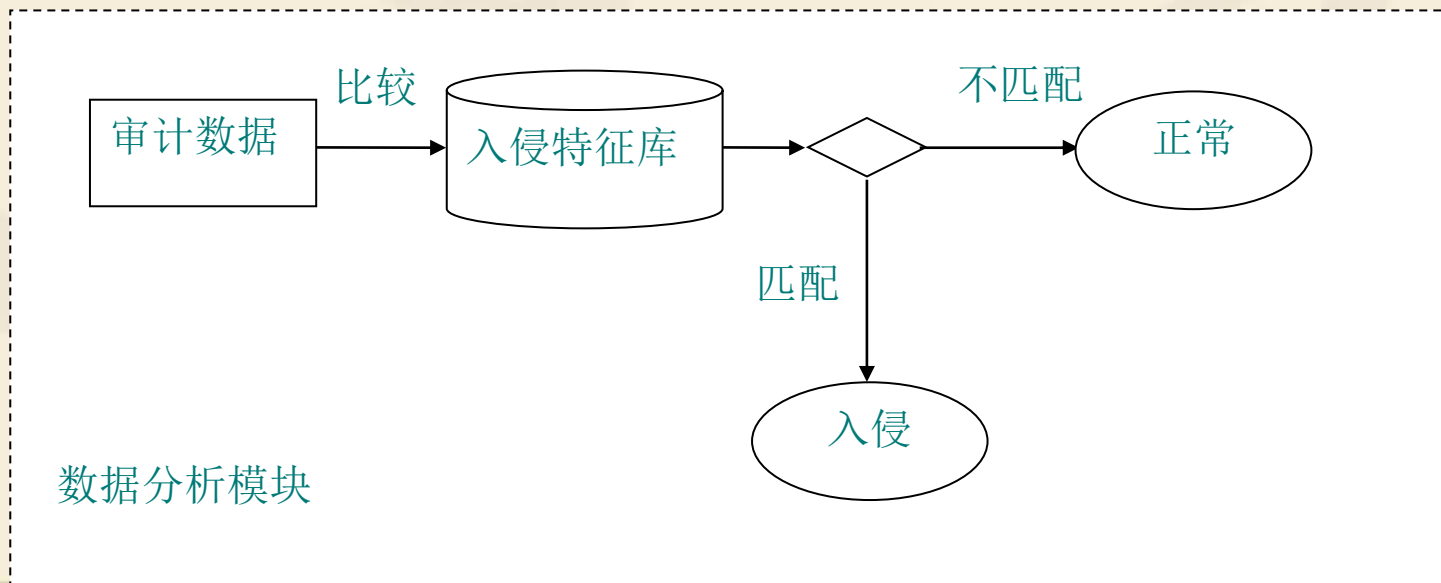


10.2.3 入侵检测方法

- ❖ 滥用检测（Misuse Detection）
- ❖ 异常检测（Anomaly Detection）

滥用检测

- ❖ 滥用检测也被称为误用检测或者基于特征的检测。这种方法首先直接对入侵行为进行特征化描述，建立某种或某类入侵特征行为的模式，如果发现当前行为与某个入侵模式一致，就表示发生了这种入侵。



滥用检测特点

- ❖ 前提：所有的入侵行为都有可被检测到的特征
- ❖ 攻击特征库：当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵
- ❖ 过程
 - 监控 → 特征提取 → 匹配 → 判定
- ❖ 无法检测出新型攻击
- ❖ 指标：误报低、漏报高
 - ∞ 误报：将正常活动定义为入侵
 - ∞ 漏报：未能检测出真正的入侵行为

异常检测

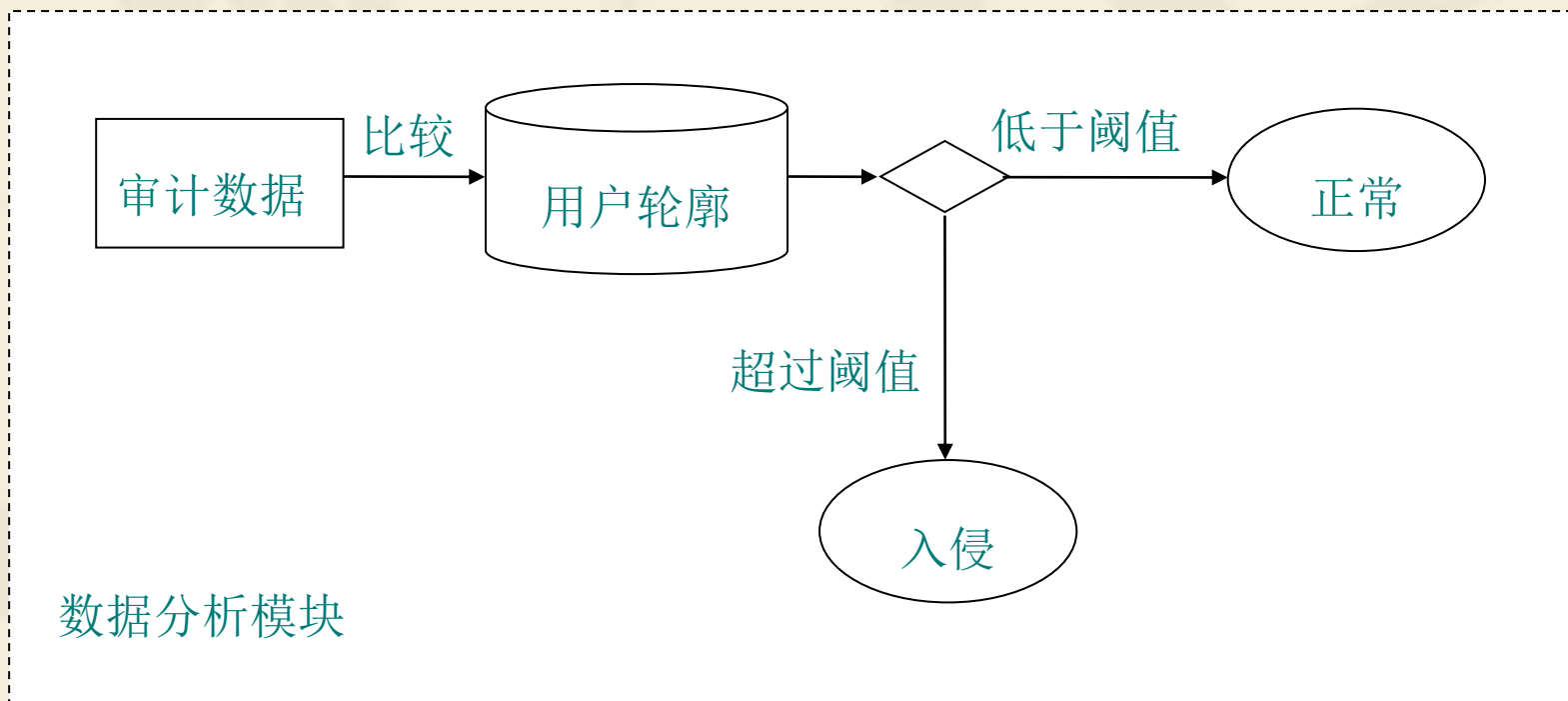
❖ 基本思想:

❧ 任何人的正常行为都是有一定规律的，并且可以通过分析这些行为产生的日志信息（假定日志信息足够完全）总结出一些规律，而入侵和滥用行为则通常与正常行为会有比较大的差异，通过检查出这些差异就可以检测出入侵。

❖ 主要方法

❧ 为正常行为建立一个规则集，称为正常行为模式，也称为正常轮廓（normal profile），也被称为“用户轮廓”，当用户活动和正常轮廓有较大偏离的时候认为异常或入侵行为。这样能够检测出非法的入侵行为甚至是通过未知攻击方法进行的入侵行为，此外不属于入侵的异常用户行为（滥用自己的权限）也能被检测到。

异常检测方法的基本流程



异常检测特点

- ❖ 前提：入侵是异常活动的子集
- ❖ 用户轮廓(Profile): 通常定义为各种行为参数及其阈值的集合，用于描述正常行为范围
- ❖ 过程
 - 监控 → 量化 → 比较 → 判定
 - ↓
 - 修正
- ❖ 指标:漏报率低,误报率高

异常检测特点

- ❖ 异常检测系统的效率取决于用户轮廓的完备性和监控的频率
- ❖ 因为不需要对每种入侵行为进行定义，因此能有效检测未知的入侵
- ❖ 难点在于如何构建用户轮廓
 - ∞ 机器学习、人工智能

异常检测使用的一些方法

- ❖ 统计异常检测
- ❖ 基于特征选择异常检测
- ❖ 基于贝叶斯推理异常检测
- ❖ 基于贝叶斯网络异常检测
- ❖ 基于模式预测异常检测
- ❖ 基于神经网络异常检测
- ❖ 基于贝叶斯聚类异常检测
- ❖ 基于机器学习异常检测
- ❖ 基于数据挖掘异常检测
- ❖

两种方式比较

- ❖ 误用检测（Misuse Detection）
 - ∞ 建立起已知攻击的规则库
 - ∞ 实时行为与规则匹配
 - ∞ 优点：检测准确率高
 - ∞ 缺点：无法检测未知入侵
- ❖ 异常检测（Anomaly Detection）
 - ∞ 建立用户或系统的正常行为模式
 - ∞ 不符合正常模式的行为活动为入侵
 - ∞ 优点：能够检测出未知的入侵
 - ∞ 缺点：难以建立正常行为模式

