NS13 – IPSEC

1.IPSec 隧道协议，基于 IP 通信环境下一种端到端的保证数据安全的机制

（作为一个隧道协议实现了 VPN 通信）

2. IPSec 包含两个安全协议和一个密钥管理协议

2.1 AH 协议

（1）全称：认证报头协议（Authentication Header)

（2）服务：

A.无连接的数据完整性验证

B.数据源身份认证

C.防重放攻击

不提供数据保密性服务

（3）使用键值哈希函数而不是数字签名，因为数字签名太慢，将大大降低网络吞吐率。

（4）服务实现方式：

A.数据完整性验证通过哈希函数（如 MD5）产生的校验来保证；

B.数据源身份认证通过在计算验证码时加入一个共享密钥来实现；

C.AH 报头中的序列号可以防止重放攻击

2.2 ESP 协议

（1）全称：封装安全有效载荷协议（Encapsulating Security Payload)

（2）服务：

A.数据保密性

B.无连接完整性验证

C.数据源认证能力

（3）ESP 除了为 IP 数据包提供 AH 已有的 3 种服务外，还提供另外两种服务：

A.数据包加密

是指对一个 IP 包进行加密，可以是对整个 IP 包，也可以只加密 IP 包的载荷部分，一般用于客户端计算机

B.数据流加密

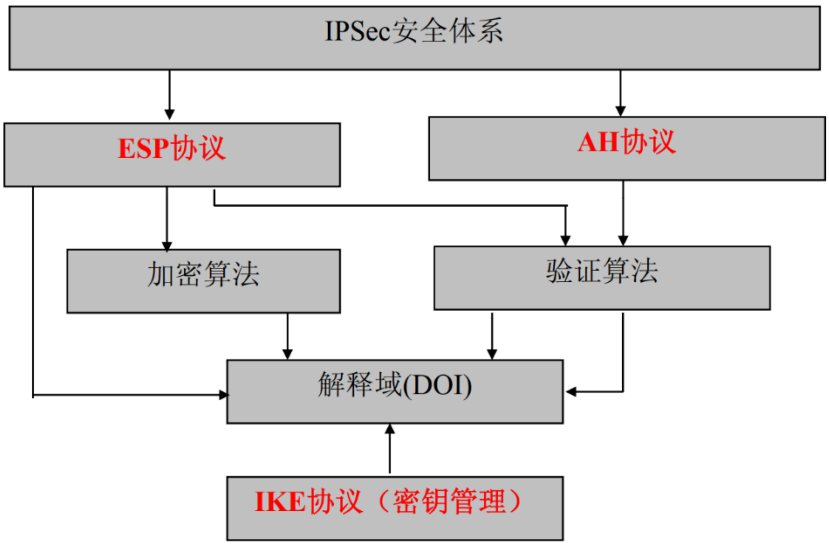
一般用于支持 IPSec 的路由器，源端路由器对整个 IP 包进行加密后传输，目的端路由器将该包解密后将原始包继续转发

2.3 IKE 协议

（1）全称：因特网密钥交换协议（Internet Key Exchange Protocol）

（2）服务：负责密钥管理，定义了通信实体间进行身份认证、协商加密算法以及生成共享的会话密钥的方法。

（3）IKE 将密钥协商的结果保留在安全联盟（SA）中，供 AH 和 ESP 以后通信时使用



AH 和 ESP 可以单独使用，也可以嵌套使用

解释域（DOI）为使用 IKE 进行协商 SA 的协议统一分配标识符。共享一个 DOI 的协议从一个共同的命名空间中选择安全协议和变、共享密码以及交换协议的标识符等，DOI 将 IPSec 的这些 RFC 文档联系到一起

3. IPSec 协议以标准加密技术为基础，例如 IPSec 使用：

3.1 DES 和其它分组加密算法来加密数据；

3.2 键值哈希算法(HMAC, MD5, SHA)来认证数据包；

3.3 验证公钥有效性的数字证书技术。

4.安全联盟 (Security Association，SA)

4.1 两台 IPSec 计算机在交换数据之前，必须首先建立某种约定，称为“安全联盟"或"安全关联"。

（确定使用算法，共享密钥）

4.2 安全联盟是单向的，这也就意味着每一对通信系统连接都至少需要两个安全联盟: 一个是从 A 到 B 另一个是从 B 到 A.

