

# 第九章 防火墙与入侵防御系统

---

- 9.1 防火墙的必要性
- 9.2 防火墙的特征和访问策略
- 9.3 防火墙的类型
- 9.4 防火墙的布置
- 9.5 防火墙的部署和配置
- 9.6 入侵防御系统
- 9.7 实例：一体化威胁管理产品

# 内容安排

---

- 9.1 防火墙的必要性
- 9.2 防火墙的特征和访问策略
- 9.3 防火墙的类型
- 9.4 防火墙的布置
- 9.5 防火墙的部署和配置
- 9.6 入侵防御系统
- 9.7 实例：一体化威胁管理产品

# 信息系统的进展



```
graph TD; A[集中式数据处理系统] --> B[局域网 LAN]; B --> C[驻地网 premises network]; C --> D[企业级网络 enterprise-wide network]; D --> E[Internet 连通性 Internet connectivity]; E --> F[企业云计算 enterprise cloud computing];
```

集中式数据处理系统，包括一个可支持许多终端与其直接连接的中央大型机系统。

局域网（**Local Area Network, LAN**）将个人计算机和终端互联，并与大型机系统互联。

驻地网（**premises network**），由许多局域网组成，将个人计算机、服务器及一台或者两台大型机相互连接起来。

企业级网络（**enterprise-wide network**），由通过专用广域网（**wide area network, WAN**）连接起来的多个不同地理分布的驻地网组成。

**Internet 连通性（Internet connectivity）**，其中多个驻地网都连接到 **Internet**，各个驻地网可以通过专用广域网连接，也可以不通过专用广域网连接。

企业云计算（**enterprise cloud computing**）拥有位于一个或多个数据中心的虚拟服务器，可以提供组织内部或对外的 **Internet** 服务。

# 9.1 防火墙的必要性

---

- 保护局域网的有效手段
- 插入驻地网和Internet之间，以建立二者间的可控链路
  - 可以是单机系统，也可以是协作完成防火墙功能的两个或者更多系统
- 用作外围防御
  - 提供一个能加强安全和审计的遏制点
  - 将内部系统与外部网络隔离

# 内容安排

---

- 9.1 防火墙的必要性
- 9.2 防火墙的特征和访问策略
- 9.3 防火墙的类型
- 9.4 防火墙的布置
- 9.5 防火墙的部署和配置
- 9.6 入侵防御系统
- 9.7 实例：一体化威胁管理产品

## 9.2 防火墙的特征和访问策略

### 设计 目标

- 所有从内部到外部的流量都必须通过防火墙，反之亦然。
- 只有经过授权的网络流量，例如符合本地安全策略定义的流量，防火墙才允许通过。
- 防火墙本身不能被渗透。

## 9.2 防火墙的特征和访问策略

### 访问策略

- 指定合适的访问策略是防火墙的规划和实施过程的关键部分
  - 这列出了授权通过防火墙的流量类型
  - 包括地址范围、协议、应用程序和内容类型等
- 该策略应由企业的信息安全风险评估和策略部门进行制定
- 应根据广义的规范来制定，即需要支持的流量类型
- 然后将策略会被提炼为具体的过滤器，被部署在合适的防火墙拓扑中

# 用来过滤流量的防火墙访问策略特征

## IP地址和协议值

这种类型的过滤器被包过滤和状态检测防火墙所使用

通常用于限制对特定服务的访问

## 应用层协议

此类过滤器通常被应用层网关所使用，且网关主要用于转发和监控特定应用层协议的信息交换

## 用户身份

通常用于那些需要确认自己正在使用某种形式的安全认证技术的内部用户

## 网络活动

基于时间或请求、请求速率或其他活动模式等考虑因素控制访问



## 9.2 防火墙的特征和访问策略

### 防火墙所具备的功能

- 定义一个遏制点
- 提供了监视安全相关事件的场所
- 为多种与安全不相关的Internet功能的实现提供一个便利的平台
- 可以作为IPSec的平台

### 局限性

- 不能阻止那些绕开防火墙的攻击
- 不能完全防止内部威胁
- 一个安全设置不当的无线局域网有可能允许来自公司外部的访问
- 笔记本电脑、PDA或便携式存储设备可能在企业网以外的地方使用时被感染，之后被连接到内部网络使用

# 内容安排

---

- 9.1 防火墙的必要性
- 9.2 防火墙的特征和访问策略
- 9.3 防火墙的类型
- 9.4 防火墙的布置
- 9.5 防火墙的部署和配置
- 9.6 入侵防御系统
- 9.7 实例：一体化威胁管理产品

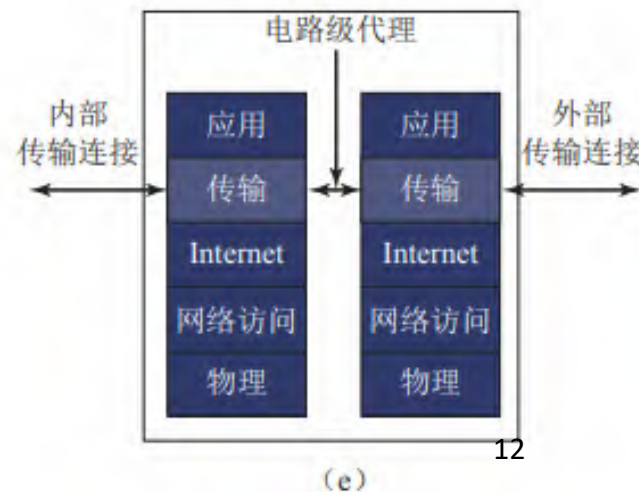
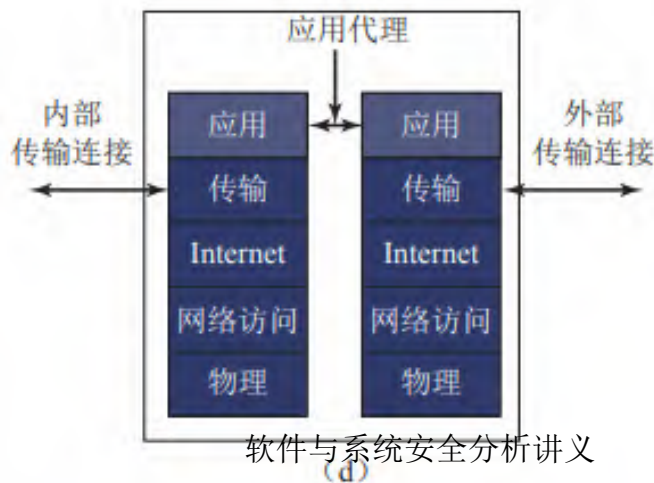
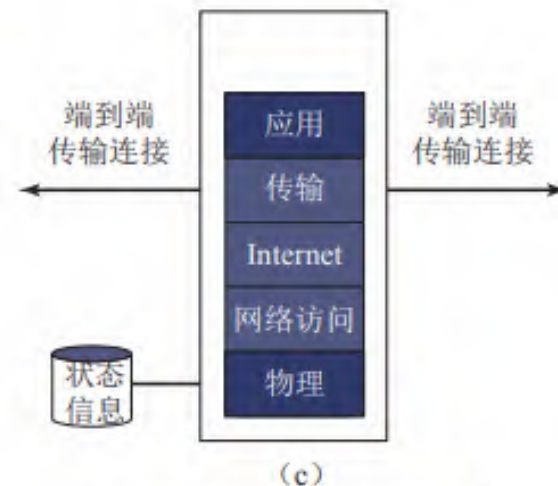
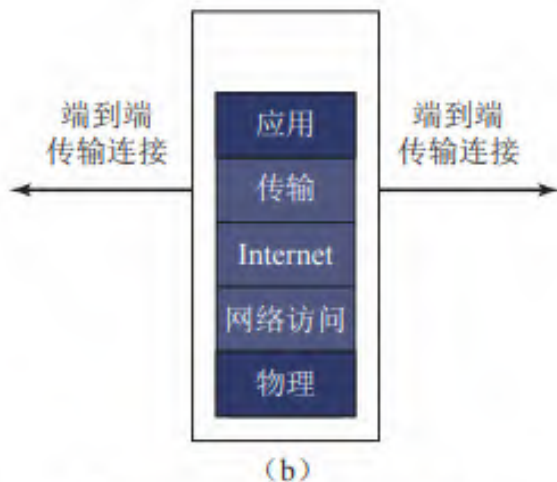
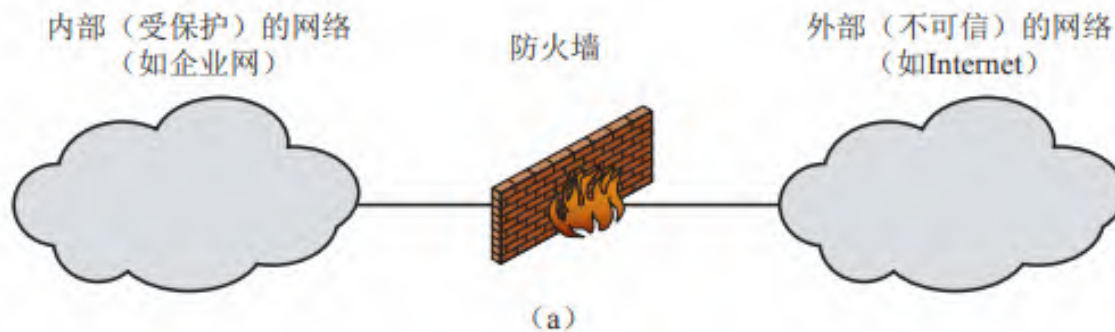
## 9.3 防火墙的类型