入侵检测的发展方向

❖ 工业界

- ❧ 主要的研究内容是如何通过优化检测系统的算法来提高入侵检测系统的综合性能与处理速度，以适应千兆网络的需求。

❖ 学术界

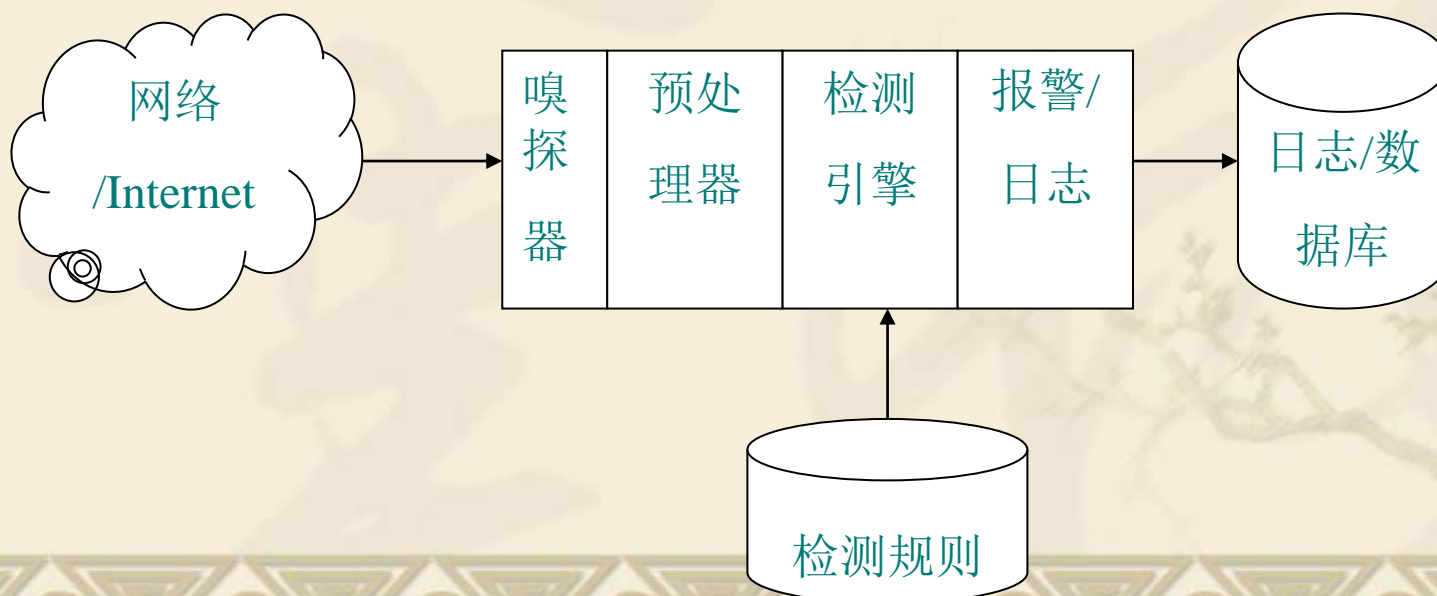
- ❧ 主要通过引入各种智能计算方法，使入侵检测技术向智能化方向发展。
 - ❖ 人工神经网络技术
 - ❖ 人工免疫技术
 - ❖ 数据挖掘技术

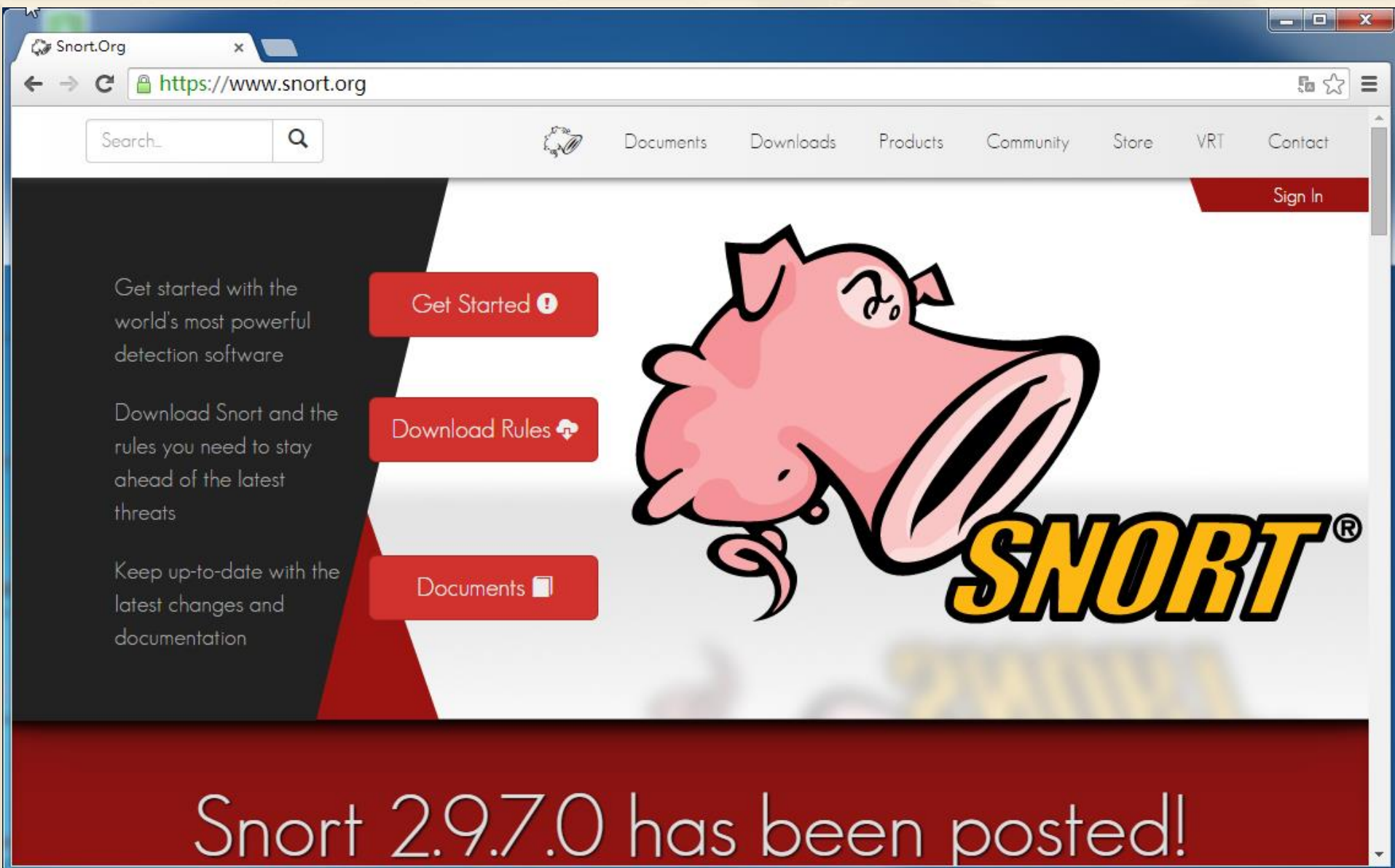
入侵检测系统的局限性

- ❖ 误报和漏报的矛盾
- ❖ 隐私和安全的矛盾
- ❖ 被动分析与主动发现的矛盾
- ❖ 海量信息与分析代价的矛盾
- ❖ 功能性和可管理性的矛盾
- ❖ 单一产品与复杂网络应用的矛盾

网络入侵检测系统Snort

- ❖ Snort是最流行的免费NIDS。
- ❖ Snort是基于滥用/异常检测的IDS，使用规则的定义来检查网络中的问题数据包。
- ❖ Snort由以下几个部分组成：数据包嗅探器、预处理器、检测引擎、报警输出模块





Snort IDS Console - Microsoft Internet Explorer

Address: <https://www.snort.org/>

Snort IDS Console Unfilter Refresh every 30 secs View alerts since 6 AM or on

Alert Information			Sensors			Top Sources			Top Targets			Top Target Ports			
	#	%	Sensor	Sigs	Alerts	IP Address	Sigs	Alerts	IP Address	Sigs	Alerts	TCP	#	UDP	#
Signatures:	62			19	482	192.168.1.1	6	186	192.168.1.1	6	186	80	513	1434	1,259
TCP Alerts View :	1,126	42%		13	177	192.168.1.1	5	5	192.168.1.1	5	5	139	108	53	242
UDP Alerts View :	1,523	57%		11	240	192.168.1.1	3	21	192.168.1.1	3	24	443	122	177	9
ICMP Alerts View :	0	0%		11	131	192.168.1.1	2	108	192.168.1.1	2	352	1433	23	111	6
Total Alerts View :	2,649	100%		9	298	192.168.1.1	2	92	192.168.1.1	2	92	3389	19	69	2