比如说 A 到 B 的发出数据通道成为 SA(out),而 B 到 A 的收入数据通道称为 SA(in)。同理有 SB(in),SB(out)，此时 SA(in)与 SB(out)则要进行协商共享加密参数

4.3 每个安全联盟可以由一个三元组惟一确定：

<SPI, 源/目的 IP 地址,IPSec 协议>

（1）安全参数索引(SPI) (是一个随机选取的惟一字符串)：安全协议识别码 (区分 AH 还是 ESP)；标识同一个目的地的 SA 。

（2）源 /目的 IP 地址。表示对方 IP 地址，对于外出数据包， 指目的地址；对于进入 IP 包，指源地址。

（3）IPSec 协议：采用 AH 或 ESP

4.4 两大主要任务

（1）创建：先协商 SA 参数，再用 SA 更新 SAD(安全联盟数据库)

在要求建立安全连接但找不到对应的 SA 的时候，便会调用 IKE,便由其来协商具体的 SA

（2）删除：遇到存活时间过期、密钥被破解等情况

4.5 SP 与 SPD

（1）SP （Security Policy，安全策略）

指示 IP 数据包提供何种保护，并以何种方式实施保护并以何种方式

实施保护。SP 主要根据源 IP 地址、目的 IP 地址、入数据还是出数据等来标识。

（2）SPD （Security Policy Database，安全策略数据库）

将所有的 SP 以某种数据结构集中存储的列表

将 IP 包发送出去时，或者接收到 IP 包时，首先要查找 SPD 来决定如何进行处理。存在 3 种可能的处理方式：丢弃、不用 IPSec 和使用 IPSec

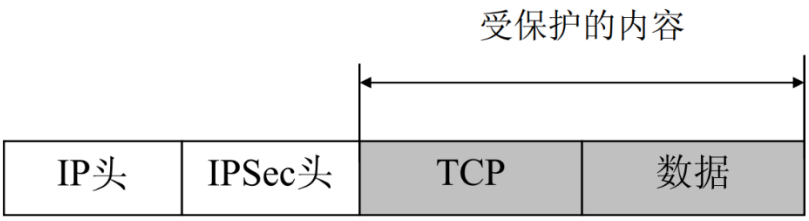
5.IPSEC 工作模式

5.1 传输模式

传输模式为上层协议提供安全保护，保护是的是 IP 包有效载荷

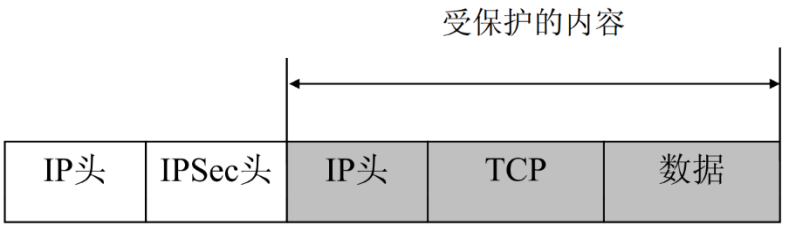
(如 TCP,UDP 和 ICMP)