---

- 9.3.1 包过滤防火墙
- 9.3.2 状态检测防火墙
- 9.3.3 应用级网关
- 9.3.4 电路级网关

# 9.3 防火墙的类型

- (a) 通用模型;
- (b) 包过滤防火墙;
- (c) 状态检测防火墙;
- (d) 应用代理防火墙;
- (e) 电路级代理防火墙



## 9.3.1 包过滤防火墙

---

- 根据一组规则来检查每个接收和发送的IP包
  - 通常是基于与IP和TCP头域匹配的规则列表
  - 根据规则匹配转发或丢弃数据包
- 两个默认策略：
  - 默认 = 丢弃：没有明确准许的将被阻止。
    - 更加保守、受控、用户可见
  - 默认 = 转发：没有明确阻止的将被准许。
    - 更易于管理和使用，但安全性较差

## 9.3.1 包过滤防火墙

### 过滤规则基于网络包中所包含的信息

- 源IP地址(source IP address): 发送IP包的系统的IP地址
- 目的IP地址(destination IP address): 包要到达的系统的IP地址
- 源和目的端传输层地址 (source and destination transport-level address): 指传输层 (例如, TCP或UDP) 端口号, 定义应用程序, 比如SNMP和HTTP;
- IP协议域 (IP protocol field): 用于定义传输协议;
- 接口 (interface): 对于有三个或者更多接口的防火墙来说, 定义哪个接口用于包的出站, 哪个接口用于包的入站。

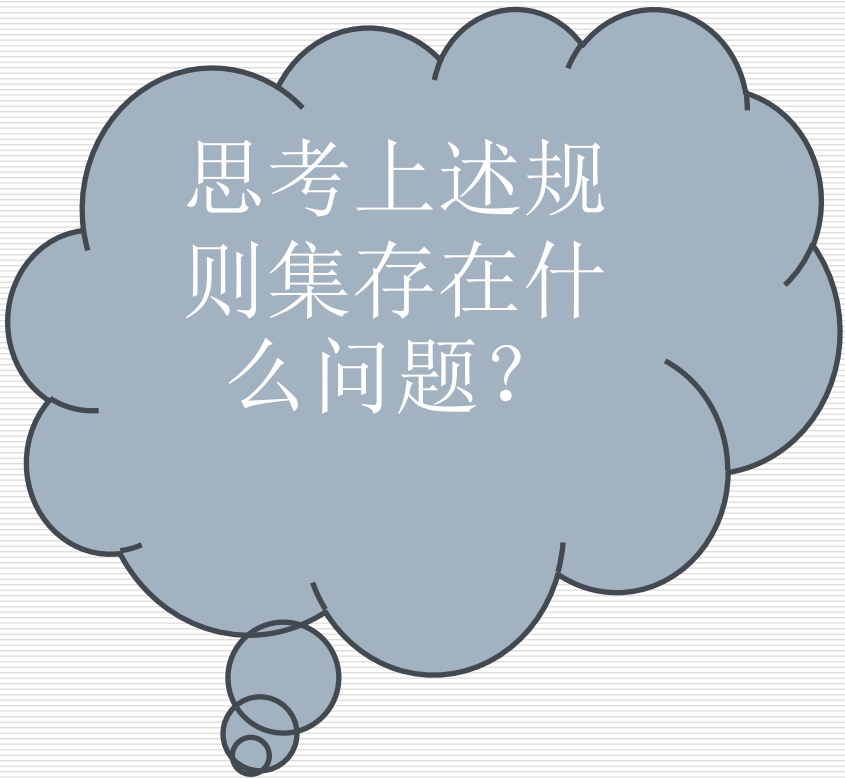
# SMTP 流量规则集的简化示例

该规则的目的是允许所有入站和出站的电子邮件流量，并禁止掉其他流量。

规则	方向	源地址	目的地址	协议	目的端口号	动作
1	进入	外部	内部	TCP	25	允许
2	离开	内部	外部	TCP	> 1023	允许
3	离开	内部	外部	TCP	25	允许
4	进入	外部	内部	TCP	> 1023	允许
5	任意	任意	任意	任意	任意	禁止

# SMTP 流量规则集的简化示例

---



思考上述规则集存在什么问题？



# SMTP 流量规则集的简化示例

---

规则 4 允许任何目标端口号大于 1023 的外部流量进入。

- 例子：外部攻击者可以建立一个从攻击者 5150 号端口到内部 Web 代理服务器 8080 号端口的连接。按理说，该行为应该是被禁止的，它可能导致服务器被攻击。
- 解决方案：防火墙规则集的每一行应该添加一个源端口域。对于规则 2 和规则 4 来说，源端口号应该被设定为 25；对于规则 1 和规则 3 来说，源端口号应该被设定为大于 1023。

# SMTP 流量规则集的简化示例

---

规则 3 和规则 4 的意图是任何内部主机都可以对外发送邮件。

- ❑ 目的端口号为 25 的 TCP 数据包将路由到目的机器上的 SMTP 服务器。这种规则的问题在于 SMTP 的接收端口号为 25，这仅仅是默认设置，外部的主机很可能还在 25 号端口上配置了其他应用。
- ❑ 例子：如果应用修改后的规则 4，攻击者很可能通过发送一个源端口号为 25 的 TCP 包，得到内部机器的访问权限。
- ❑ 解决方案：在规则的每一行加入 ACK 标记域。

## 9.3.1 包过滤防火墙

---

### □ 优势

- 简单；通常对用户透明，速度非常快

### □ 弱点

- 无法防止利用特定应用的漏洞或功能所进行的攻击
- 有限的日志功能
- 不支持高级用户身份验证
- 易受TCP/IP协议漏洞攻击
- 配置不当可能导致漏洞

# 针对包过滤防火墙攻击方式及应对措施

## IP 地址欺骗攻击

- 攻击方式：攻击者从外部发送数据包，伪装成内部可信主机的源 IP 地址，试图绕过基于源地址的安全措施。
- 应对措施：丢弃所有从外部接口到达且源 IP 地址为内部地址的数据包。通常在防火墙外的路由器上实施。

## 源路由攻击

- 攻击方式：攻击者指定数据包的路由路径，试图绕过不检查源路由信息的安全措施。
- 应对措施：丢弃所有使用了源路由选项的数据包。

## 细小分段攻击

- 攻击方式：攻击者将数据包分割成极小的片段，将 TCP 头信息分散到多个片段中，试图绕过仅检查第一个片段的过滤规则。
- 应对措施：确保第一个片段包含完整的传输头信息。如果第一个片段被否决，则丢弃后续所有片段。

## 9.3.2 状态检测防火墙

---

通过创建  
出站TCP连  
接目录来  
加强TCP流  
量的规则

每个当前建立的连接都有一个条目

数据包筛选器仅允许符合此目录中某个条目的  
配置文件的数据包进入编号较高的端口

---

查看数据  
包信息，  
但也记录  
有关TCP连  
接的信息

跟踪TCP序列号以防止依赖于序列号的攻击

检查FTP、IM和SIPS命令等协议的数据

---

## 9.3.2 状态检测防火墙

---

- ❑ 状态检测防火墙通过建立一个出站（outbound）TCP 连接目录来强制执行 TCP 流量的规则，如下表所示。每个当前建立的连接都有一个条目。当数据包符合这个目录中的某项时，包过滤器才允许到达高端口号的入站流量通过。
- ❑ 一个状态数据包检测防火墙不仅可以检查与包过滤防火墙相同的数据包信息，还可以记录有关 TCP 连接的信息。
- ❑ 一些状态检测防火墙还跟踪 TCP 包的序号，以阻止基于序号的攻击，如会话劫持攻击。
- ❑ 为了识别和跟踪相关的连接，一些状态检测防火墙甚至限制了一些众所周知的协议如 FTP、HTTP、IM 和 SIP 命令等的应用数据量。

## 9.3.2 状态检测防火墙

---

源地址	源端口	目的地址	目的端口	连接状态
192.168.1.100	1030	210.9.88.29	80	已建立
192.168.1.102	1031	216.32.42.123	80	已建立
192.168.1.101	1033	173.66.32.122	25	已建立
192.168.0.106	1035	177.231.32.12	79	已建立
223.43.21.231	1990	192.168.1.6	80	已建立
219.22.123.32	2112	192.168.1.6	80	已建立
210.99.212.18	3321	192.168.1.6	80	已建立
24.102.32.23	1025	192.168.1.6	80	已建立
223.21.22.12	1046	192.168.1.6	80	已建立