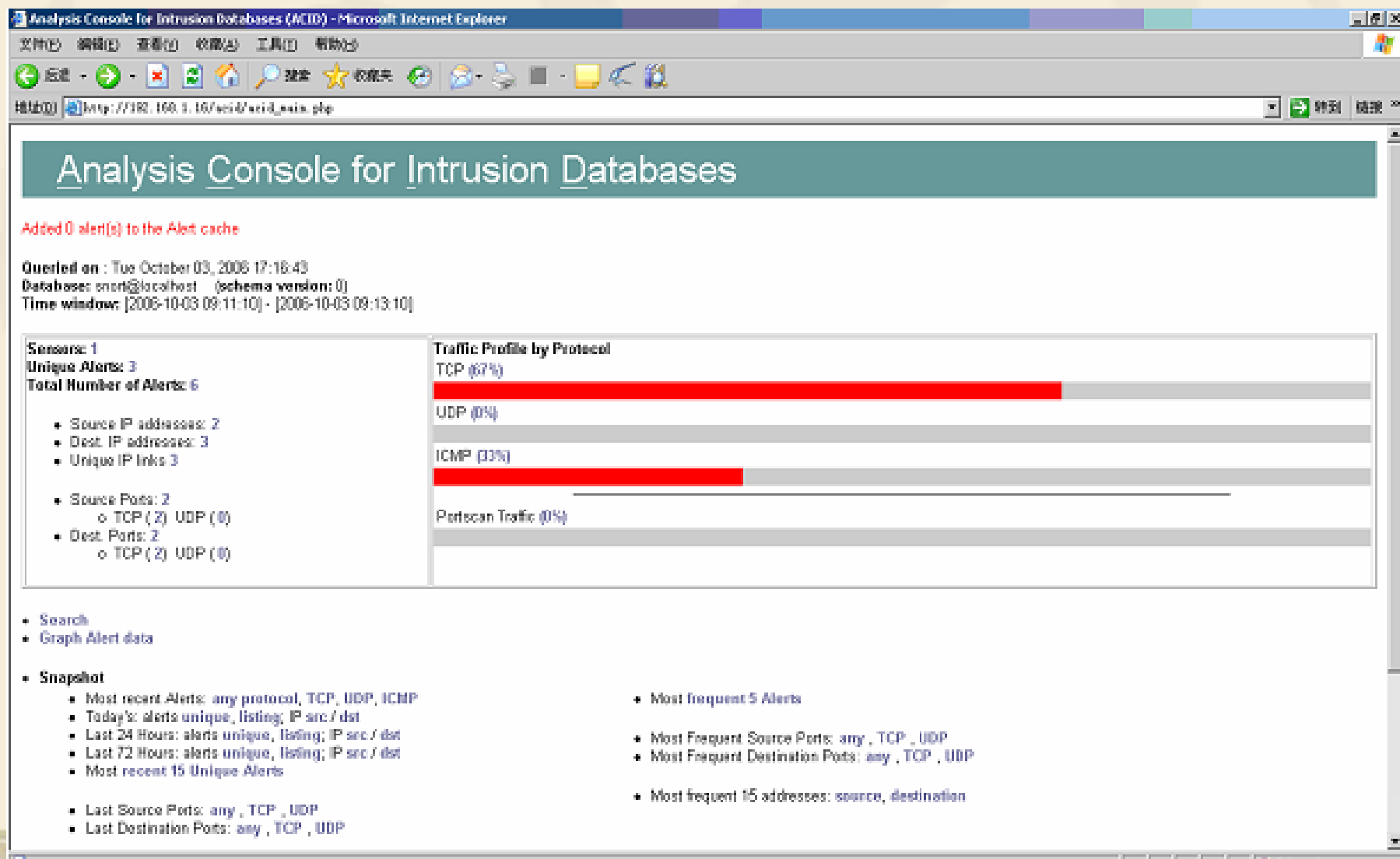
Alert Overview by Signature

Earliest Alert: 2004-12-29 06:01:03
Latest Alert: 2004-12-29 15:57:12

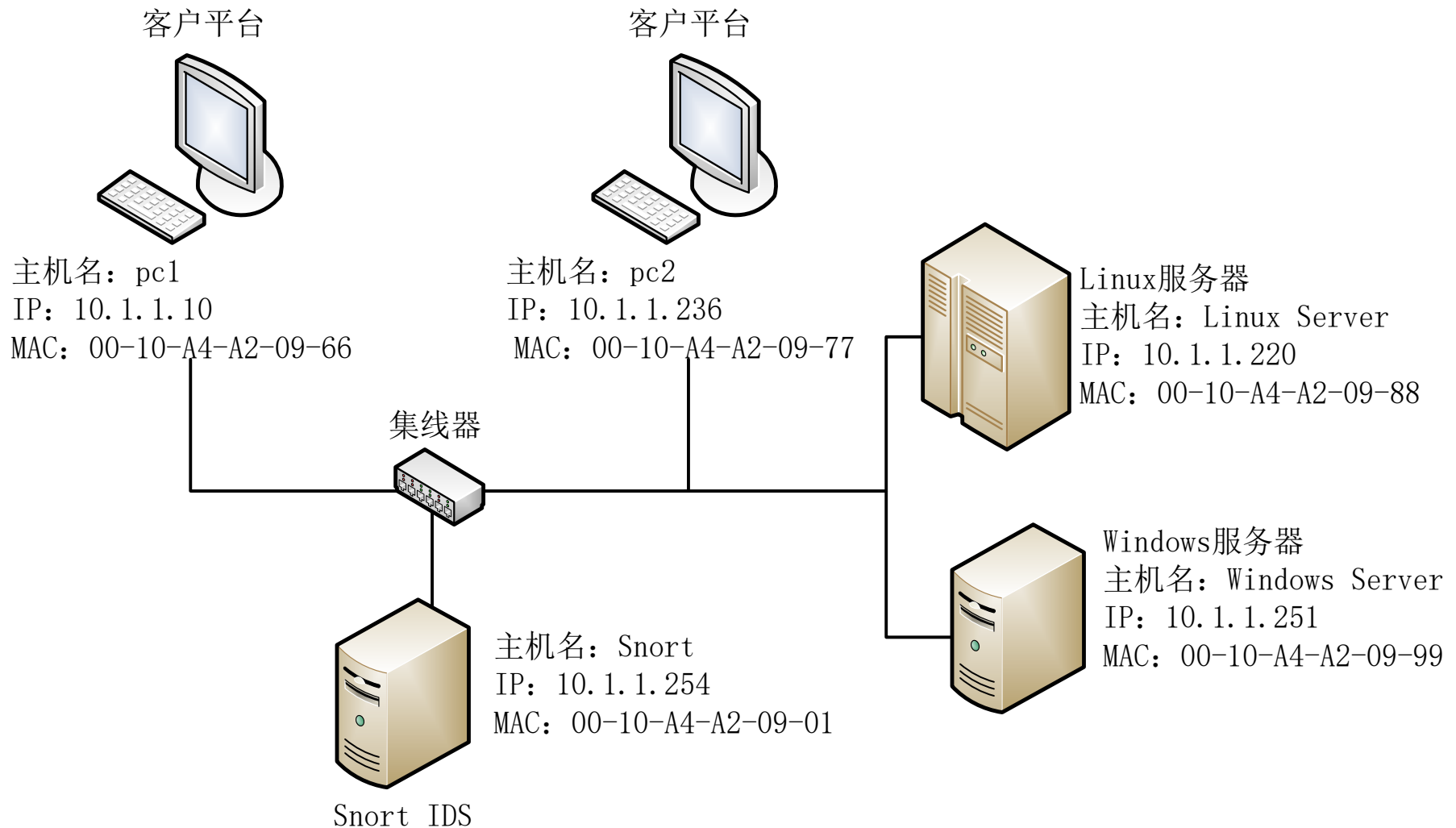
Signatures					
Prio	Signature	# Sensors	# Alerts	# Srcs	# Dests
1	WEB-MISC cross site scripting attempt [sid 1497]	2	353	2	2
1	P2P Fasttrack kazaa/morpheus traffic [sid 1699]	2	145	3	49
1	MS-SQL/SMB raiseerror possible buffer overflow [sid 1386]	2	117	1	1
1	WEB-MISC NetObserve authentication bypass attempt [sid 2441]	1	110	1	1
1	MS-SQL/SMB xp_cmdshell program execution [sid 681]	2	33	1	1
1	WEB-MISC PCT Client Hello overflow attempt [sid 2515]	2	25	1	8
1	MS-SQL xp_cmdshell - program execution [sid 687]	1	17	2	1
1	MS-SQL/SMB xp_reg* registry access [sid 689]	2	12	1	1
1	MS-SQL/SMB sp_password password change [sid 677]	2	10	1	1
1	MS-SQL/SMB sp_delete_alert log file deletion [sid 678]	2	10	1	1
1	MS-SQL sp_start_job - program execution [sid 673]	2	6	1	1
1	MS-SQL sa login failed [sid 688]	1	5	1	1