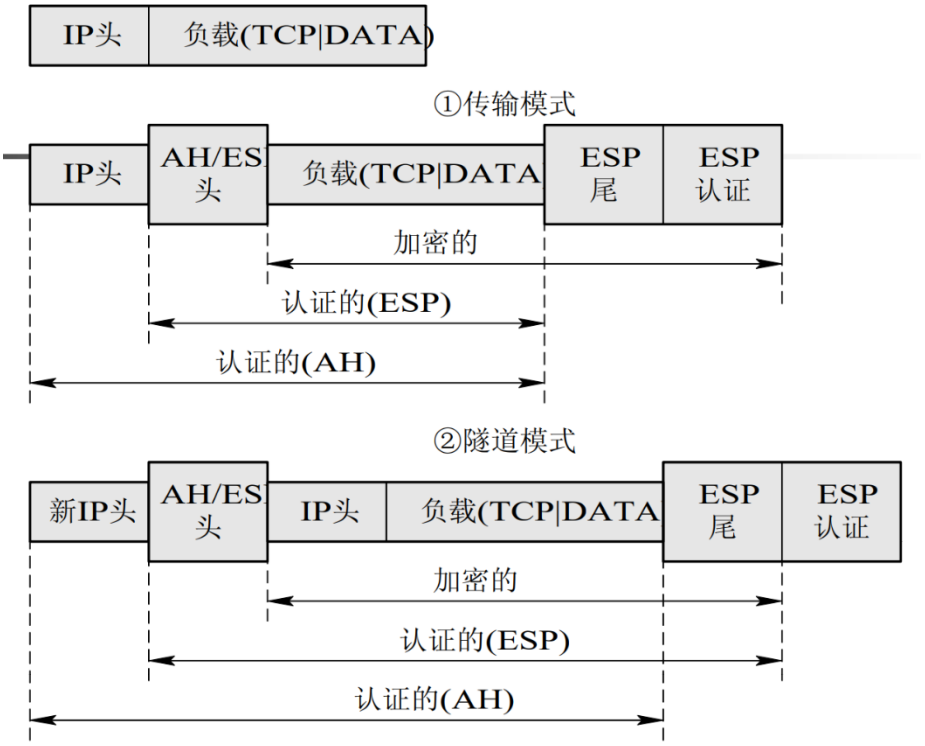
用于两台主机之间的安全通信



5.2 隧道模式

为整个 IP 包提供保护。隧道模式首先为原始隧道模式首先为原始 IP 包增加 AH 或 ESP 字段，然后再在外部增加一个新的 IP 头



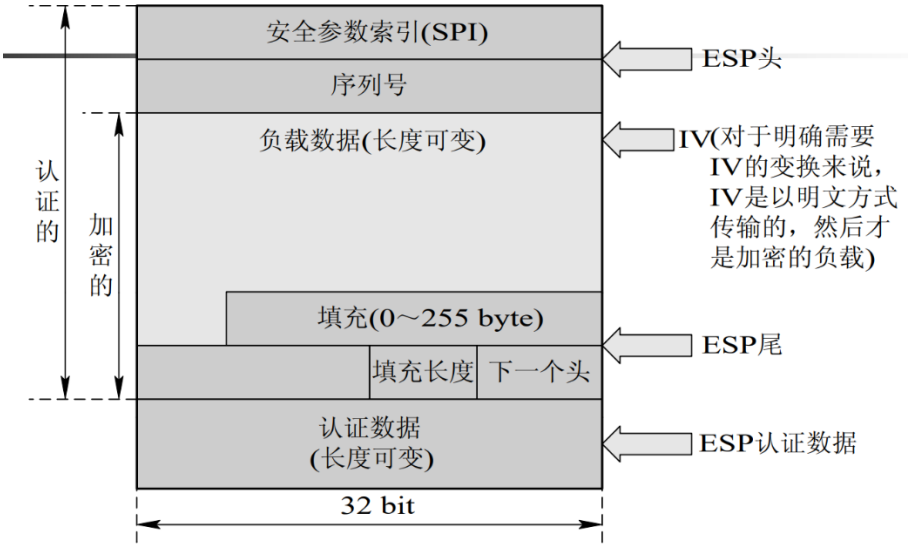


在传输模式当中，只处理 IP 有效负载，并不修改来原的 IP 协议报头，优点为在每个于数据包只增加了少量的字节。公共网络上的其它设备可以看到最终的目的和源地址。

传输模式的 IP 报头是以明文方式传输的，因此很容易遭到某些通信量分析攻击。但攻击者无法确定传输的是电子邮件还是其它应用程序。

在隧道模式当中，原有的整个 IP 包都受到保护并作为新的有效荷载，

优点在于不用修改任何端系统就可以获得 IP 安全性能。隧道模式同样还可以防止通信量分析攻击。在隧道模式中，因为内外 IP 头的地址可以不一样，攻击者只能确定隧道的端点，而不是真正的数据包源和目的站点。



ESP 头结构

6.IKE 与 ISAKMP

IKE 真正定义了一个密钥交换的过程，而 ISAKMP 只是定义了一个通用的可以被任何密钥交换协议使用的框架

IKE 目前定义了四种模式：

主模式、积极模式、快速模式、新组模式

7.IKE 阶段

IKE 第一阶段用于建立 ISAKMP 的安全联盟 。

第一阶段假设并没有安全通道存在，因此必须建立这样一条安全通道来保护 ISAKMP 消息。 这个 SA 同后续为其它服务建立的 SA 的不同之处在于：此 SA 由 ISAKMP 拥有。该 SA 包含了各种密钥材料，它们将用于后续 ISAKMP 消息的加密和认证消息的加密和认证，以及用于推导非 ISAKMP 安全联盟的密钥

第二阶段用于为不同的服务协商各自的安全联盟。使用第一阶段产生的 ISAKMP SA 保护后续所有的第二阶段 ISAKMP 消息。

这个阶段的目的是更新第一阶段建立的密钥材料，它们会用于推导各种服务所需的密钥，例如用于加密和认证消息。

NS14 – Network Isolation

1.基本概念：

安全域：安全域是以信息涉密程度划分的网络空间。

公共服务域是指既不涉及国家秘密也不涉及工作秘密，是一个向因特网络完全开放的公共信息交换空间（如因特网）

电子政务内网为涉密域，外网为非涉密域。

网络隔离，主要是指把两个或两个以上可路由的网络两个以上可路由的网络（如 TCP/IP）通过不可路由的协议通过不可路由的协议（如 IPX/SPX、NetBEUI 等）进行数据交换而达到隔离目的。