## 补充： 防火墙的基本原理

---

- 例如，如果用户不希望来自**206.246.131.227**的人访问自己的站点，那么就可以在防火墙上配置过滤规则阻止**206.246.131.227**的连接请求，禁止他们的访问。
- 在这些人的终端上，他们可以见到“**Connection Refused**”(连接被拒绝)的消息或其他相似的内容(或者他们什么也接收不到，连接就中断了)。



## 补充： 防火墙的基本原理

---

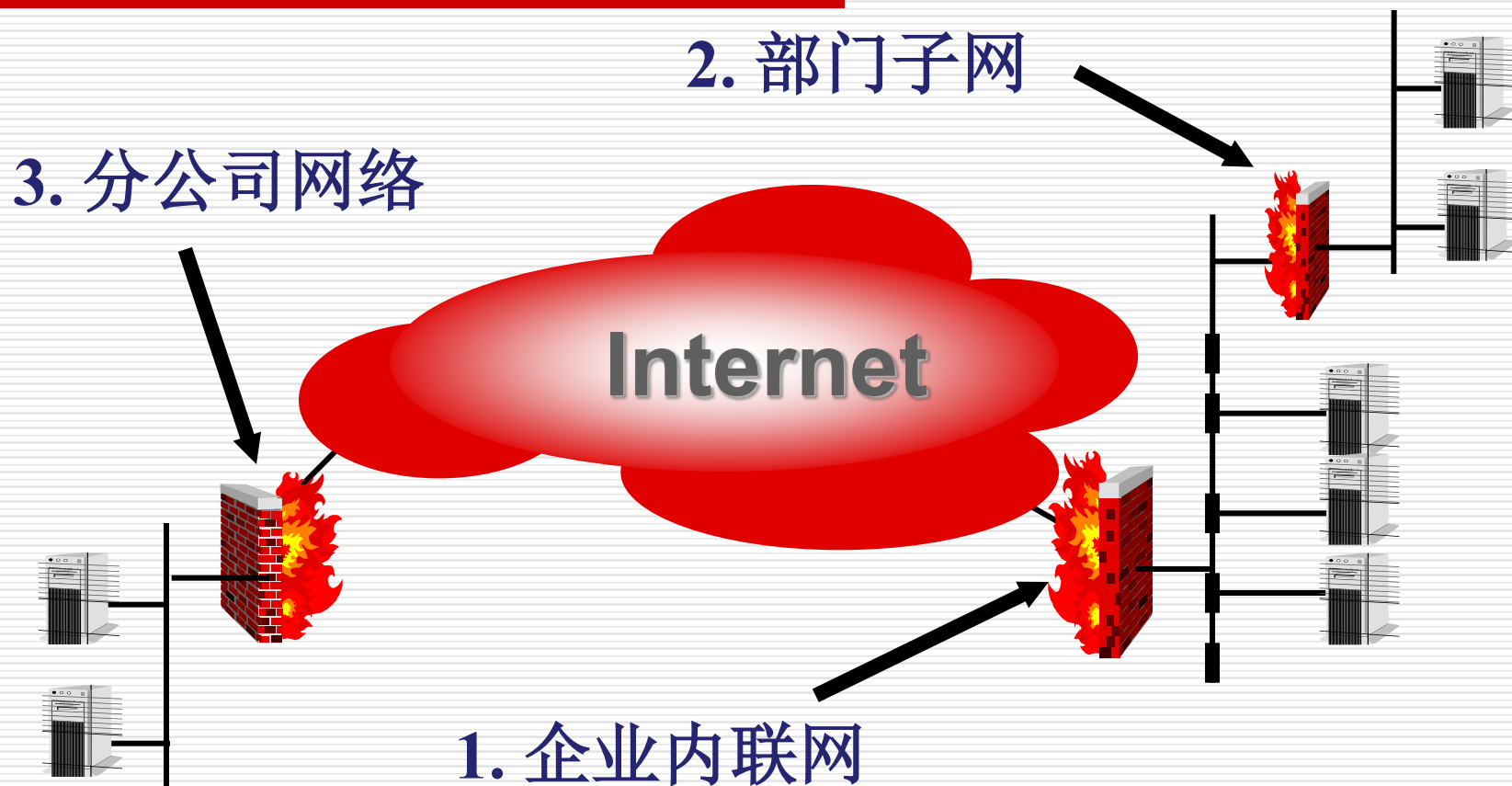
- 防火墙通常是单独的计算机、路由器或防火墙盒（专有硬件设备），他们充当访问网络的唯一入口点，并且判断是否接受某个连接请求。
- 只有来自授权主机的连接请求才会被处理，而剩下的连接请求被丢弃。

## 补充： 防火墙的基本原理

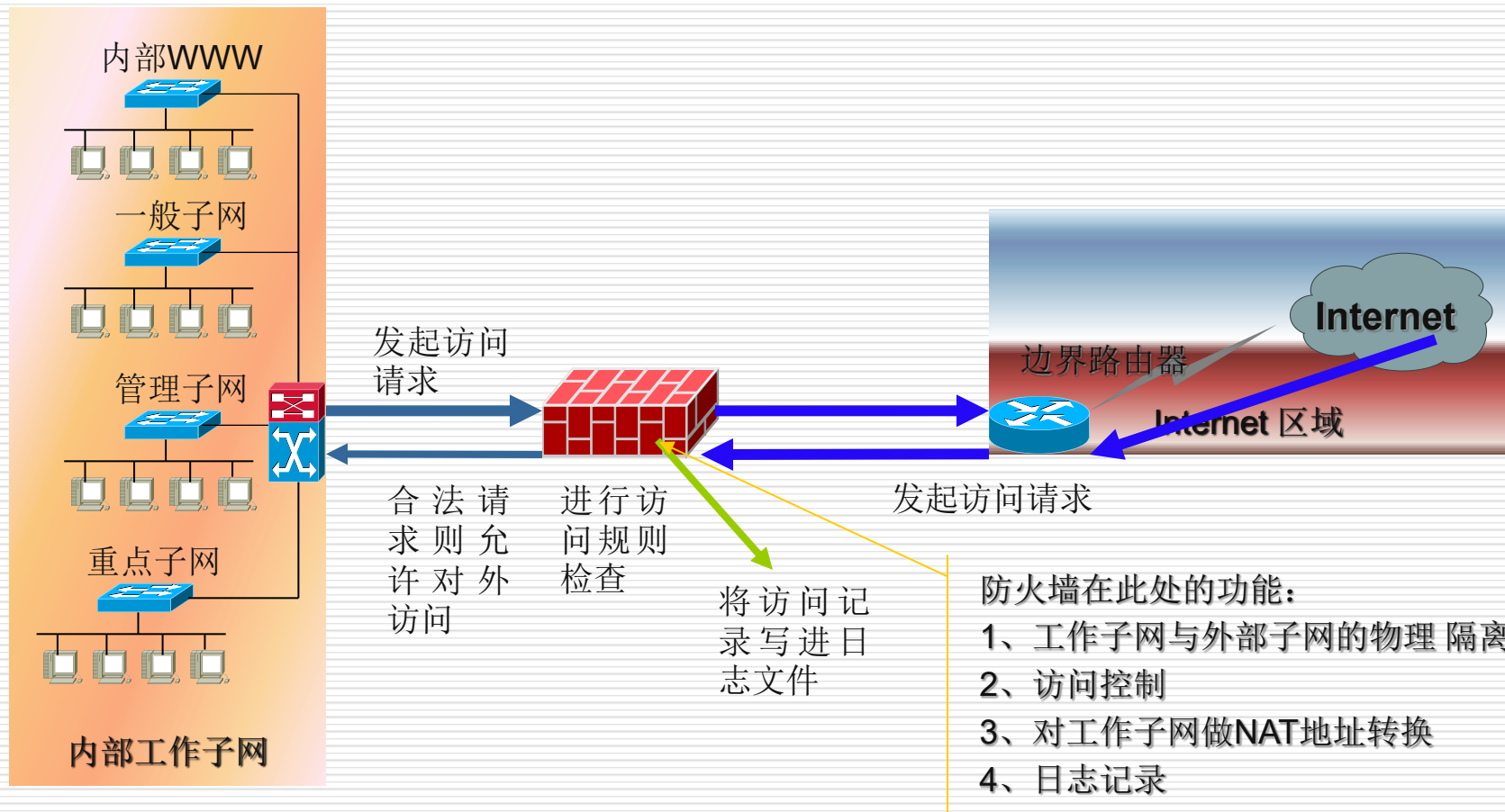
---

- 防火墙主要用于保护内部安全网络免受外部网不安全网络的侵害。
  - 典型情况：安全网络为企业内部网络，不安全网络为因特网。
- 但防火墙不只用于因特网，也可用于 **Intranet** 各部门网络之间（内部防火墙）。  
例：财务部与市场部之间。

