

# 信息安全解决方案

冠群金辰  
刘海林

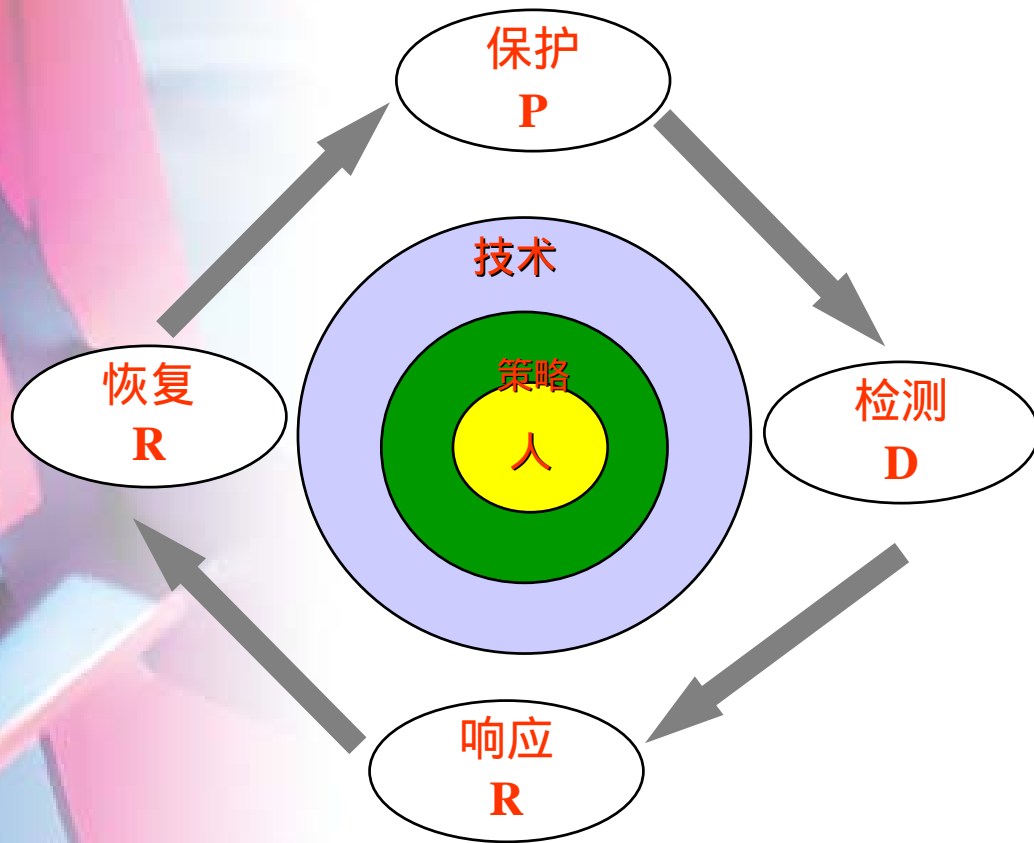
- 
- An abstract 3D graphic on the left side of the slide, featuring several rectangular blocks in shades of blue and red, arranged in a complex, overlapping structure. A thin white line curves around the top of the blocks.
- 信息安全的需求
  - 冠群金辰的解决方案
  - 冠群金辰安全产品目录

# 信息安全的历史

## 信息安全的发展经历了三个历史时期:

- 通信安全 (COMSEC)
  - 保密性。
- 信息安全 (INFOSEC)
  - 保密性、完整性、可用性。
- 信息保障 (IA)
  - 保密性、完整性、可用性、可控性、不可否认性

# 信息保障（IA）概念：PDRR模型



# PDRR模型技术及产品基础

- 保护:

- 操作系统安全、数据库系统安全访问控制、口令等保密性和完整性技术。

- 检测:

- 病毒检测、漏洞扫描、入侵检测、用户身份鉴别等技术。

- 反应:

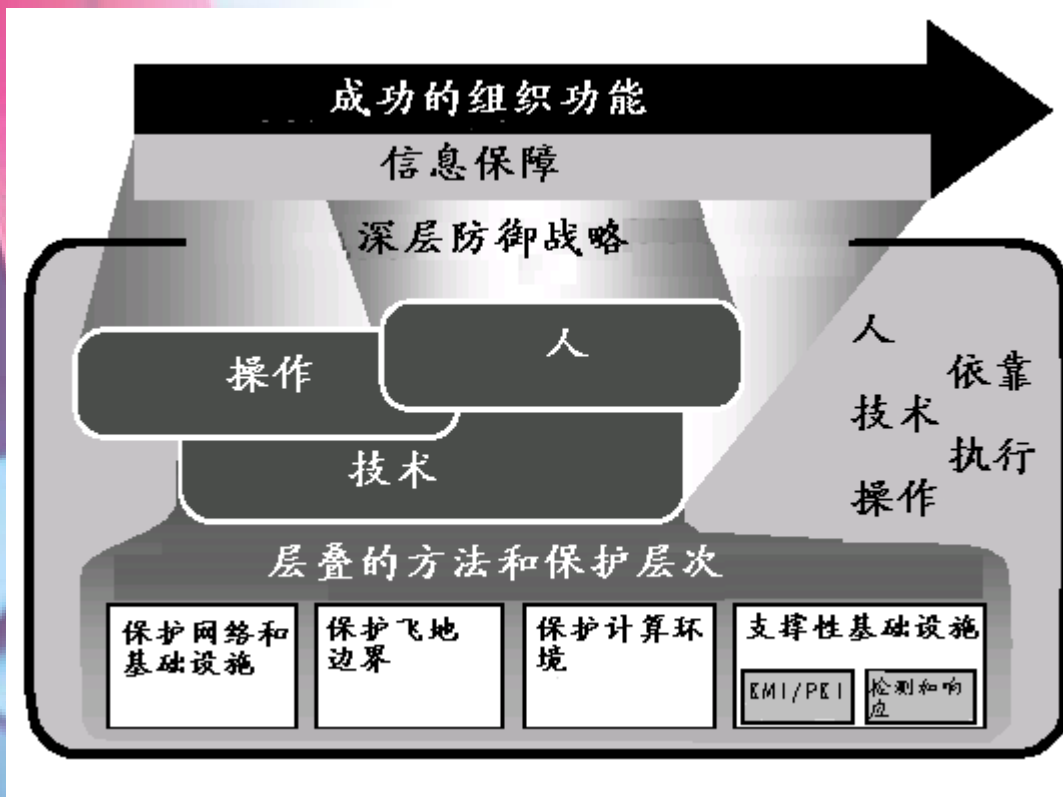
- 监视、关闭、切换、跟踪、报警、修改配置、联动、阻断等技术。

**问题: PDRR在实际网络中如何布置?**

- 恢复:

- 备份、恢复等

# IATF 深层防御战略



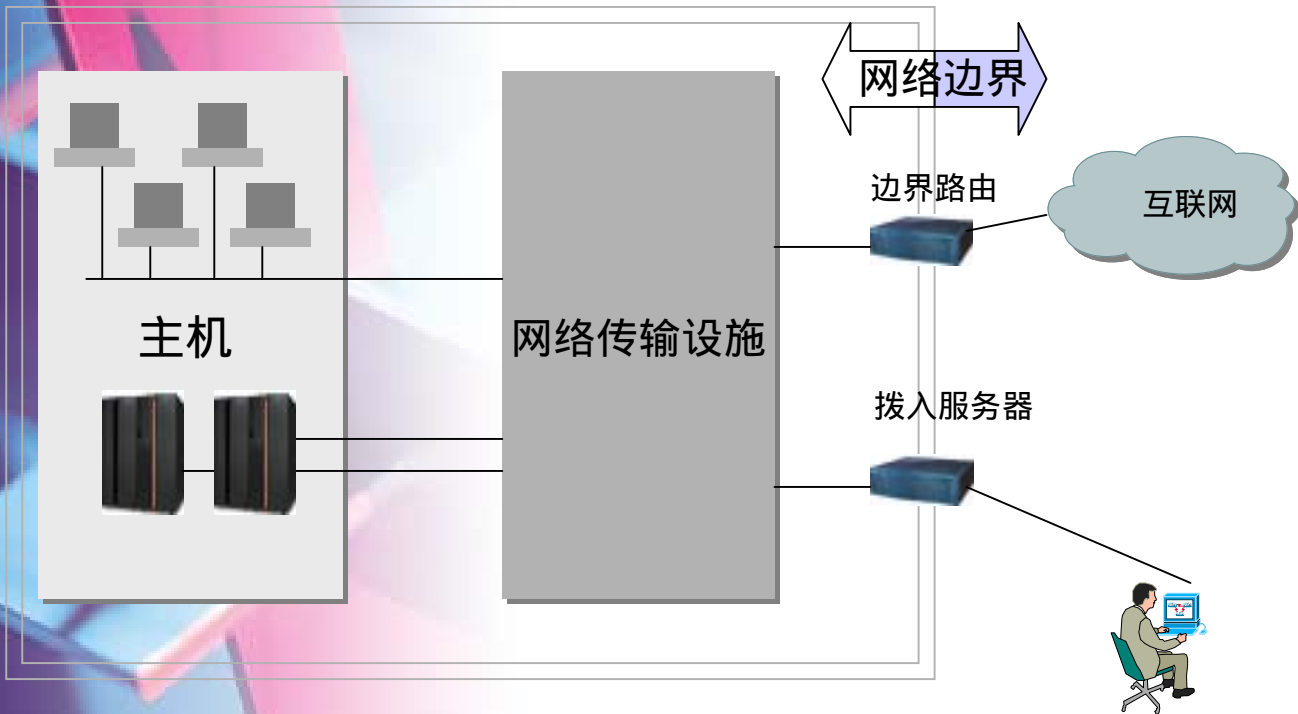
# IATF：信息保障技术层面

- 主机
- 网络传输设施
- 网络边界
- 支撑性基础设施
  - KMI /PKI
  - 检测响应中心

# IATF中PDRR的实现

网络传输设施	主机	网络边界	支撑性基础设施
骨干网管理安全	操作系统	防火墙	KMI /PKI
WLAN	IDS	IDS	IDS
	防病毒	VPN	
	漏洞扫描	漏洞扫描	
	防火墙	病毒检测	
	保密及完整性机制	身份鉴定	
		保密及完整性机制	
		签名机制	