由于其原理主要是采用了不同的协议，所以通常也叫协议隔离

2. 隔离技术

第一代隔离技术——完全的隔离

第二代隔离技术——硬件卡隔离

第三代隔离技术——数据转播隔离

第四代隔离技术——空气开关隔离

第五代隔离技术——安全通道隔离

3. 隔离技术原理：

3.1 当外网需要有数据到达内网的时候，隔离设备将所有的协议剥离并将原始的数据写入到存储介质当中。

3.2 当写入完成之后，将与外网连接中断，并将数据推向内网，内网收到数据后进行协议封装并交给应用系统。

4. 每一次数据交换，隔离设备经历了数据的 隔离设备经历了数据的接受、存储和转发三个过程。

物理隔离的一个特征，就是内网与外网永不连接，内网和外网在同一时间最多只有一个同隔离设备建立非 TCP/IP 协议的数据连接。

优点：外网的破坏影响不到内网。

5. 网络隔离技术分类

5.1 基于代码、内容等隔离的反病毒和内容过滤技术

5.2 基于网络层隔离的防火墙技术

5.3 基于物理链路层的物理隔离技术

6. 网络隔离技术需要具有的安全要点

¬要具有高度的自身安全性

¬要确保网络之间是隔离的

¬要保证网间交换的只是应用数据

¬要对网间的访问进行严格的控制和检查

¬要在坚持隔离的前提下保证网络畅通和应用透明

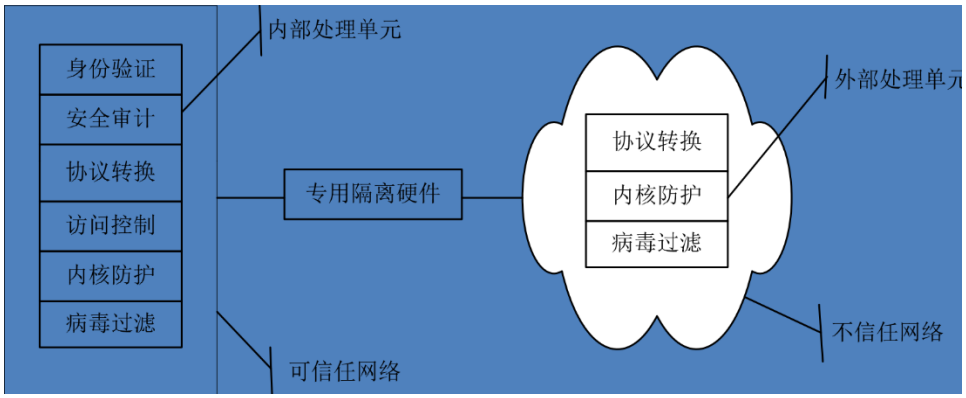
7. 隔离的关键点

要尽量提高网间数据交换的速度，并且对应用能够透明支持，以适应复杂和高带宽需求的网间数据交换。

8.隔离网闸

隔离网闸（安全隔离与信息交换,GAP)，是在保证两个网络安全隔离的基础上实现安全信息交换和资源共享的技术。

对固态存储介质只有“读”和“写”两个命令



9. 隔离网闸要点

1）专用硬件设计保证了物理隔离下的信息交流。

GAP 均采用专用隔离硬件的设计完成隔离功能

同时该硬件不提供编程软接口，不受系统控制，

2）集合多种安全技术消除数据交换中的安全隐患。在专用硬件基础上，

紧密集成了内核防护、协议转化、病毒查杀、身份验证、访问控制、安全审计等模块。这些模块可以与隔离硬件结合形成整体的防御体系。

3）网闸以安全隔离为基础，并集成多种防护技术，其软硬一体设计形成整 体多层面的安全防护。

4）灵活高效数据交换形式确保应用需求

NS15 – Firework

1. 防火墙是由软件和硬件组成的系统，它处于安全的网络 和不安全的网络之间根据由系统管理员设置的访问控制规则，对数据流进行过滤。

2. 对于数据流的处理方式：

2.1 允许通过

2.2 拒绝并返回拒绝信息

2.3 直接丢弃

(防火墙工作于 OSI 模型的层次越高，能提供的安全保护等级就越高)

(防火墙通常建立在 TCP/IP 模型基础上)