Done Internet

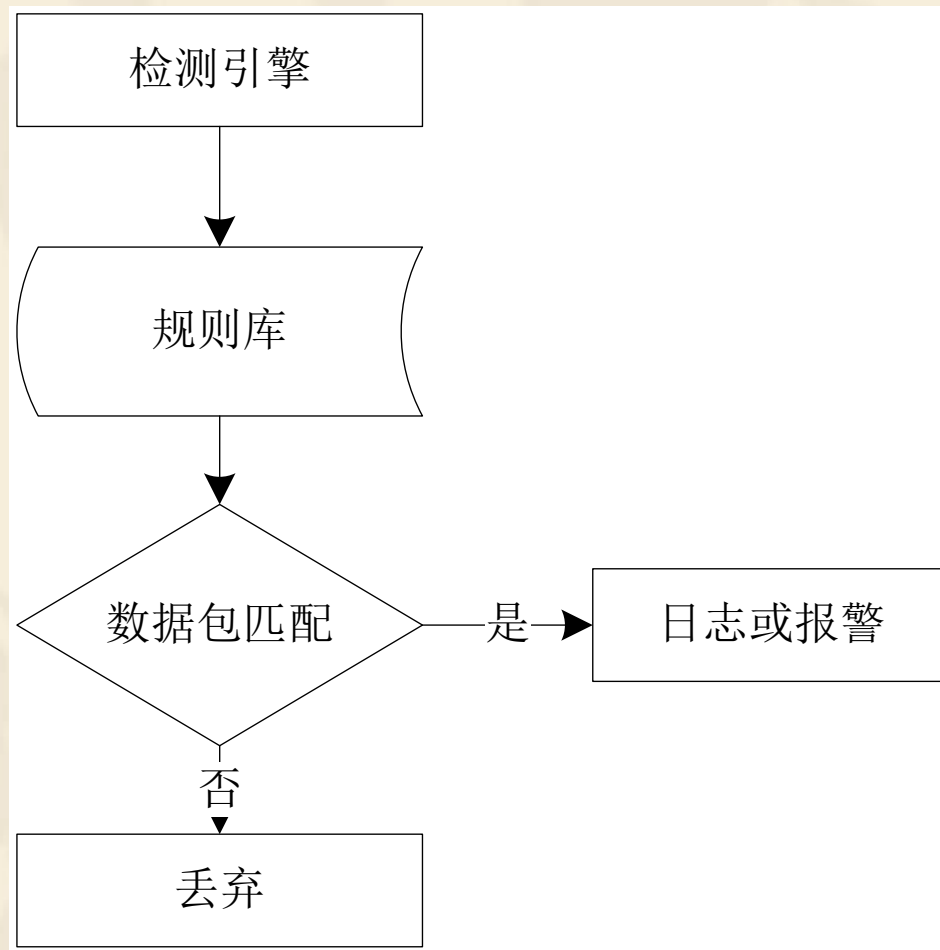
Snort的检测报告



Snort在网络中的应用



Snort的检测流程



Popular IDS Products

- RealSecure



- www.iss.net/securing_e-business/security_products/intrusion_detection/

- Cisco Secure IDS

Cisco Intrusion Detection



- www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/

- Network ICE



- www.networkice.com

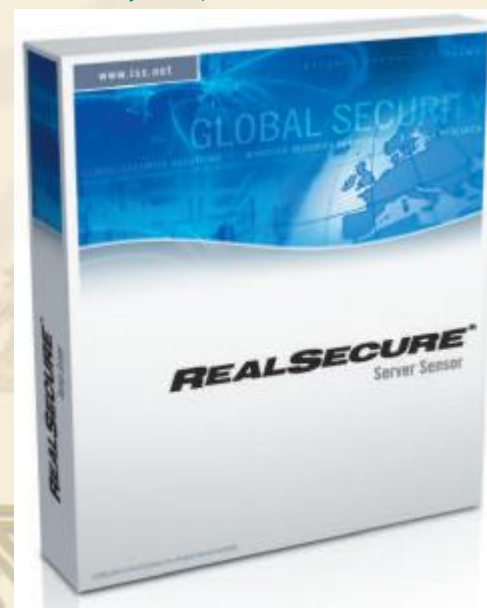
- Snort

- www.snort.org

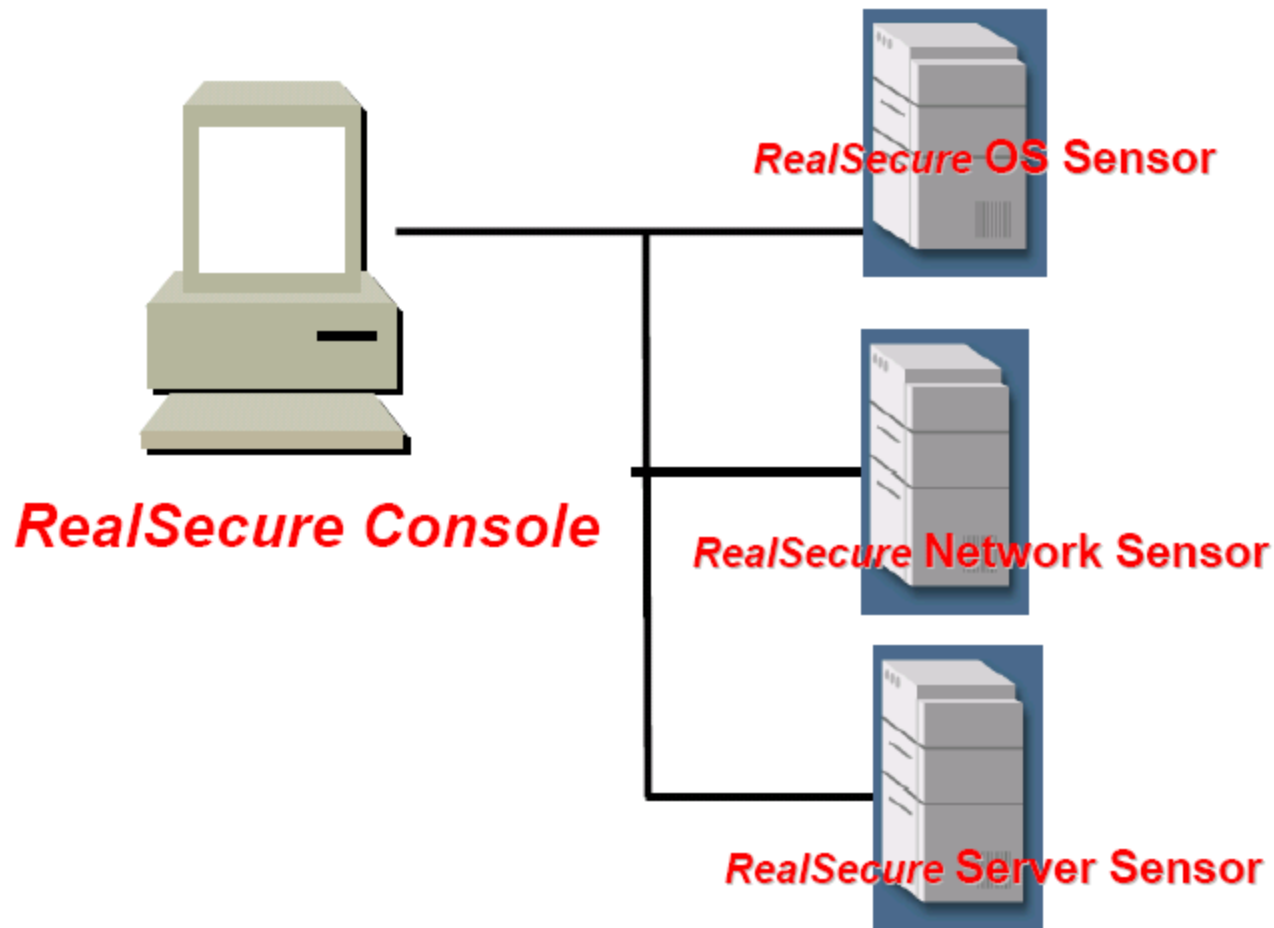


RealSecure

- ❖ **1996年**， **RealSecure**首先被作为一种传统的基于传感器的网络入侵检测系统来开发，
- ❖ **1998年**成为一种混合入侵检测系统
- ❖ 正在努力提供一种混合的**OS**日志及网络分组性能，设计为放置在协议栈的**IP**层之下和**IP**层之上
- ❖ 多种响应方式



RealSecure基本结构



10.2.4 蜜网技术

1. 蜜罐技术

蜜罐（Honeypot）是一种安全资源，它的价值就在于被探测、被攻击或被攻陷。可见，Honeypot可以是带有欺骗、诱捕性质的网络、主机和服务。除了欺骗攻击者，Honeypot没有其他正常的业务用途，因此任何访问Honeypot的行为都是可疑的。

10.2.4 蜜网技术

2. 蜜罐技术---分类

根据交互程度可将蜜罐分为：低交互（**Low-interaction**）蜜罐和高交互（**High-interaction**）蜜罐。低交互蜜罐通过模拟操作系统和服务来实现其功能，黑客只能在仿真服务指定的范围内动作，仅允许少量的交互。该方法结构简单，容易部署，风险程度低。高交互蜜罐通常必须由真实的操作系统来构建，提供给黑客真实的系统和服务。高交互蜜罐一般位于受控环境中，可防止攻击者使用蜜罐主机发起对外攻击。该种蜜罐可以获得大量的有用信息，通过真实的系统，可以学习黑客运行的全部动作；还可以获取未知的攻击行为。