# 补充：防火墙示意图



# 补充：一个典型的防火墙使用形态



## 补充： 防火墙的基本原理

---

- ❑ 防火墙能分析任何协议的报文。基于它的分析，防火墙可以采取各种行动。
- ❑ 防火墙实现数据流控制的功能是通过预先设定安全规则来实现的。安全规则由匹配条件和处理方式两个部分组成：如果满足这个条件，将执行这种动作。
- ❑ 通常，这些规则由系统管理员根据自己组织中的访问策略镜像来制订和装备。

# 补充：防火墙的基本策略

---

- 大多数防火墙规则中的处理方式包括：
  - Accept: 允许数据包或信息通过
  - Reject: 拒绝数据包或信息通过，并且通知信息源该信息被禁止
  - Drop: 直接将数据包或信息丢弃，并且不通知信息源
- 所有的防火墙在规则匹配的基础上都会采用以下两种基本策略中的一种：
  - 没有明确禁止的行为都是允许的
  - 没有明确允许的行为都是禁止的

# 防火墙的基本策略

---

## □ 没有明确禁止的行为都是允许的

- “默认拒绝”原则
- 当防火墙采用这条基本策略时，规则库主要由处理方式为Accept的规则构成
- 通过防火墙的信息逐条与规则进行匹配，只要与其中任何一条匹配，则允许通过，如果不能与任何一条规则匹配则认为该信息不能通过防火墙。

## □ 没有明确允许的行为都是禁止的

- “默认允许”原则
- 基于该策略时，防火墙中的规则主要由处理手段为Reject或Drop的规则组成
- 通过防火墙的信息逐条与规则进行匹配，一旦与规则匹配就会被防火墙丢弃或禁止，如果信息不能与任何规则匹配，则可以通过防火墙。

## □ 前者比较严格，后者则相对宽容。可以灵活结合这两者进行规则制订。

## 补充：包过滤防火墙

---

- 在基于**TCP/IP**协议的网络上，所有往来的信息都是以一定格式的信息包的形式传送，包中包含发送者的**IP**地址和接受者的**IP**地址信息。
- 当这些信息包被送上因特网时，路由器会读取接受者的**IP**并选择一条合适的物理线路发送出去，信息包可能经由不同的线路抵达目的地，当所有的包抵达目的地后会重新组装还原。



## 补充：包过滤防火墙（2）

---

- 包过滤式防火墙会在系统进行**IP**数据包转发时设定访问控制列表，检查所有通过的数据包信息，并按照给定的规则进行访问控制和过滤。
- 如果对防火墙设定某一**IP**地址的站点为不适宜访问的话，那么，从这个地址来的所有信息都会被防火墙屏蔽掉。

# 包过滤防火墙（3）

---

- 包过滤防火墙可以在一台路由器中实现，路由器采用包过滤功能以增强网络的安全性。
- 许多商业路由器产品都可以通过编程实现包过滤功能，如**Cisco**、**Bay Networks**、**3COM**、**DEC**、**IBM**等路由器产品。

## 补充：包过滤防火墙（4）

---

- 当前，几乎所有的包过滤装置（过滤路由器或包过滤网关）都是按如下**6**种方式操作：
- **(1).**对于包过滤装置的有关端口必须设置包过滤准则，也称为过滤规则。
- **(2).**当一个数据包到达过滤端口时，将对该数据包的头部进行分析。大多数包过滤装置只检查**IP**、**TCP**或**UDP**头部内的字段。
- **(3).**包过滤规则按一定的顺序存储。当一个包到达时，将按过滤规则的存储顺序依次运用每条规则对包进行检查。

## 补充：包过滤防火墙（5）

---

- **(4).**如果一条规则禁止传递或接收一个包，则不允许该数据包通过。
- **(5).**如果一条规则允许传递或接收一个包，则允许该数据包通过。
- **(6).**如果一个数据包不满足任何规则，则该包被阻塞。

# 补充：包过滤技术发展阶段（1）

---

## □ 第一代：静态包过滤

- 这种类型的防火墙根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。
- 过滤规则基于数据包的报头信息进行制定。
- 包过滤类型的防火墙要遵循的一条基本原则是“最小特权原则”，即明确允许那些管理员希望通过的数据包，禁止其他的数据包

# 静态包过滤原理

Source	Destination	Permit	Protocol
Host A	Host C	Pass	TCP
Host B	Host C	Block	UDP

控制策略

查找对应的  
控制策略

根据策略决定如  
何处理该数据包

拆开数据包

数据包

安全网域

Host C Host D

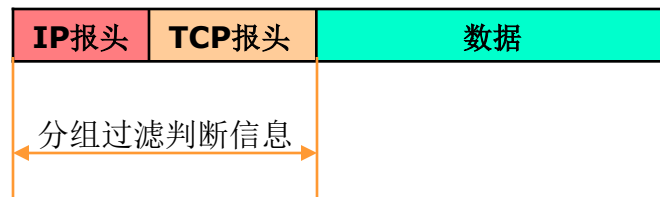
数据包

数据包

数据包



过滤依据主要是TCP/IP报头里面的  
信息，不能对应用层数据进行  
处理



# 补充：包过滤技术发展阶段（2）

---

## □ 第二代：动态包过滤

- 该类防火墙避免了静态包过滤所具有的问题，采用动态设置包过滤规则的方法，后来发展成为所谓**包状态检测技术**。
- 它采用了一个在网关上执行网络安全策略的软件引擎，称之为**检测模块**。
- 检测模块在不影响网络正常工作的前提下，采用抽取相关数据的方法对网络通信的各层实施检测，建立状态连接表，并将进出网络的数据当成一个个会话，通过状态表跟踪会话状态，动态更新状态连接表。
- 它不仅根据规则表，更考虑了数据包是否符合会话所处的状态，提供了完整的对传输层的控制能力。