# 深层防御战略在实际建设中的技术体现

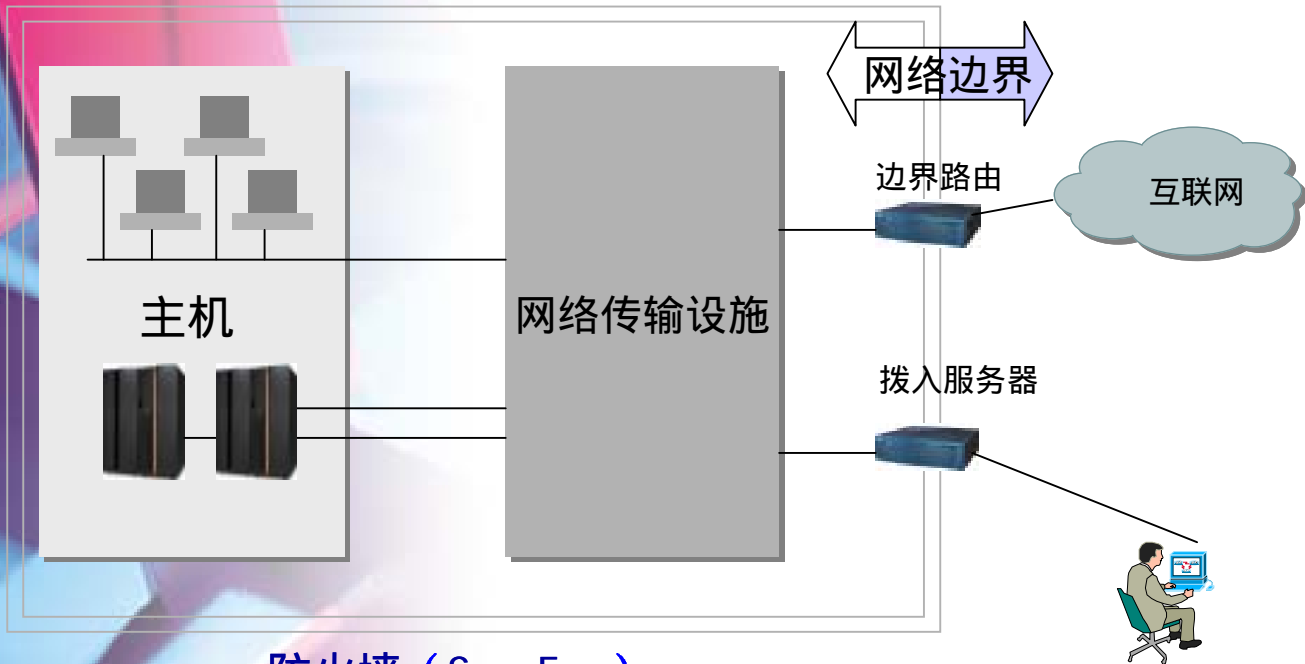


- 
- An abstract 3D graphic on the left side of the slide, featuring several rectangular blocks in shades of blue and red. The blocks are arranged in a way that suggests depth and perspective, with some overlapping others. The lighting is soft, creating a sense of volume and shadow.
- 信息安全的需求
  - 冠群金辰的解决方案
  - 冠群金辰安全产品目录

# 我们有些什么

- 👉 主机核心防护 (eTrust Access Control )
- 👉 防火墙 (SecuE)
- 👉 入侵检测系统 (eTrust Intrusion Detection)
- 👉 安全漏洞扫描系统 (eGuard Scanner)
- 👉 KILL安全胃甲系统
- 👉 邮件内容过滤系统(KILL MailShield Gateway)
- 👉 企业虚拟专用网 (eTrust VPN)

# 我们能满足用户的安全要求



- 主机核心防护 (eAC)
- 入侵检测系统 (eID)
- 边界漏网拦截系统 (Killed ManShield Gateway)
- 企业虚拟专用网 (eTrust VPN)

- 
- An abstract 3D graphic on the left side of the slide, featuring several rectangular blocks in shades of blue and red. The blocks are arranged in a way that suggests depth and perspective, with some overlapping others. The lighting is soft, creating a sense of volume and shadow.
- 信息安全的需求
  - 冠群金辰的解决方案
  - 冠群金辰安全产品目录

# 冠群金辰: 完备的安全工具

- 👉 主机核心防护 (eTrust Access Control )
- 👉 入侵检测系统 (eTrust Intrusion Detection)
- 👉 防火墙 (SecuE)
- 👉 安全漏洞扫描系统 (eGuard Scanner)
- 👉 KILL安全胃甲系统
- 👉 邮件内容过滤系统(KILL MailShield Gateway)
- 👉 企业虚拟专用网 (eTrust VPN)