3. 蜜罐技术——原理

诱骗技术：诱骗技术在蜜罐技术体系中是最为关键的技术和难题。目前的诱骗技术主要有：模拟服务端口，模拟系统漏洞和应用程序，IP地址空间欺骗，流量仿真，网络动态配置，蜜罐主机等。

数据收集：为了捕获攻击者的行为，其使用的技术和工具按照获取信息的位置可分为：基于主机的数据收集和基于网络的数据收集。在Honeypot所在的主机上几乎可以捕获攻击者行为的所有数据，如连接情况、远程命令、系统日志信息和系统调用序列等；在网络上捕获Honeypot的数据，风险小、难以被发现。可以收集到防火墙日志、入侵检测系统日志和蜜罐主机系统日志等。

3. 蜜罐技术---原理

数据控制技术：用于控制攻击者的行为，蜜罐系统允许所有进入的访问，但是它对外出的访问进行严格控制。通常有两层数据控制，连接控制和路由控制。分别由防火墙和路由器来完成。

数据分析技术：是将蜜罐捕获的各种数据分析成为有意义、易于理解的信息。

4. 蜜网技术

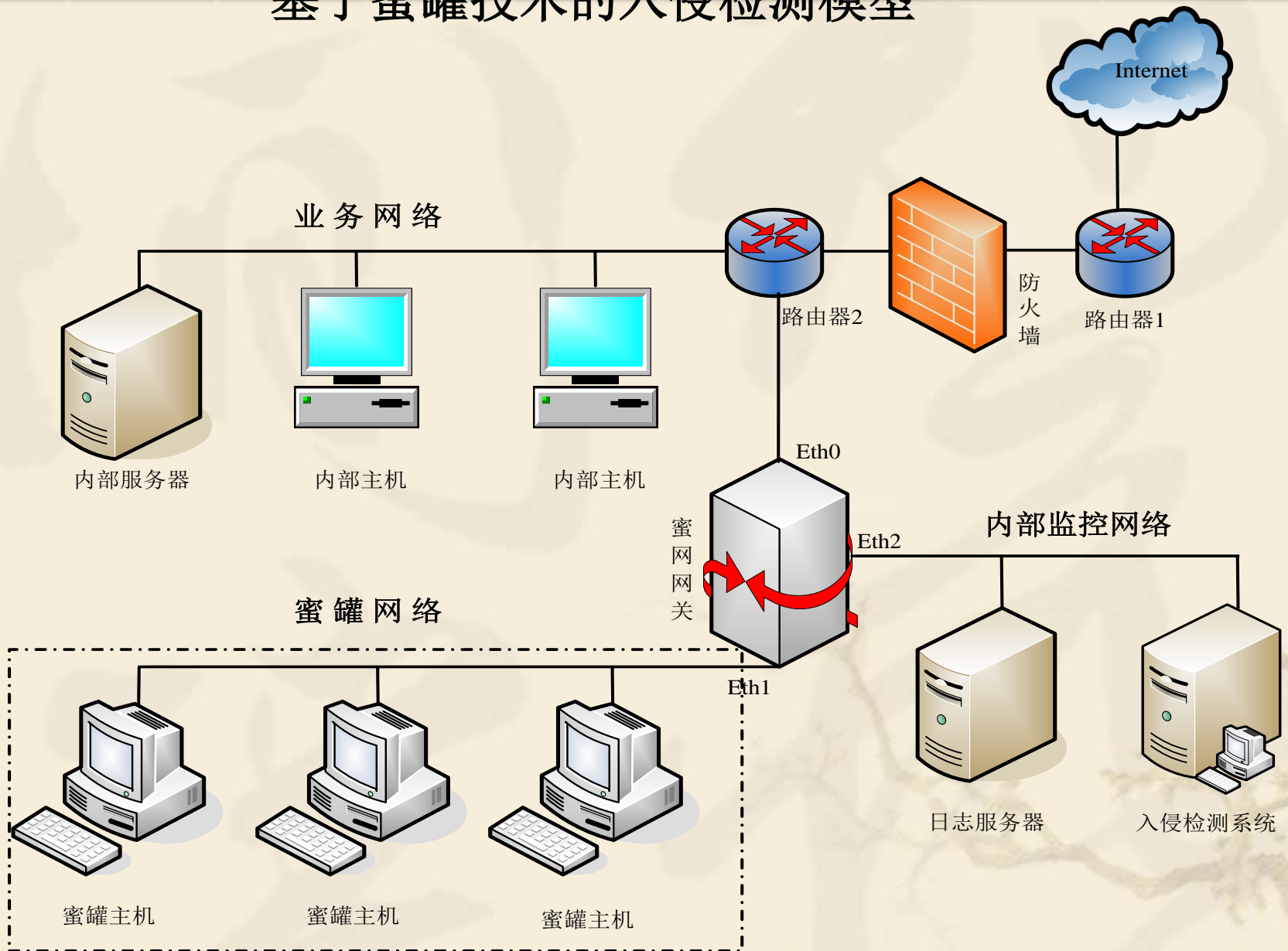
蜜网（Honeynet）是一种高交互的Honeypot，通过建立一个标准产品系统的网络，将该网络置于某种访问控制设备（通常是防火墙）之后，并进行观察。Honeynet中的系统提供完整的操作系统和应用软件，攻击者可以与其交互、进行探测、攻击和利用。

4. 蜜网技术

在Honeynet构建的高度可控网络中，可监控恶意用户所使用的工具、方法和动机。Honeynet体系结构包含了三个关键功能元素，即数据控制、数据捕获和数据采集。数据控制和数据捕获遵循了蜜罐的基本原理，数据采集是Honeynet独特的关键功能元素，通过将多个Honeynet组织的数据采集并存储在一个点，并对它们进行综合分析，可以提高Honeynet的研究价值。

5. 基于蜜罐技术的入侵检测模型

基于蜜罐技术的入侵检测模型



- 诱骗网络是由多台蜜罐主机构成的蜜网，该蜜网通过一个以桥接模式部署的蜜网网关（HoneyWall）与外部网络连接。
- 作为关键部件，蜜网网关是蜜网与其它网络的唯一连接点，有三个网络接口，其中Eth0连接外网，Eth1连接蜜网，两个接口以桥接方式连接，不提供IP地址和网卡MAC地址，同时也不对转发的网络数据包进行TTL递减和网络路由。
- 蜜网网关的存在并不对网络数据包的传输过程进行任何改动，从而使得蜜网网关很难被攻击者发现。蜜网网关的Eth2接口连接内部管理监控网络，使得安全研究人员能够远程对蜜网网关进行控制，并能够对蜜网网关捕获的攻击数据进行进一步分析。该接口使用一个内部IP，并通过严格的访问控制策略进行防护。
- 蜜网网关是蜜网与外部网络的唯一连接，所以进出蜜网的网络流量都将通过它，所以在蜜网网关上能够实现对网络数据流的控制和捕获控制。

11.3 入侵防御系统IPS

- ❖ 入侵防御系统（Intrusion Prevention System, IPS）是2000年之后出现的一种安全技术。
- ❖ 其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。