# 补充：包过滤技术发展阶段（3）

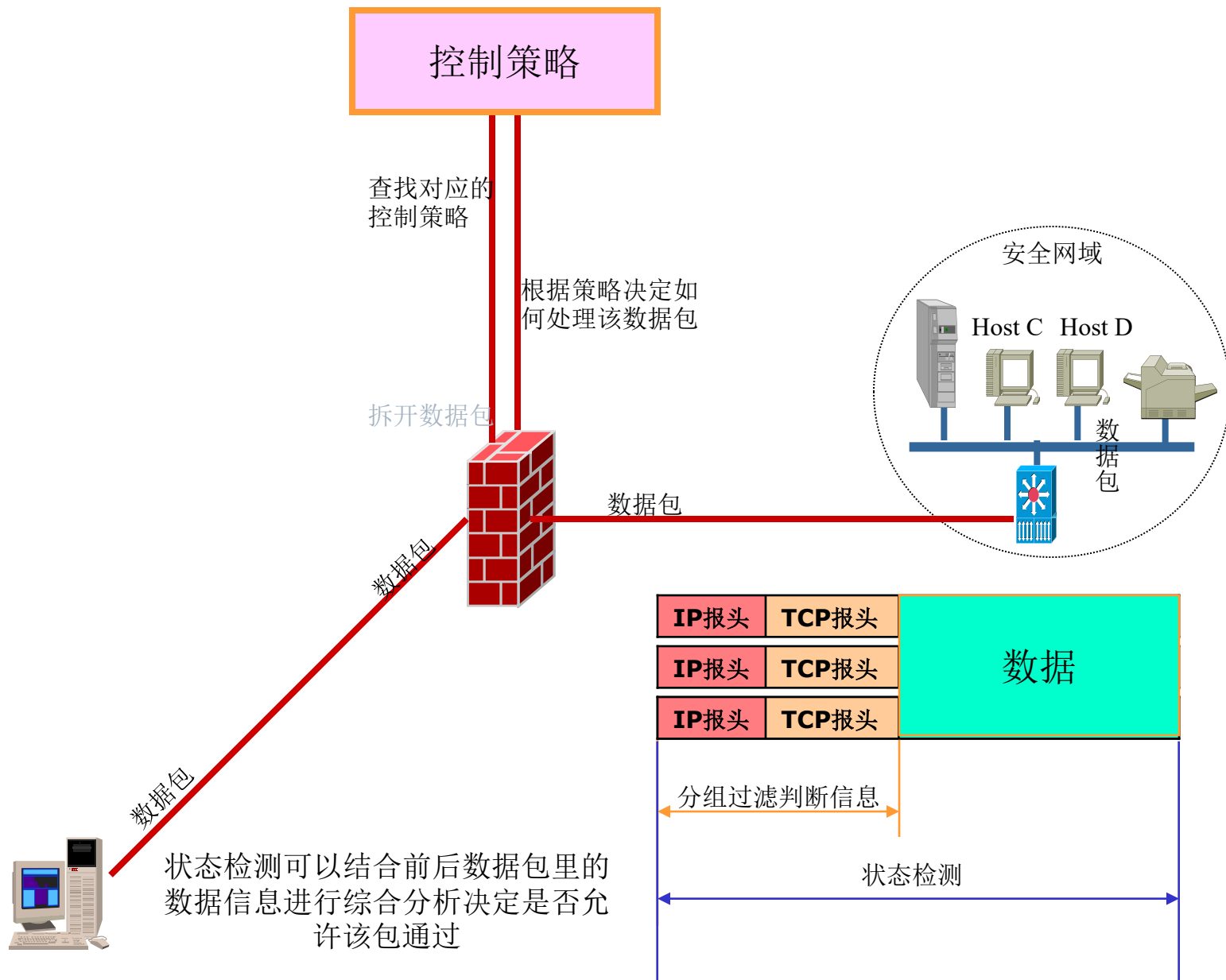
---

## □ 第二代：动态包过滤（续）

- 此技术对网络通信的各层实施监测分析，提取相关的通信和状态信息，并在动态连接表中进行状态及上下文信息的存储和更新，这些表被持续更新，为下一个通信检查提供累积的数据。
- 能够提供对基于无连接的协议（UDP）的应用（DNS、WAIS、etc）及基于端口动态分配的协议（RPC）的应用（如NFS、NIS）的安全支持，静态的包过滤和代理网关都不支持此类应用。



# 状态检测原理



## 9.3.3 应用级网关

---

- 也称为应用程序代理
- 充当应用级流量中继器
  - 用户使用TCP/IP应用程序联系网关
  - 用户已通过身份验证
  - 网关联系远程主机上的应用程序，并在服务器和用户之间中继TCP段
- 每个应用程序都必须有代理代码
  - 可能会限制支持的应用程序功能
- 往往比数据包过滤器更安全，缺点是每个连接上都有额外的处理开销

## 9.3.4 电路级网关

### 电路级代理服务器

- 建立两条TCP连接，一条在自身和内部主机TCP用户之间，另一条在自身和外部主机TCP用户之间
- 将TCP段从一个连接中继到另一个连接，而不检查内容
- 安全功能包括判断哪些连接是允许的

### 通常在内部用户受信任时使用

- 可以使用应用级网关入站和电路级网关出站
- 降低日常开销

## 9.3.4 电路级网关

### SOCKS电路级网关

- ❑ FC1928中定义了SOCKS的第5版
- ❑ 旨在为TCP和UDP域中的客户端—服务器应用程序提供框架，以便于安全地使用网络防火墙的服务
- ❑ 客户端应用程序联系SOCKS服务器，进行身份验证，发送中继请求
- ❑ 服务器评估并建立或拒绝连接



# 内容安排

---

- 9.1 防火墙的必要性
- 9.2 防火墙的特征和访问策略
- 9.3 防火墙的类型
- 9.4 防火墙的布置
- 9.5 防火墙的部署和配置
- 9.6 入侵防御系统
- 9.7 实例：一体化威胁管理产品

## 9.4 防火墙的布置

---

- 9.4.1 堡垒主机
- 9.4.2 基于主机的防火墙
- 9.4.3 网络设备防火墙
- 9.4.4 虚拟防火墙
- 9.4.5 个人防火墙

## 9.4.1 堡垒主机

---

- ❑ 系统被确定为网络安全的关键优势
- ❑ 用作应用级或电路级网关的平台
- ❑ 常见特征：
  - 运行操作系统的安全版本，仅提供基本服务
  - 可能需要用户身份验证才能访问代理或主机
  - 每个代理都可以限制访问的功能和主机
  - 每个代理模块是专门为网络安全设计的非常小的软件包，经过安全检查
  - 每个代理都是独立的、非特权的
  - 磁盘使用有限，因此为只读代码

## 9.4.2 基于主机的防火墙

基于主机的防火墙是一个用于保障个人主机安全的软件模块。

这个模块在许多操作系统中是自带的，或者以附件的形式提供。

主机驻留（host-resident）防火墙能够过滤和限制数据包流。

通常，这样的防火墙位于服务器上。

优势：

可以根据主机环境定制过滤规则

保护独立于拓扑结构提供

提供额外的保护层



## 9.4.3 网络设备防火墙

---

- ❑ 防火墙功能，尤其是数据包过滤和状态检测功能，通常在网络设备（如路由器和交换机）中提供以监视和过滤通过设备的数据包流。
- ❑ 它们用于与堡垒主机和基于主机的防火墙一起提供额外的保护层。

## 9.4.4 虚拟防火墙

---

- ❑ 在虚拟化环境中，不是使用物理上独立的设备作为服务器、交换机、路由器或防火墙堡垒主机，而是使用这些设备的虚拟化版本，共享相同的物理硬件。
- ❑ 管理该环境中的虚拟机的管理程序也可以提供防火墙功能。

## 9.4.5 个人防火墙

---

- ❑ 控制个人计算机或工作站与Internet或企业网络之间的网络流量
- ❑ 供家庭或公司使用
- ❑ 通常是个人计算机上的软件模块
- ❑ 可以安装在路由器中，该路由器将所有家庭计算机连接到DSL、电缆调制解调器或其他互联网接口
- ❑ 通常比基于服务器或独立防火墙简单得多
- ❑ 主要作用是拒绝未经授权的远程访问
- ❑ 监控出站活动，来试图检测和阻断蠕虫和其它的恶意软件的行为

# 内容安排

---

- 9.1 防火墙的必要性
- 9.2 防火墙的特征和访问策略
- 9.3 防火墙的类型
- 9.4 防火墙的布置
- 9.5 防火墙的部署和配置
- 9.6 入侵防御系统
- 9.7 实例：一体化威胁管理产品

## 9.5 防火墙的部署和配置

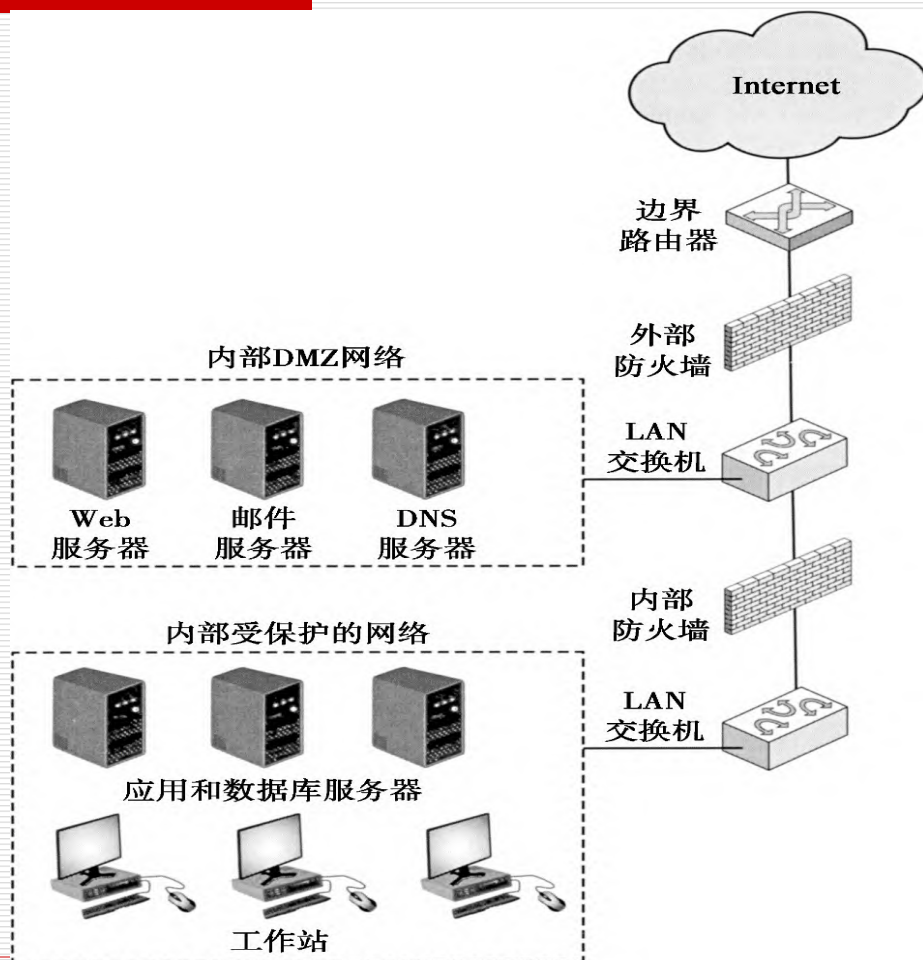
---

- 9.5.1 DMZ网络
- 9.5.2 虚拟专用网络
- 9.5.3 分布式防火墙
- 9.5.4 防火墙部署和拓扑结构小结

## 9.5.1 DMZ网络

右图为防火墙配置示例

- 外部防火墙被设置在局域网或者企业网络的边缘，紧接在连接Internet或者某个广域网（WAN）的边界路由的内侧。
- 一个或更多内部防火墙则负责保护企业内部网。