# 冠群金辰: 安全产品来源

- CA公司提供产品及源码
  - 中文本地化
  - 排除原产品安全后门
- 自主开发
  - 与CA无关

# 主机核心防护（eAC）

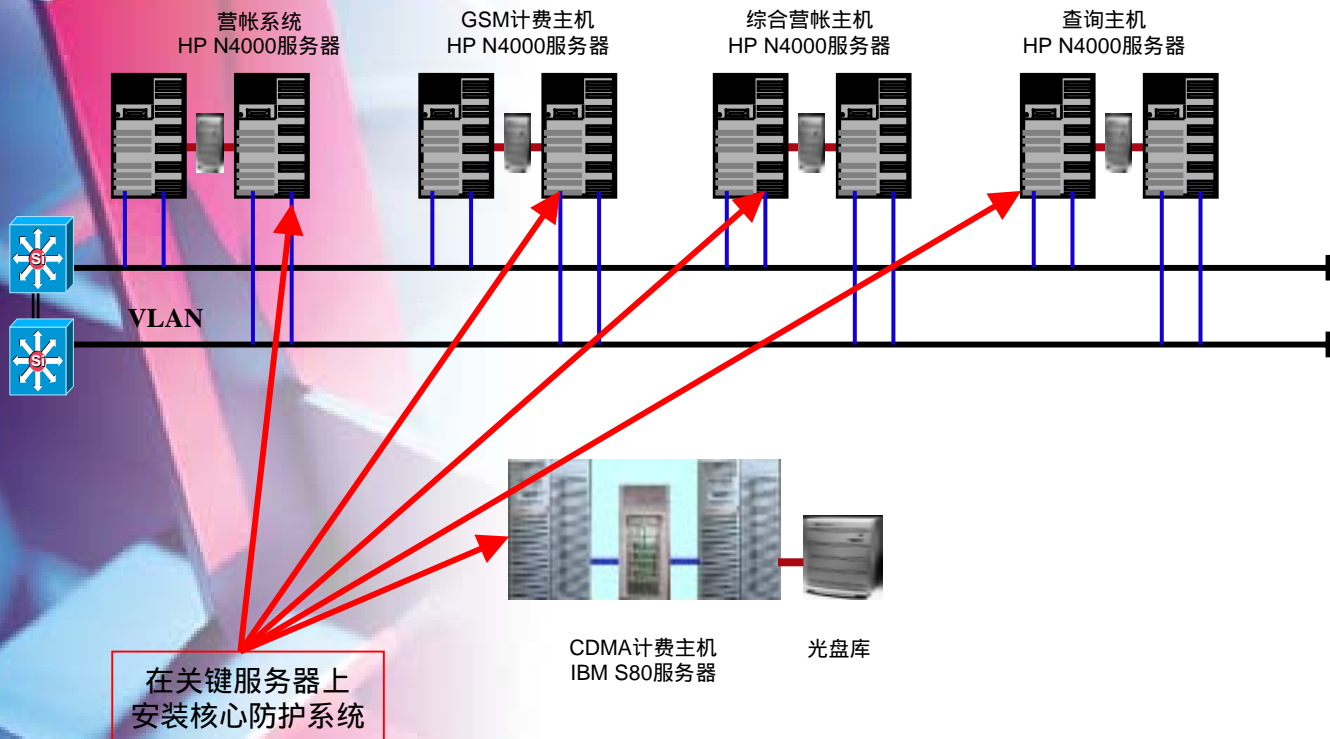
- 提升操作系统的安全等级

- 限制超级用户权限
- 细粒度安全访问控制
- 增强的资源保护
- 防止缓冲区溢出攻击
- 主机防火墙
- 强身份认证
- 完备的审计功能
- 集中分布式管理

# 主机核心防护（eAC）

- 操作系统的安全是用户业务的最直接保护
- 适用环境
  - AIX
  - IRIX
  - HP-UX
  - DEC-UNIX
  - SUN
  - SCO/Unixware
  - NCR MP-RAS
  - Sequent
  - SINIX
  - Linux
  - NT/2000

# 电信业务系统核心防护图示



# 入侵检测系统 (eID)













- 性能高、功能多
- 适用环境
  - NT/2000/98
  - Hub或交换机端口镜像 (SPAN、RAP、Port Mirroring)