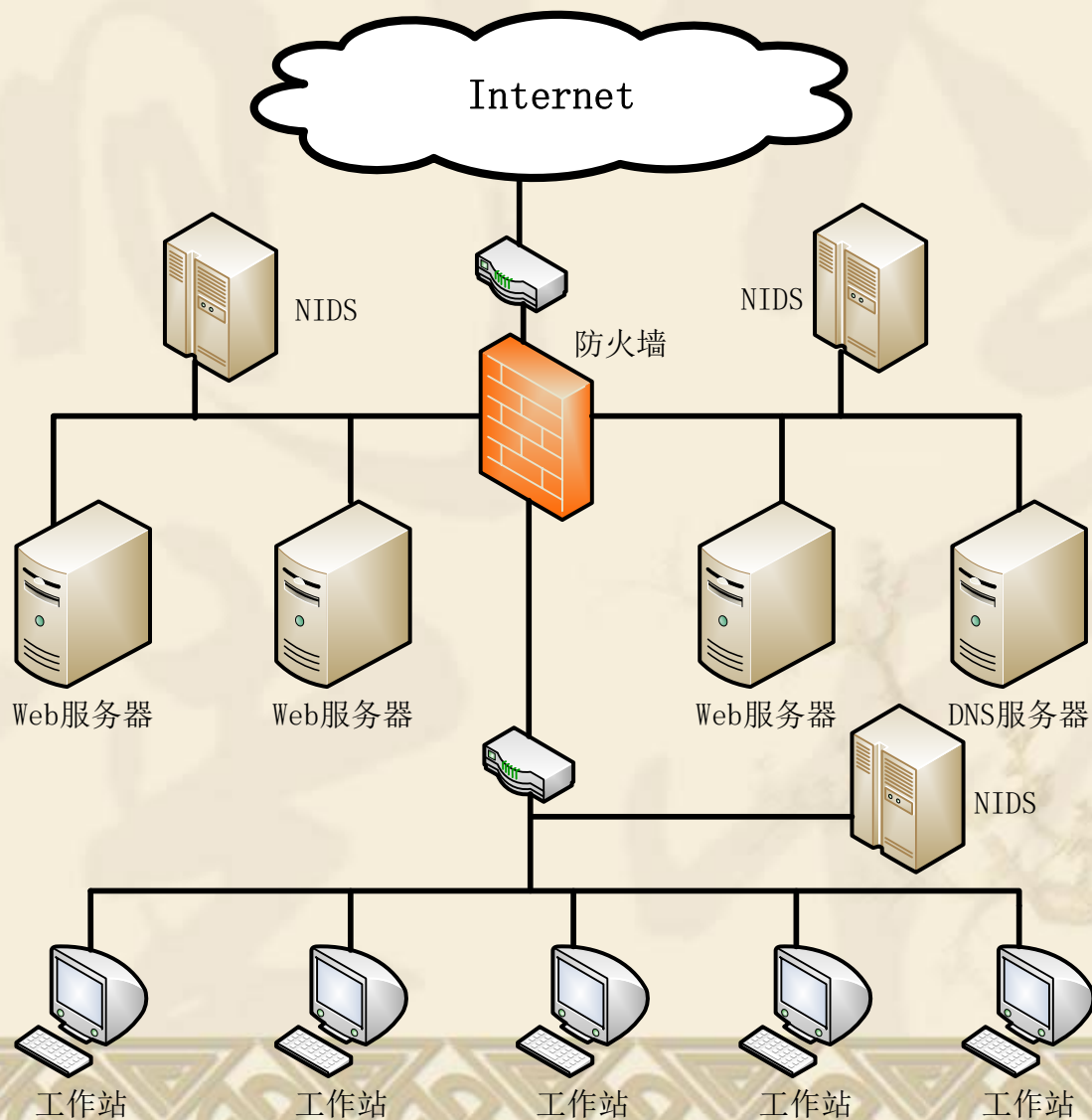
入侵防御系统的产生

- ❖ 对于**防火墙**来说，它被串行部署在网络进/出口处，对进出的所有数据流进行检查和过滤。因此，它的性能大小会对网络吞吐量有极大的影响。
- ❖ 尽管许多防火墙具备在应用层工作的能力，但对于一个网络流量较大的网络而言，如果防火墙在应用层进行过滤，往往会因为巨大的处理需求而使得防火墙成为网络的瓶颈。
- ❖ 因此，**防火墙的应用主要还是以低层包过滤为主**。这时，防火墙就对应用层的深层攻击行为无能为力了。

IDS无法进行实时的阻断

- ❖ 对于IDS来说，它被旁路部署在网络内部，作为防火墙的有益补充，能够及时发现那些穿透防火墙的深层攻击行为。但正是由于它是旁路部署，所以它无法对这些深层攻击进行实时的阻断。

NIDS在网络中的部署



IPS

- ❖ 将IDS的深层分析能力和防火墙的在线部署功能结合起来，形成一个新的安全产品，这就是IPS产品的起源
- ❖ 一种能防御防火墙所不能防御的深层入侵威胁（入侵检测）的在线部署（防火墙方式）安全产品。

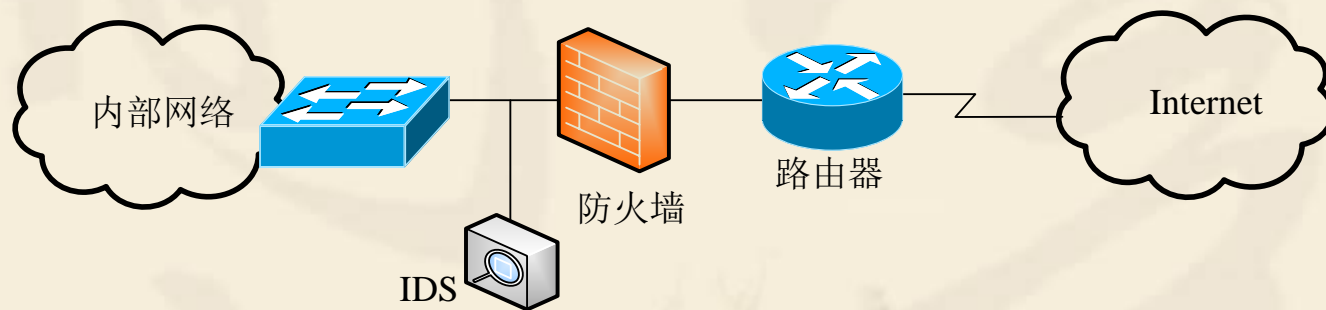
IPS的发展

- ❖ 在2000年，Network ICE公司首次提出了IPS这个概念，并于同年的9月18日推出了BlackICE Guard。它是一个串行部署的IDS，直接分析网络数据并实时对恶意数据进行丢弃处理。
- ❖ 2002年IPS概念传入国内

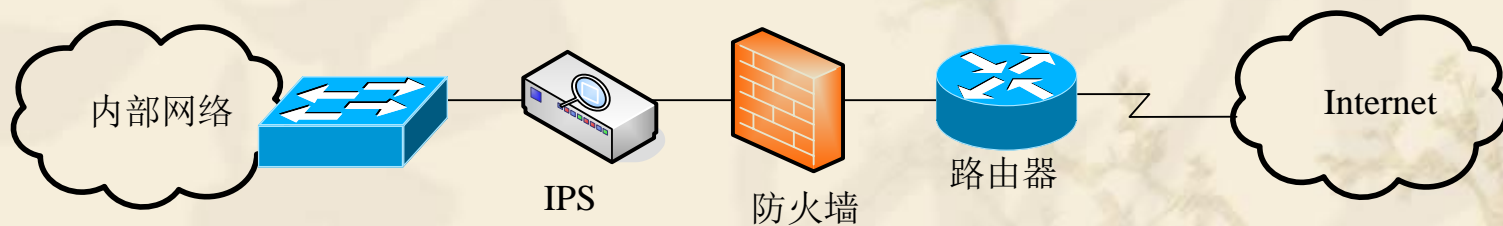
- ❖ IDS旁路检测的部署形式下，误警对正常业务不会造成影响，仅需要花费资源去做人工分析。
- ❖ 串行部署的IPS一旦出现了误报或滥报，触发了主动的阻断响应，用户的正常业务就有可能受到影响，因此，IPS概念在2005年之前的国内市场表现平淡。
- ❖ 自2006年起，大量的国外厂商的IPS产品进入国内市场，各本土厂商和用户都开始重新关注起IPS这一并不新鲜的“新”概念，并推出了相应的IPS产品。

入侵防御系统与入侵检测系统的区别

❖ 使用方式不同



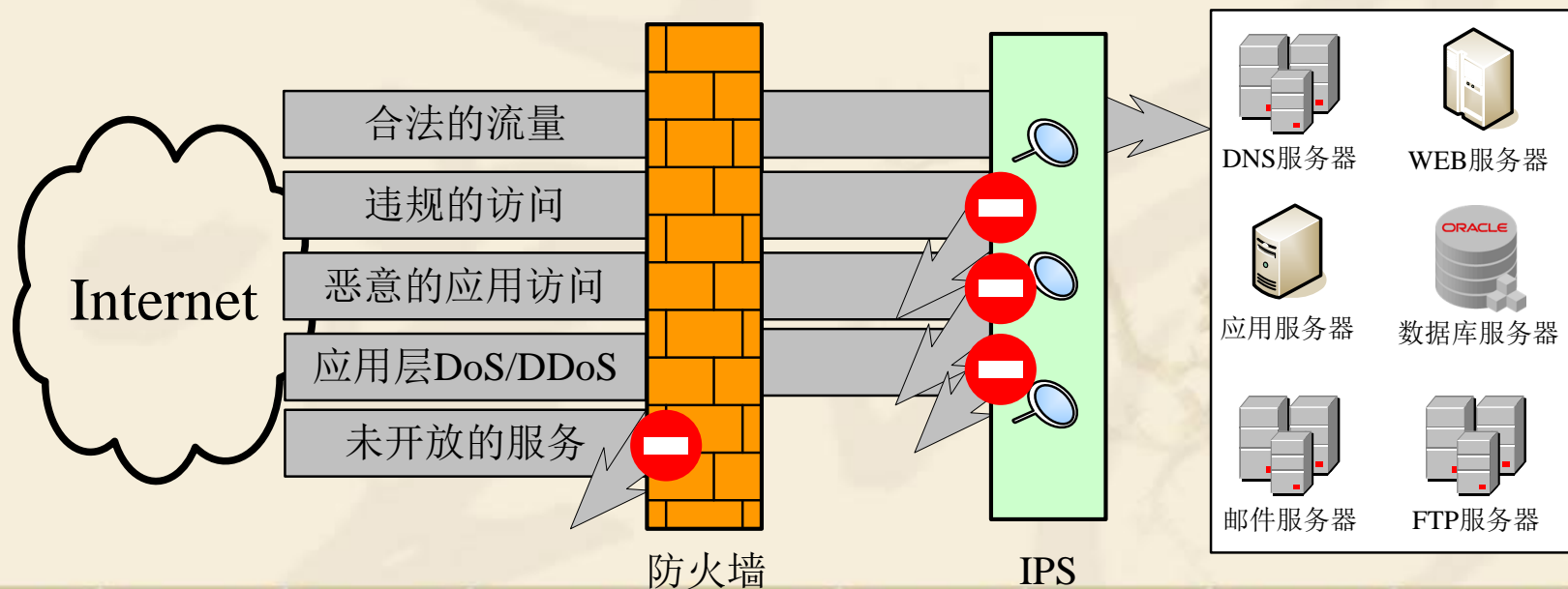
(a) IDS旁路并联



(b) IPS链路串联

IPS与防火墙相互补充

- ❖ 防火墙是粒度比较粗的访问控制产品，在基于TCP/IP协议的过滤方面表现出色
- ❖ IPS的功能比较单一，它只能串联在网络上，对防火墙所不能过滤的攻击进行过滤。
- ❖ 防火墙和IPS构成了一个两级的过滤模式，可以最大地保证系统的安全