3. 防火墙分类：

3.1 包过滤防火墙

3.2 电路级网关防火墙

3.3 应用级网关防火墙

4. 防火墙设计结构：

4.1 静态包过滤

使用分组报头中存储的信息控制网络传输。当过滤设备接收到分组时，把报头中存储的数据属性与访问控制策略对比，根据对比结果的不同，决定该传输是被丢弃还是允许通过。

（1）依据： 包的目的地址及目的端口 包的源地址及源端口 应用协议

（2）优点： 直接使用路由器软件过滤，无需专门购买设备，减少投资，对网络的性能影响较低

缺点： 安全性较低，缺状态感知能力，容易被 IP 欺骗，创建访问控制规则比较麻烦

（3）静态包过滤防火墙是最原始的防火墙，静态数据包过滤发生在网络层上

（4）过滤位置可以在网络入口处也可以在网络出口处

（5）安全性考虑：

A. IP 地址欺骗：用可信用户机源地址替代

B. 隐信道攻击：包过滤器不会检查数据包的净荷部分

C. 无“状态感知”能力

4.2 动态包过滤

通过包的属性和维护一份连接表来监视通信会话的状态而不是简单依靠标志的设置

（1）具有状态感知能力

（2）动态包过滤防火墙工作于传输层

（3）对于外出的数据包进行身份记录表，便于相同连接的数据包通过

（4）动态包过滤防火墙需要对已建连接和规则表进行动态维护。并且能察觉到新建连接与已建连接之间差别

（5）优点：对网络性能影响小，安全性比静态高，由状态感知能力，成本较低

缺点：仅仅工作与网络层，只检查 IP 和 TCP 头；易被 IP 欺骗；难于创建规则，必须要考虑规则的先后次序；如果连接在建立时没有遵循三步握手协议，就会引入的风险