# eID: 网络的安全监视系统功能

- 全面的攻击方式库
- URL访问限制
- 字匹配扫描
- 网络活动回放
- 网络病毒检测
- 网络行为追踪审计
- 安全产品的联动
- 网络流量统计功能

# 丰富的攻击库支持

## 可检测的弱点列表

弱点	规则名称	CVE 参考	BugTraq ID
! NT IIS Showcode ASP Vulnerability	 <a href="#">HTTP IIS Intrusions/Scans</a>	<a href="#">GENERIC-MAP-NOMATCH</a>	<a href="#">167</a>
NT IIS SSL DoS Vulnerability	 <a href="#">HTTP IIS Intrusions/Scans</a>	<a href="#">GENERIC-MAP-NOMATCH</a>	<a href="#">521</a>
! NT IIS4 Buffer Overflow Vulnerability	 <a href="#">HTTP Generic Intrusions/Scans</a>	<a href="#">GENERIC-MAP-NOMATCH</a>	<a href="#">307</a>
NT IIS4 DoS - ExAir Sample Site Vulnerability	 <a href="#">HTTP IIS Intrusions/Scans</a>	<a href="#">CVE-1999-0449</a>	<a href="#">193</a>
NT IIS4 Log Avoidance Vulnerability	 <a href="#">HTTP IIS Intrusions/Scans</a>	<a href="#">CVE-1999-0448</a>	<a href="#">191</a>
NT IIS4 Remote Web-Based Administration Vulnerability	 <a href="#">HTTP IIS Intrusions/Scans</a>	<a href="#">GENERIC-MAP-NOMATCH</a>	<a href="#">189</a>
NT IIS4 Shared ASP Cache Vulnerability	 <a href="#">HTTP IIS Intrusions/Scans</a>	<a href="#">CVE-1999-0348</a>	<a href="#">195</a>
! NT IMail Imapd Buffer Overflow DoS Vulnerability	 <a href="#">IMAP Generic Intrusions/Scans</a>	<a href="#">CVE-1999-0412</a>	<a href="#">502</a>
NT IMail IMonitor Buffer Overflow DoS Vulnerability	 <a href="#">IMAP Generic Intrusions/Scans</a>	<a href="#">CVE-1999-0385</a>	<a href="#">504</a>
NT IMail Web Service Buffer Overflow DoS Vulnerability	 <a href="#">IMonitor status.cgi DoS</a>	<a href="#">CVE-1999-0385</a>	<a href="#">505</a>
NT Index Server Directory Traversal Vulnerability	 <a href="#">HTTP - IDS Evasion Techniques</a>	<a href="#">GENERIC-MAP-NOMATCH</a>	<a href="#">950</a>
! NT Services.exe Denial of Service	 <a href="#">RFPoison NT DoS Attack</a>	<a href="#">GENERIC-MAP-NOMATCH</a>	<a href="#">754</a>

### NT Services.exe Denial of Service

一个经特殊处理的包可导致拒绝 NT 4.0 主机服务，致使本地管理和网络通信几乎瘫痪。这种攻击将使可执行的“服务”崩溃，反过来，又将使机器丧失通过“命名管道”进行操作的能力。结果是用户不能远程使用登录、注销、管理注册、创建新文件、共享连接或远程管理。Internet Information Server 等服务也不能按预期的正常进行。重启受影响的机器可恢复这些功能，但前提是不要再受到攻击。问题在于 srvsvc.dll 调用 services.exe 的方式。某个 MSRPC 调用将返回 NULL 值，services.exe 不能正确地解释 NULL 值。这反过来又会导致 services.exe 的崩溃。如果该拒绝访问攻击结合其它一些方式，可能会另它产生对主机的 Debugger (即 Dr Watson) 调用，如果这是一个“特洛伊”调用，可能在目标主机上执行恶意代码。

#### 影响到的系统:

- Microsoft Windows NT 4.0
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP6

# eID: URL访问限制

- 能够指定禁止访问的URL
  - 防止资源滥用
  - 防止访问





# eID: 字匹配扫描

- 防止泄露敏感信息
- 防止访问非法信息
  - 邮件扫描
  - 网站访问

# 内容过滤的应用案例（1）

The screenshot shows the eFrast Intrusion Detection interface. On the left, a tree view displays a directory structure for domains like jv01, jv02, jv03, jv04, jv05, and jv06. The right pane shows a web page with the URL `http://www.sina.com.cn` and a news article titled "少数“法轮功”顽固分子在天安门广场滋事被制止". The article text discusses Falun Gong activities during the 51st anniversary of the PRC. At the bottom, a statistics table shows network activity data.