- 防御穿透防火墙的应用层攻击
- 防御Web、FTP等外联服务

分布式部署

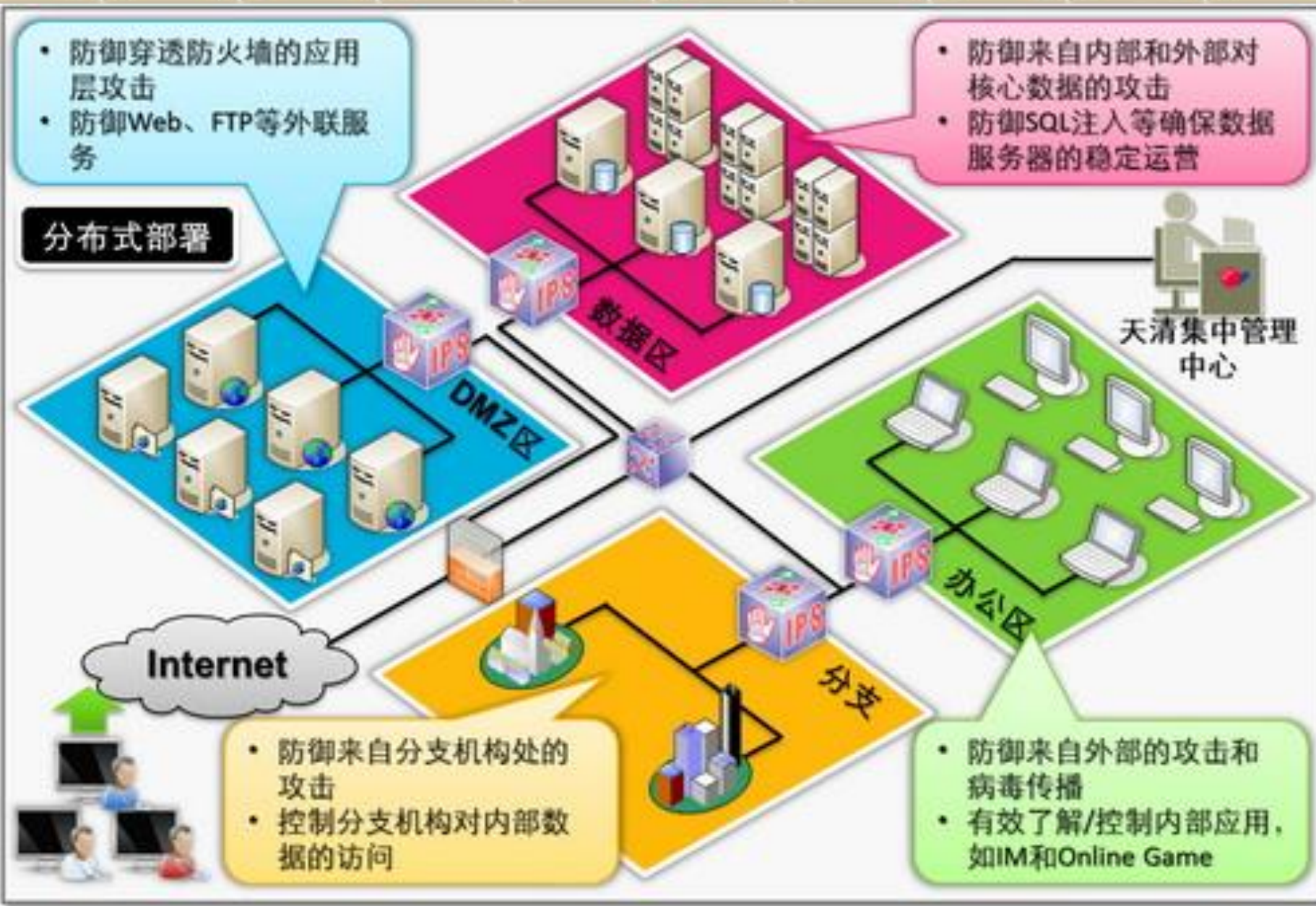
- 防御来自内部和外部对核心数据的攻击
- 防御SQL注入等确保数据服务器的稳定运营

天清集中管理中心

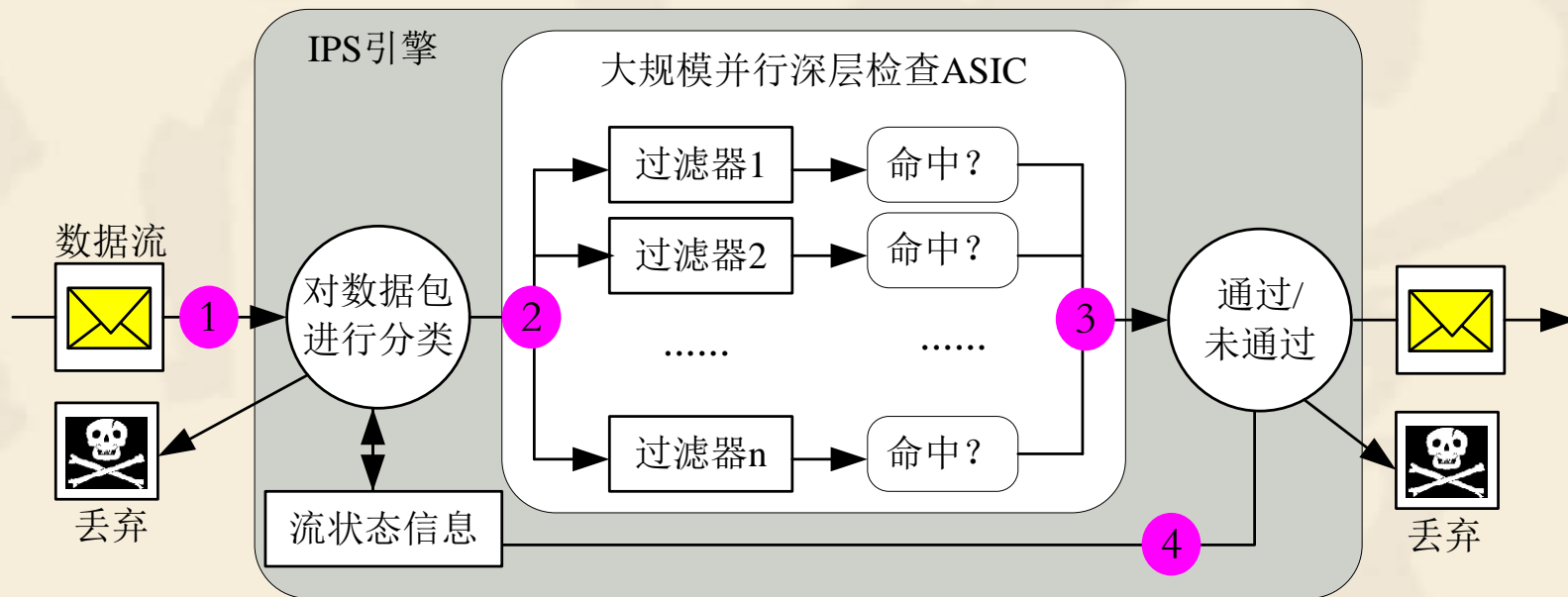
Internet

- 防御来自分支机构处的攻击
- 控制分支机构对内部数据的访问

- 防御来自外部的攻击和病毒传播
- 有效了解/控制内部应用，如IM和Online Game



IPS的基本原理



- ❖ IPS拥有数目众多的过滤器，能够防止各种攻击。
- ❖ 每种过滤器都设有相应的过滤规则
- ❖ 过滤器引擎集合了流水和大规模并行处理硬件，能够同时执行数千次的数据包过滤检查
- ❖ 当新的攻击手段被发现之后，IPS就会创建一个新的过滤器