## 9.5.1 DMZ网络

---

### 外部防火墙目的:

- 为DMZ系统提供符合其需要并同时保证其外部连通性的访问控制和保护措施。
- 同时也为企业网络的其它部分提供基本的安全保护。

### 内部防火墙有如下三个服务目的:

- 增加了更严格的过滤能力
- 对于DMZ网络，内部防火墙提供双重的保护功能。
- 多重内部防火墙可以用来分别保护内部网的每个部分不受其它部分的攻击，

## 9.5.2 虚拟专用网络VPN

定义：一组通过公共网络（如Internet）相互连接的计算机，利用加密技术和特殊协议提供安全性。

用途：为远程工作者和移动职员提供对公司系统的访问途径，节省专用网络成本，并将广域网管理任务转移给服务提供商。

### 安全需求

挑战：公共网络暴露了公司通信，使其易受窃听和未授权访问威胁。

解决方案：通过VPN使用加密和身份验证技术，在不安全网络环境中建立安全连接。



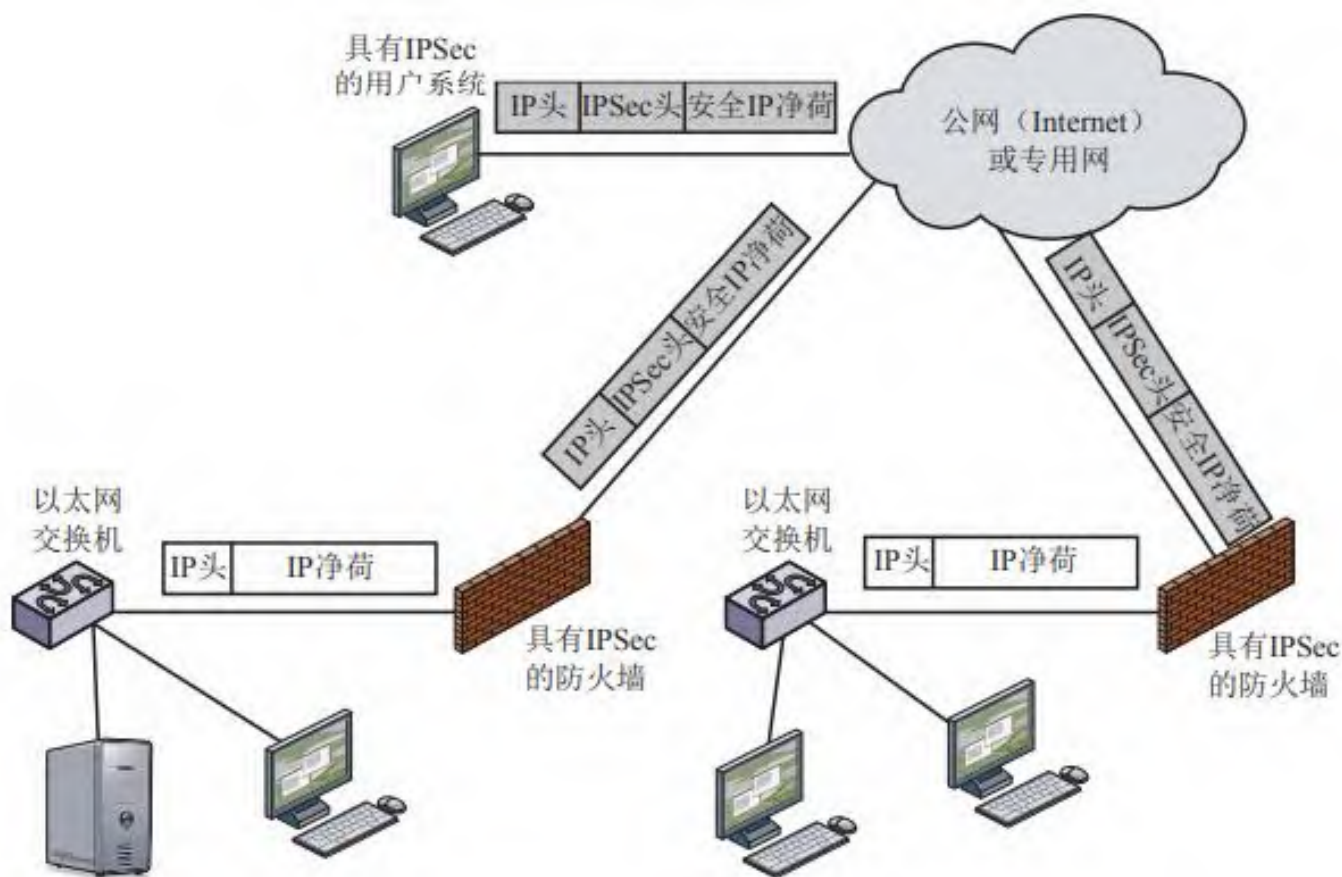
## 9.5.2 虚拟专用网络VPN

---

### IPSec协议（IP 安全）

- 功能：在IP层面上提供加密、解密、压缩、解压缩及认证功能，确保数据传输的安全性。
- 应用：在网络设备中工作，例如路由器或防火墙，负责局域网与外网的连接。
- 透明性：对局域网上的工作站和服务器是透明的，不影响用户操作。

# 一个VPN安全场景



## 9.5.2 虚拟专用网络VPN

---

### 防火墙内部部署：

- 数据流双向加密。
- 防火墙无法执行过滤、日志记录或病毒扫描等安全功能。

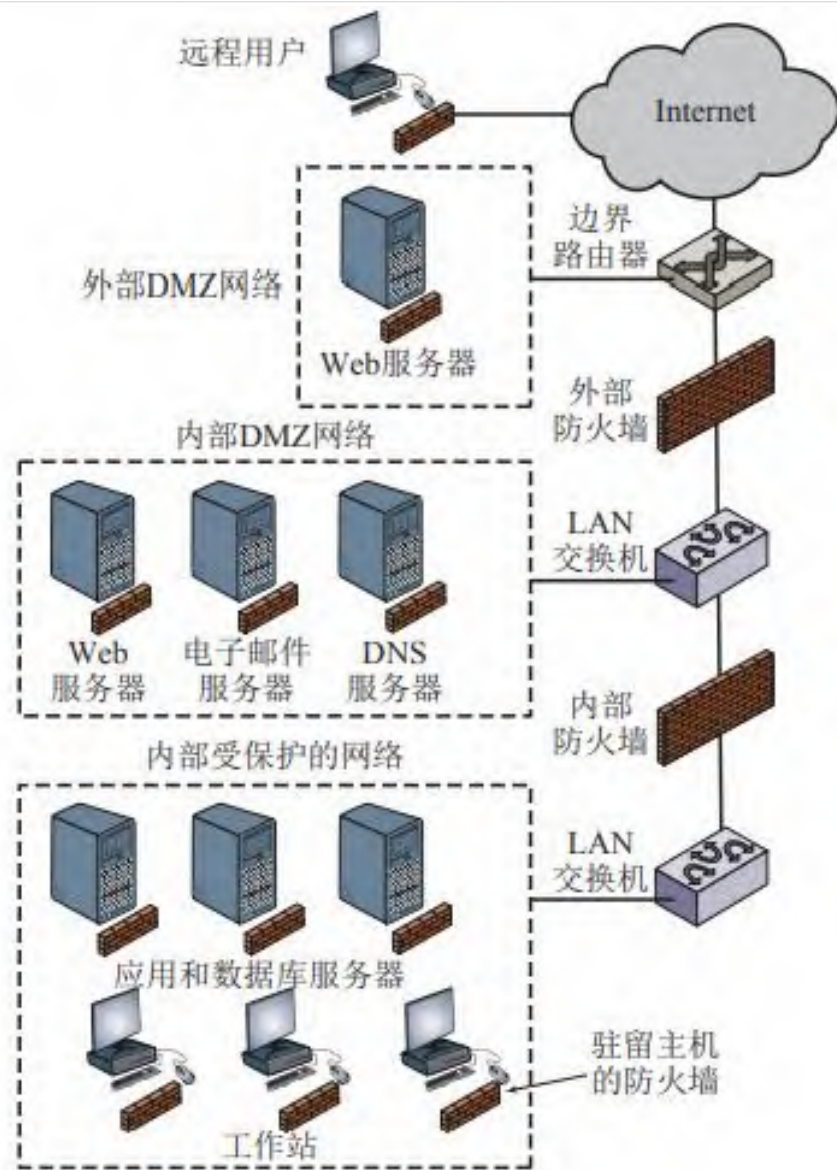
### 边界路由器部署：

- 可能比防火墙部署更不安全。
- 设备本身的安全性较低，可能影响用户对IPSec平台的信任度。

## 9.5.3 分布式防火墙

右图分布式防火墙配置示例

- 管理员可以在数百个服务器和工作站上配置驻留主机的防火墙，同时在本地和远程用户系统上配置个人防火墙。
- 许多工具允许网络管理员穿过整个网络设定安全策略和监视网络的安全。