静态基于数据包 动态基于会话

4.3 电路级网关

作为代理服务器的一部分在应用代理类型的防火墙中实现。

电路级网关又称做线路级网关，当两个主机首次建立 TCP 连接时，电路级网关在两个主机之间 建立一道屏障。

（1）来自 Internet 的请求，作为服务器接收外来请求并转发。

（2）内部主机请求访问 Internet， 担当代理服务器

（3）与包过滤器的区别：

除了进行基本的包过滤检查外，还要增加对连接建立过程中的握手信息 SYN、 ACK 及序列号合法性的验证

（4）位于会话层

（5）基本原理：

A. 在转发一个数据包之前，首先将数据包的 IP 头和 TCP 头与由管理员定义的规则表相比较

B. 如果会话合法，包过滤器就开始逐条扫描规则，直到发现一条与数据包中的有关信息一致

C. 电路级网关在其自身与远程主机之间建立一个新连接，这一切对内网中用户都是完全透明的

（6）优点：

A. 性能比包过滤防火墙稍差，但是比应用代理防火墙好

B. 切断了外部网络到防火墙后的服务器直接连接

C. 比静态或动态包过滤防火墙具有更高的安全性

缺点：

A. 不能对数据净荷进行检测，无法抵御应用层攻击

B. 当增加新的内部程序或资源时，往往需要对许多电路级网关的代码进行修改

4.4 应用级网关

必须为特定的应用服务编写特定的代理程序，被称为“服务代理”，在网关内部分别扮演客户机代理和服务器代理的角色。

不同于包过滤防火墙那样可以过滤所有不同服务的数据流

（1）位于应用层

（2）应用代理程序与电路级网关有两个重要区别：

A.代理是针对应用的。

B.代理对整个数据包进行检查，因此能在 OSI 模型的应用层上对数据包进行过滤

（3）优点：安全性较高；有强大的认证功能；有强大的日志功能；规则配置比较简单

缺点：灵活性差；性能不高；配置繁琐

4.5 状态检查包过滤

能够理解并学习各种协议和应用，以支持各种最新的应用；

能从应用程序中收集状态信息并存入状态表中，以供其他应用或协议做检测策略。

（1）通信信息：防火墙的检测模块位于操作系统的内核，在网络层之下， 能在数据包到达网关操作系统之前对它们进行分析。

（2）通信状态：状态检测防火墙在状态表中保存以前的通信信息，记录从受保护网络发出的数 据包的状态信息。

（3）优点：由动态过滤包所有的优点；

没有打破客户/服务器模型；

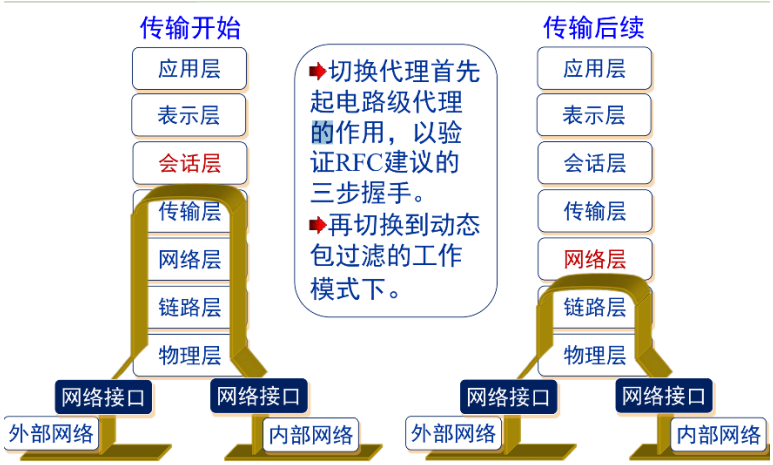
提供继承的动态包过滤功能；运行速度更快

缺点：采用单线程进程，对防火墙性能产生很大影响；

不能满足对高并发连接数量的要求；

仅提供较低水平的安全性

4.6 切换代理



（1）优点：