IPS的局限性

❖ 单点故障

- ❧ 嵌入式的IPS设备出现问题，就会严重影响网络的正常运转。
- ❧ 在很多安全解决方案中，IPS采用双机备份冗余配置

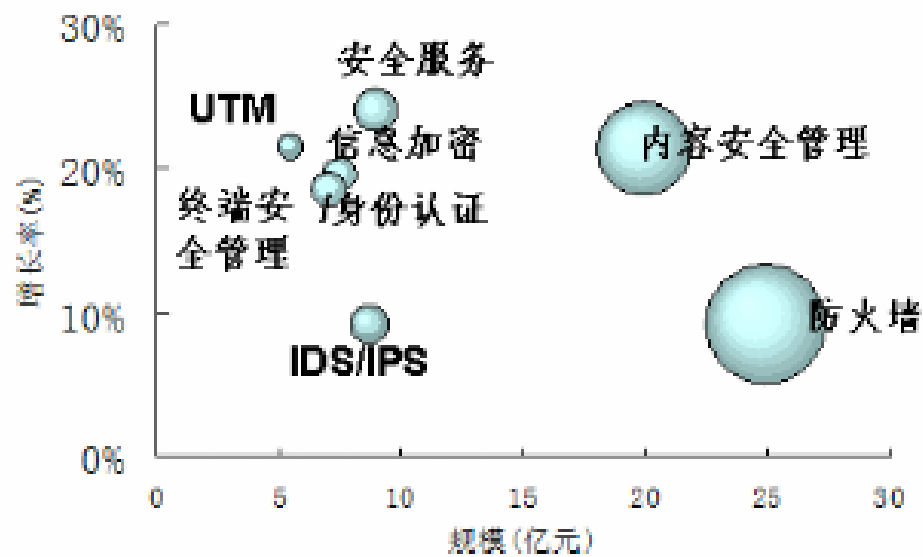
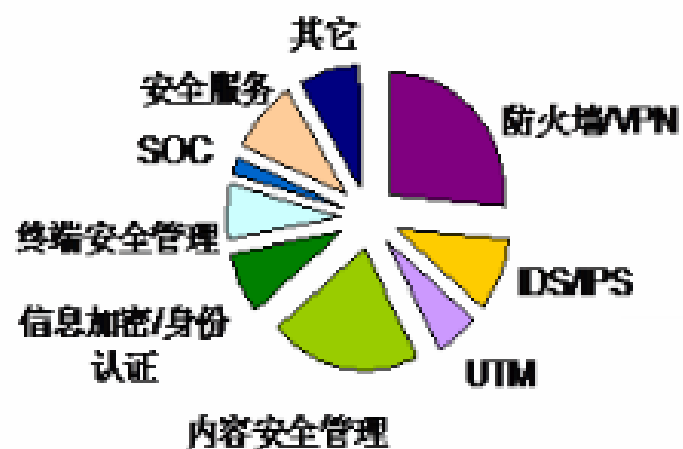
❖ 性能瓶颈

- ❧ 和防火墙一样，IPS是一个潜在的网络瓶颈。
- ❧ 高端 IPS 产品供应商都通过使用自定义硬件来提高IPS的运行效率

❖ 误报率和漏报率

统一威胁管理UTM

- ❖ 统一威胁管理（**Unified Threat Management, UTM**）是**2002**年之后出现的一种信息安全概念以及在这一新概念下所设计出的安全产品。
- ❖ 从硬件上看，它通常是一台集成了防火墙、**IDS**、**VPN**、防病毒网关等相关功能的安全设备。
- ❖ 近几年来，**UTM**发展十分迅速，在信息安全市场上的份额逐年提高，成为信息安全领域的新宠。



UTM概述

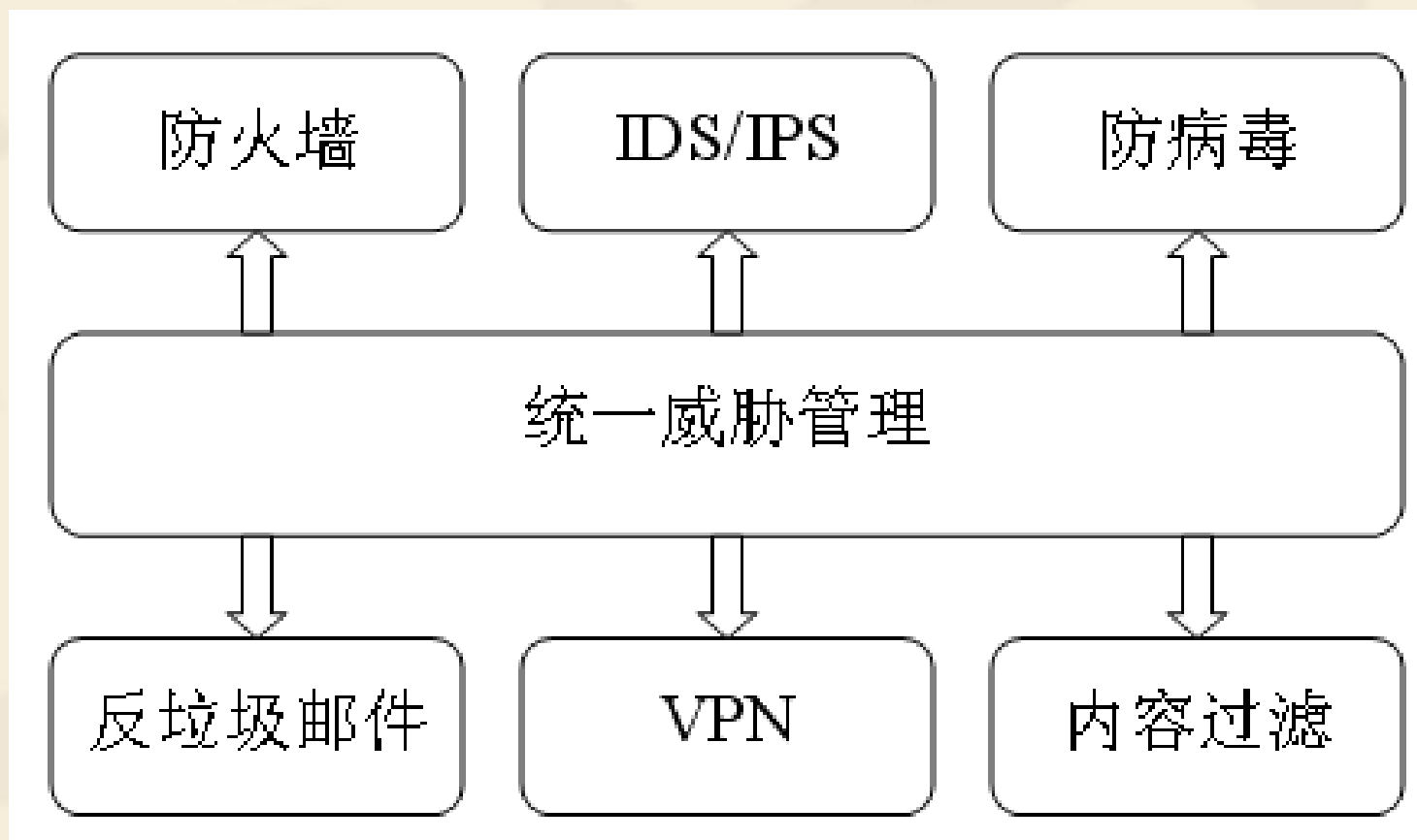
- ❖ 为了满足用户对防火墙、IDS、VPN、反病毒等产品的集中部署与管理需求，一些安全厂商提出将多种安全技术整合在同一个产品当中，这便是UTM的雏形。
- ❖ 2004年9月美国著名的国际数据公司（International Data Corporation, IDC）正式提出UTM的概念，将防病毒、入侵检测与防御、防火墙等结合于一体的安全设备命名为统一威胁管理。

UTM的产生和发展的必然性

- ❖ 如果用户购买众多的安全网关，比如防病毒网关、垃圾邮件网关、防拒绝服务攻击网关、内容过滤网关等等，再加上路由器和防火墙这样的网关，整个安全防御系统就显得十分臃肿和繁杂。多功能集成在一起的综合型网关成为市场需求。
- ❖ UTM确实能够带来价值。UTM降低了安装和维护的复杂度，能够实现“无干预”运行。

UTM的定义

- ❖ 由硬件、软件和网络技术组成的具有专门用途的设备，它主要提供一项或多项安全功能。它将多种安全特性集成于一个硬设备里，构成一个标准的统一管理平台。**UTM设备应该具备的基本功能包括网络防火墙、网络入侵检测/防御和防病毒网关功能。**



UTM的优势

- ❖ UTM设备大大降低了安全系统构件的复杂性，一体化的设计简化了产品选择、集成和支持服务的工作量。
- ❖ UTM设备的维护量通常很小，因为这些设备通常都是即插即用的，只需要很少的安装配置。

UTM的局限性

- ❖ UTM作为一个希望提供多样化检测能力的网关设备，必须在性能和检测能力上寻求平衡，在高带宽环境下两方面都达到很高水平是不可能。
- ❖ 由于UTM自身的检测是多方面的检测，而且这些检测结果还要用于阻断/通行的判断。这样的复杂状态，使得目前UTM设备的高可用性能力普遍要弱于防火墙和路由器。
- ❖ 因此，UTM不适合作为高带宽高性能要求的网关，也不适合作为深度检测数据源存在。
- ❖ UTM应当部署在带宽不大，流量不大，对于高可用性的要求一般，但是对于综合安全防护要求高，不希望过多人工维护和干预的网关位置。
- ❖ 所以，UTM通常只能部署在中小企业的大部分网关位置，或者大型企业和机构的低端接入网关位置。

本章总结

❖ 防火墙

- ❧ 包过滤防火墙
- ❧ 状态防火墙
- ❧ 应用网关代理防火墙

❖ 入侵检测系统

- ❧ 基于主机的IDS
- ❧ 基于网络的IDS

❖ 入侵防御系统IPS

- ❧ 在线检测和响应

❖ 统一威胁管理UTM

- ❧ 适用于小型企业的综合解决方案