## 9.5.4 防火墙部署和拓扑结构小结

主机驻留防火墙	包括个人防火墙软件和服务器上的防火墙软件
屏蔽路由器	外部网络与内部网络之间具有无状态或者全部包过滤功能的单个路由器
独立内嵌堡垒主机	位于内部和外部路由器之间的单个防火墙物理或虚拟设备
独立T型堡垒主机	有能够连接到部署着能够被外界访问的服务器的DMZ的第三方网络接口
双内嵌堡垒主机	DMZ被夹在两个堡垒防火墙中间
双T型堡垒主机	DMZ位于堡垒防火墙的一个独立的网络接口上。
分布式防火墙配置	被大型商业机构和政府部门使用

# 内容安排

---

- 9.1 防火墙的必要性
- 9.2 防火墙的特征和访问策略
- 9.3 防火墙的类型
- 9.4 防火墙的布置
- 9.5 防火墙的部署和配置
- 9.6 入侵防御系统
- 9.7 实例：一体化威胁管理产品

## 9.6 入侵防御系统

---

- 9.6.1 基于主机的IPS
- 9.6.2 基于网络的IPS
- 9.6.3 分布式或混合式IPS
- 9.6.4 Snort Inline

## 9.6 入侵防御系统

---

- ❑ 也称为入侵检测防御系统（IDPS）
- ❑ 它是IDS的扩展，能够尝试阻止或预防检测到的恶意活动
- ❑ 基于主机、基于网络、基于分布式或混合式这几种类别
- ❑ 异常检测来识别非法用户的行为，或者用特征和启发式检测来识别已知的恶意行为
- ❑ 像防火墙一样，可以阻断网络流量，但却需要根据预设的算法来决定后面该干些什么



## 9.6.1 基于主机的IPS

可以使用特征/启发式检测或异常检测来识别攻击

- 特征：重点在于从应用程序网络流量的内容或系统调用的顺序之中，查找可被认为是恶意行为的特征
- 异常：IPS主要寻找能够表明某软件为恶意的行为模式

**HIPS处理的恶意行为类型示例包括：**

- 修改系统资源
- 提权攻击
- 缓冲区溢出攻击
- 访问电子邮件通信录
- 目录遍历

## 9.6.1 基于主机的IPS

为特定的平台作适当的定制

一套通用的工具可以在台式系统或者服务器系统中使用

一些HIPS套装被设计用来保护特定种类的服务器，例如Web服务器和数据库服务器

- 在这种情形，HIPS搜寻特殊的应用攻击。

可以使用沙箱方法

- 沙箱特别适合移动代码，如Java小程序和脚本语言
- HIPS将这些代码隔离在一个独立的系统区域内，然后运行它并监视其行为

HIPS通常提供桌面保护的区域：系统调用；文件系统访问；系统注册表设置；主机输入/输出

## 9.6.1 基于主机的IPS

### HIPS的角色

- 许多行业观察员注意到企业终端，包括桌面系统和便携式电脑系统，已经成为了黑客活动和犯罪的主要目标
  - 因此，安全设备提供商们现在更加重视终端安全产品的开发
  - 传统的终端安全是由一系列功能不同的产品共同提供的，比如反病毒软件、反垃圾邮件软件和个人防火墙
- 该方法旨在由单一产品提供集成的功能组
  - 集成的HIPS方法的优点是多种工具配合紧密，威胁防护更加广泛，管理也更简单
- 更为谨慎的做法是将**HIPS**作为涉及网络层设备（例如，防火墙或者基于网络的IPS）的一整套策略中的一个组件使用

## 9.6.2 基于网络的IPS

---

- ❑ 具有修改或丢弃数据包和断开TCP连接权限的内嵌NIDS
- ❑ 使用诸如特征/启发式检测和异常检测之类的技术
- ❑ 可提供流数据的保护
- ❑ 求对一个数据包序列中的应用净荷进行重组
- ❑ 用于识别恶意数据包的方法：

模式  
匹配

状态  
匹配

协议  
异常

传输  
异常

统计  
异常

## 9.6.3 分布式或混合式IPS

---

### 分布式或混合式IPS

收集大量基于主机和基于网络的传感器数据，将其传送到中央处理系统。

而中央处理系统能够对这些数据进行关联分析，并更新特征和行为模式，从而使得所有的协作系统可以应对和防御恶意行为。

目前已经有若干这样的系统被提出，其中最为著名的就是**数字免疫系统**（digital immune system）。

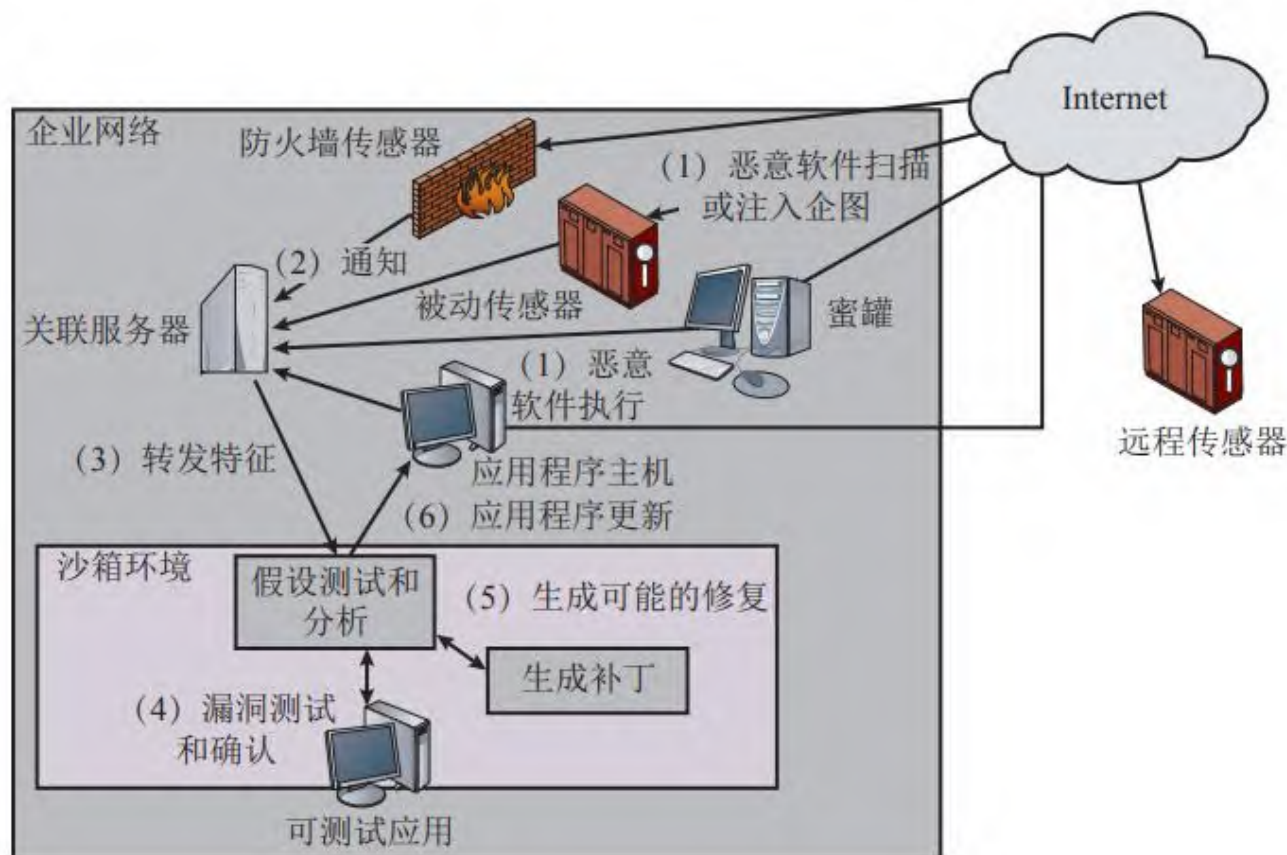
## 9.6.3 分布式或混合式IPS

### 数字免疫系统

- 全面防御恶意软件引起的恶意行为
- 由IBM开发，Symantec完善
- 这一发展的动机主要有基于网络的恶意软件的威胁、由Internet所带来的不断增长的传播速度以及对该情形全面掌控的需求
- 数字免疫系统能否成功主要取决于恶意软件分析系统检测新的恶意软件的能力