A.与传统电路级网关相比，对网络性能造成影响要小。

B.于对三步握手进行了验证，降低了 IP 欺骗的风险

缺点：

A.不是一个电路级网关

B. 没检查数据包的净荷部分，因此具有较低的安全性

（不及于传统的电路级网关）

C. 难于创建规则

4.7 空气隙（物理隔离）

防火墙切断了客户机到服 务器的直接连接，并且对硬盘数据的读/写操作都是独立进行的

（1）优点：

A.切断了与防火墙后面服务器的直接连接，消除了隐信道攻 击的风险

B. 采用强应用代理对协议头长度进行检测，因此能够消除缓冲

器溢出攻击。

C. 与应用级网关结合使用，空气隙防火墙能提供很高的安全性

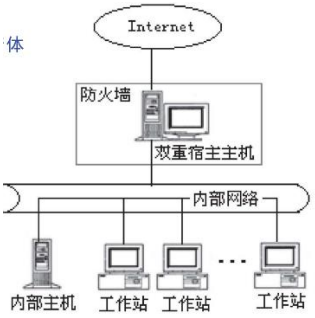
缺点：

降低网络性能；适用范围窄；结构复杂，成本高

5.防火墙体系结构

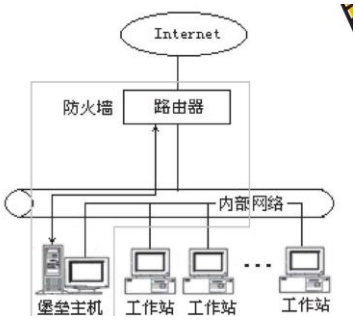
5.1 双重宿主主机体系结构

有多个网络接口，该主机可以作为接口之间的路由器，并可以发送数据包



5.2 主机过滤体系结构

主机+过滤路由器



5.3 子网过滤体系结构

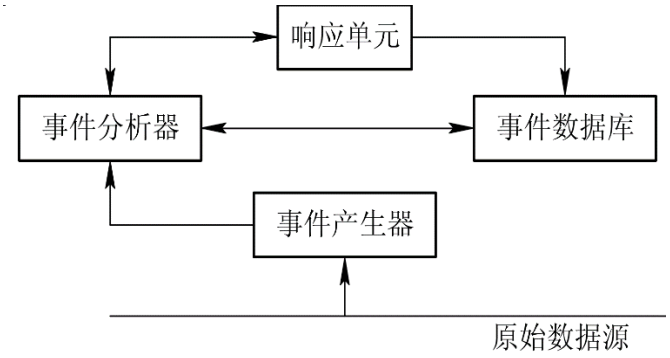
NS16 – IDS

1.入侵检测概念：（IDS, Intrusion Detection System）

入侵检测就是通过收集信息并对其进行分析，从中发现网络或系从中发现是否有违反安全策略的行为和遭到攻击的迹象，同时做出响应。

2. Pt-防护时间 > Dt-检测时间 + Rt-响应时间,能做到这样说明系统安全

3.入侵检测系统基本结构：



CIDF 模型

4. 入侵检测系统的种类，根据入侵检测系统输入数据的来源来看，可分为：

基于主机的入侵检测系统和基于网络的入侵检测系统

还有基于内核的高性能入侵检测系统和分布式的入侵检测系统

5. 基于主机的 IDS：

通常以系统日志、应用程序日志等审计记录文件作为数据源

（1）分为：网络连接检测与主机文件检测

（2）优点：能够确定攻击是否成功；非常适合于加密和交换环境；近实时的检测和响应；不需要额外的硬件；可监视特定的系统行为

缺点：占用主机的系统资源；所需配置的 IDS 数量众多；实时性较差；隐蔽性较差；检测效果取决于日志系统

6.基于网络的 IDS：

以原始的网络数据包作为数据源，使用网络适配器

（1）行为：

1) 检测端口扫描。

2) 检测常见的攻击行为。

3) 识别各种各样可能的 IP 欺骗攻击。

4) 当检测到一个不希望的活动时，基于网络的 IDS 将采取包括干涉入侵者发来的通信，或重新配置附近的防火墙策略以封锁从入侵者的计算机或网络发来的所有通信