# 恶意软件监控系统的布置

右图展示了一个最初被设计用来检测蠕虫的混合式架构的例子



## 9.6.4 Snort Inline

使Snort能够作为入侵防御系统发挥作用

包括一个可替换选项，该选项允许Snort用户修改数据包，而不是丢弃数据包

对蜜罐实现有用

攻击者看到了故障，但无法找出其原因

Snort Inline 加入了 3 种新的规则来提供入侵防御功能：

- 丢弃
  - 依据规则中定义的规则拒绝数据包，并将结果记录下来
- 拒绝
  - 拒绝一个数据包并且记录结果，还返回一个错误消息
- 简单丢弃
  - 拒绝一个数据包，但是并不记录它



# 内容安排

---

- 9.1 防火墙的必要性
- 9.2 防火墙的特征和访问策略
- 9.3 防火墙的类型
- 9.4 防火墙的布置
- 9.5 防火墙的部署和配置
- 9.6 入侵防御系统
- 9.7 实例：一体化威胁管理产品

## 9.7 实例：一体化威胁管理产品

一体化威胁管理（unified threat management, **UTM**）系统

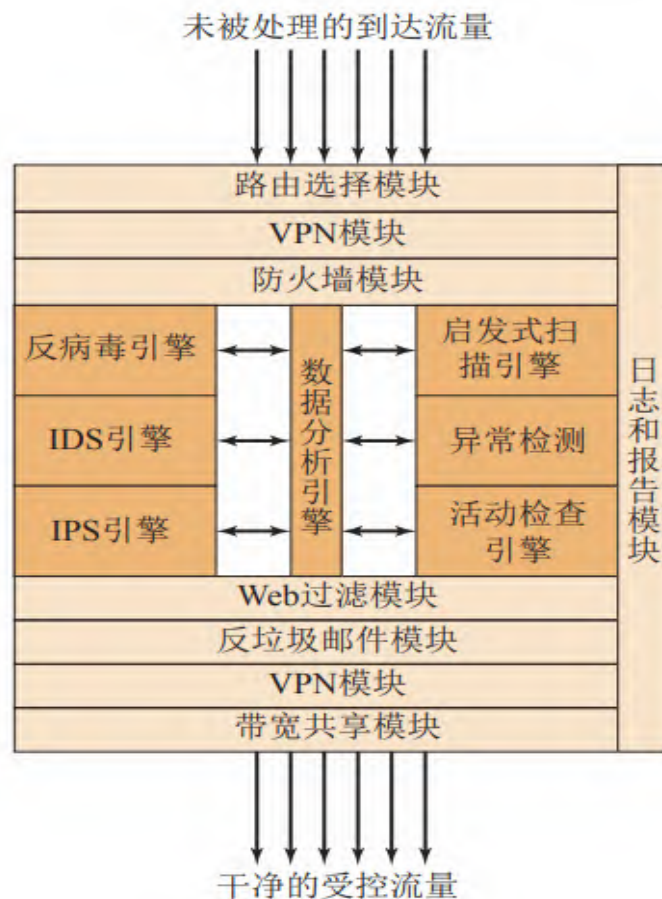
将多种安全特性集成在一个盒子里的产品。

包含在这一类中的设备，必须能够实现网络防火墙、网络入侵检测和防护，以及反病毒网关的功能。

设备的全部功能不一定要同时使用，但必须固有地存在于该设备中。

## 9.7 实例：一体化威胁管理产品

右图是一个典型的UTM设备的体系结构



# 实例：

## 右表 Sidewinder G2安全设 备攻击防护 摘要—传输 层举例

攻击和 Internet 威胁	防护措施
TCP	
无效的端口号 无效的序列号 编号 SYN 洪流 XMAS 树攻击 无效的 CRC 校验值 零长度字符串 随机数据作为 TCP 头部 TCP 劫持攻击 TCP 欺骗攻击 小 PMTU（路径最大传输单元）攻击 SYN 攻击 脚本小子攻击 分组骗术：利用不同的 TCP 选项集	强制使用正确 TCP 标记 强制使用 TCP 报文头长度 确保正确的 3 次握手 正确地关闭 TCP 会话 将会话分为内部会话和外部会话两段 强制使用正确的 TCP 标记法 管理 TCP 会话超时 阻止 SYN 攻击 重组数据包确保正确性 适当处理 TCP 超时和重传计时器 所有 TCP 代理都受到保护 通过访问列表进行传输控制 在未打开的端口处丢弃 TCP 包 代理阻止分组骗术
UDP	
无效的 UDP 包 利用随机 UDP 数据以绕开规则 连接预测 UDP 端口扫描	验证正确的 UDP 包 在未打开的端口处丢弃 UDP 包

# 实例：

## 右表 Sidewinder G2安全设 备攻击防护 摘要—应用 层举例 (1/3)

攻击和 Internet 威胁	保护措施
DNS	
对 AAAA 查询错误的 NXDOMAIN 响应可能引起拒绝服务条件	不允许负缓存 (negative caching) 防止 DNS 缓存中毒
ISC BIND 9 在 9.2.1 之前的版本允许远程攻击者用一个有缺陷的 DNS 包来引起一次拒绝服务 (关机)。该包触发一个错误条件, 即当 message.c 中的 dns_message_findtype() 函数中的 rdataset 参数不为 NULL 时, 该包不能被正确处理	错误形成的 DNS 消息会影响防火墙的运行, Sidewinder G2 可以防止这样的恶意使用 防止 DNS 查询攻击 防止 DNS 应答攻击
攻击和 Internet 威胁	保护措施
DNS 信息阻碍及其他 DNS 滥用	预防区域传输和区域查询 真正的基于 Type Enforcement 技术的 DNS 分割保护, 将 DNS 划分为公共 DNS 区域和专用 DNS 区域 关闭递归的能力
FTP	
FTP 反弹攻击 PASS 攻击 FTP 端口注入攻击 TCP 分段攻击	Sidewinder G2 可以过滤 FTP 命令以阻止这些攻击 真正的网络隔离阻止分段攻击
SQL	
SQL 网络中间人攻击	受 Type Enforcement 技术保护的智能代理 经过非透明连接隐藏内部 DB



# 实例：

## 右表 Sidewinder G2安全设 备攻击防护 摘要—应用 层举例 (2/3)

实时流协议（RTSP）	
缓冲区溢出 拒绝服务	受 Type Enforcement 技术保护的智能代理 协议验证 拒绝多播流量 检查建立和拆除的方法 验证 PNG 和 RSTP，丢弃所有其他的数据包 辅助端口的监视
SNMP	
SNMP 洪泛攻击 默认团体攻击 暴力攻击 SNMP 攻击	过滤 SNMP 版本 1、2c 的网络流量 过滤读、写和通知消息 过滤 OIDS 过滤 PDU（协议数据单元）
SSH	
挑战 - 响应缓冲区溢出 SSHD 允许用户覆盖 “Allowed Authentication” 位 OpenSSH buffer_append_space 缓冲区溢出 OpenSSH/PAM 挑战 - 响应缓冲区溢出 OpenSSH 信道代码 offer-by-one	Sidewinder G2 v6.x 中嵌入的 Type Enforcement 技术严格限制了 Secure Computing 对 OpenSSH 守护进程代码的版本修改的能力
SMTP	
Sendmail 缓冲区溢出 Sendmail 拒绝服务攻击 Sendmail 的远程缓冲区溢出 Sendmail 地址解析缓冲区溢出 SMTP 异常 SMTP 蠕虫攻击 SMTP 邮件洪泛攻击 中继攻击 病毒、木马、蠕虫	受 Type Enforcement 技术保护的 Sendmail 结构 分割 出于控制目的的 Sendmail 自定义 利用 Type Enforcement 技术防止缓冲区溢出 Sendmail 检查 SMTP 的异常情况 协议确认 反垃圾邮件过滤器 邮件过滤、依据邮件大小和关键词 特征码反病毒

# 实例：一体化威胁管理产品

右表  
Sidewinder  
G2安全设  
备攻击防护  
摘要—应用  
层举例  
(3/3)

攻击和 Internet 威胁	保护措施
电子邮件地址欺骗 MIME 攻击 网络钓鱼电子邮件	反中继 MIME/ 反病毒过滤器 防火墙反病毒 通过病毒扫描反网络钓鱼
间谍软件	
广告软件用于收集与营销相关的信息 掩护马 特洛伊木马 恶意软件 后门圣诞老人	内置于 Sidewinder G2 的 SmartFilter URL 过滤机制，经过配置能够过滤间谍软件的 URL，防止恶意下载

# 总结

防火墙的必要性

防火墙的特征和  
访问策略

防火墙的类型

防火墙的布置

- 包过滤防火墙
- 状态检测防火墙
- 应用级网关
- 电路级网关
- 堡垒主机
- 基于主机的防火墙
- 网络设备防火墙
- 虚拟防火墙
- 个人防火墙

防火墙的部署和配置

入侵防御系统

实例：一体化威胁管  
理产品

- DMZ 网络
- 虚拟专用网
- 分布式防火墙
- 防火墙部署和拓扑结构  
小结
- 基于主机的 IPS
- 基于网络的 IPS
- 分布式或混合式 IPS
- Snort Inline



---

谢谢各位!