（2）优点：攻击者转移证据更困难；实时检测和应答；能够检测到未成功的攻击企图；操作系统无关性；较低的成本

缺点：它只能监视通过本网段的活动，并且精确度较差；在交换网络环境中难于配置；防欺骗的能力比较差；对于加密信息无能为力

6.两类 IDS 检测软件对比：

7. 基于内核的入侵检测系统采取措施防止缓冲区溢出， 增加文件系统的保护，封闭信号，从而使得入侵者破坏系统变得困难

8. IDS 的分析方式：

异常检测的入侵检测系统和采用误用检测的入侵检测系统

8.1 异常检测：

前提是假定所有的入侵行为都是异常的假定所有的入侵行为都是异常的，即入侵行为是异常行为的子集

建立正常行为轮廓再去判断是否为异常的行为

8.1.1 所需考虑的问题有：

（1）特征量的选择：

选取合适的数据来让模型最优化，体现出用户行为特征

（2）阈值的选定：

选定合适的判断范围

（3）比较频率选择：

比较频率要是适中，否则会造成漏警或者性能消耗

8.1.2 该方法的技术难点在于：

A. “正常”行为特征轮廓的确定行为特征轮廓的确定；

B. 特征量的选取；

C. 特征轮廓的更新

8.1.3

优点：

- 能够检测出新的网络入侵方法的攻击；
- 较少依赖于特定的主机操作系统；
- 对于内部合法用户的越权违法行为的检测能力较强。

缺点：

- 误报率高；
- 行为模型建立困难；
- 难以对入侵行为进行分类和命名。

8.1.4 技术分类

A. 统计分析异常检测

B. 贝叶斯推理异常检测

C. 神经网络异常检测

D. 模式预测异常检测

E. 数据采掘异常检测

8.2 误用检测

其基本前提是：假定所有可能的入侵行为都能被识别和表示

8.2.1 原理

首先对已知的攻击方法进行攻击签名表示，然后根据已经定义好的攻击签名，通过判断这些攻击签名是否出现来判断入侵行为的发生与否。这种方法是通过直接判断攻击签名的出现与否来判断入侵行为

8.2.2 优点：

检测准确度高；

技术相对成熟；

便于进行系统防护。

缺点：

不能检测出新的入侵行为；

完全依赖于入侵特征的有效性；

维护特征库的工作量巨大；

难以检测来自内部用户的攻击

8.2.3 技术分类：

A. 专家系统误用检测

B. 特征分析误用检测

C. 模型推理误用检测

D. 条件概率误用检测

E. 键盘监控误用检测

9. 异常检测技术和误用检测技术的比较

入侵检测系统必须不断地学习并更新已有的行为轮廓。

误用检测技术只能检测出已有的入侵模式，必须不断地对新出现的入侵行为进行总结和归纳，且配置任务重，可人工添加。

异常检测技术报告有更多的数据，而误用报告则列举出入侵行为的类型和名称， 以及提供相应的处理建议