Client/Bytes	Total	FTP	HTTP (World Wide Web)	Other
Total	4,481,102	55,601	140,790	4,284,711

# 内容过滤的应用案例（2）

The screenshot displays the efrust Intrusion Detection application window. The title bar reads "efrust Intrusion Detection". The menu bar includes "Data", "Edit", "View", "Functions", "Settings", and "Help". The toolbar contains various icons for file operations and system functions. A status bar at the bottom indicates "Tracing active" and "Far Help, press F1".

The main window is divided into several panes:

- Left Pane:** A tree view showing network activity. The root is "HTTP (World Wide Web)", followed by "Other", "FTP Data", and two sub-entries for "jv02.domain1.com" and "jv03.domain2.com". A "Session started" icon is visible under the second sub-entry.
- Top Status Bar:** A message reads: "Switching workspaces at regular periods ensues two databases: one with the current data and one with old data up to the last switching. Select: Data => Open Workspace, to view the secondary workspace."
- Right Pane:** A chat window with a transcript of a speech. The text is in Chinese and appears to be a Q&A session. The speaker discusses the importance of sincerity, the impact of the Cultural Revolution, and the need for collective activities. The transcript includes questions and answers, as well as a closing statement by the speaker.
- Bottom Status Bar:** A log entry reads: "On Sun Nov 12 16:33:15 Server jv03.domain2.com started HTTP (World Wide Web) for the first time". Below this, there are tabs for "Clients", "Servers", "Users", "Recent activity", and "Other services". A "New network activity" notification is also present.

# 内容过滤的应用案例（3）

The screenshot displays the eTrust Intrusion Detection interface. At the top, a banner asks, "Do you find all those DNS addresses confusing? How about giving them nicknames?". The main window shows an email log entry for "SMTP (Outgoing Email)" with the following details:

- Date: Mon, 13 Nov 2000 00:14:42 +0800
- Subject: falangong
- From: administrator <administrator@jv03.DOMAIN2.com>
- To: 'Administrator' <Administrator@jv01.DOMAIN1.com>

The email body contains the following text:

正当全国人民欢庆国庆五十一周年，庆祝我体育健儿在奥运会取得优异成绩为国争光之际，10月1日上午，少数“法轮功”邪教组织顽固分子受在境外的李洪志等人的煽动，到北京天安门广场进行非法聚集活动，企图扰乱天安门广场的秩序，破坏人民群众在天安门广场参观游览的喜庆气氛。在场群众对这些“法轮功”顽固分子的行为十分反感和气愤。为了维护正常的社会秩序，确保人民群众度过一个欢乐祥和的节日，在场执勤民警迅速将做事的“法轮功”顽固分子带离现场。天安门广场秩序井然，人民群众欢庆国庆的活动正常进行。（完）

Below the email content, a log of network activity is visible:

```
On Mon Nov 13 00:02:23 Server jv03.domain2.com started SMTP (Outgoing Email) for the first time
On Mon Nov 13 00:02:23 Client jv01.domain1.com started SMTP (Outgoing Email) for the first time
On Mon Nov 13 00:01:44 Server jv01.domain1.com started SMTP (Outgoing Email) for the first time
On Mon Nov 13 00:01:44 Client jv03.domain2.com started SMTP (Outgoing Email) for the first time
On Sun Nov 12 23:54:01 Server jv01.domain1.com started SMTP (Outgoing Email) for the first time
On Sun Nov 12 23:54:01 Client jv03.domain2.com started SMTP (Outgoing Email) for the first time
On Sun Nov 12 23:52:13 Server jv03.domain2.com started SMTP (Outgoing Email) for the first time
On Sun Nov 12 23:52:13 Client jv01.domain1.com started SMTP (Outgoing Email) for the first time
```

The bottom of the window shows a taskbar with various applications open, including "开始", "hi - 画图", "资源管...", "eTrust...", "命令提...", "域名服...", "我的电脑", "http\_r...", "aaa - ...", and the system clock showing "0:23".



# eID: 网络行为追踪审计

- 全面的行为审计模式
  - 帮助管理员跟踪最终用户或应用程序对网络的使用
  - 帮助管理员对网络进行规划
  - 帮助管理员改善网络安全状况

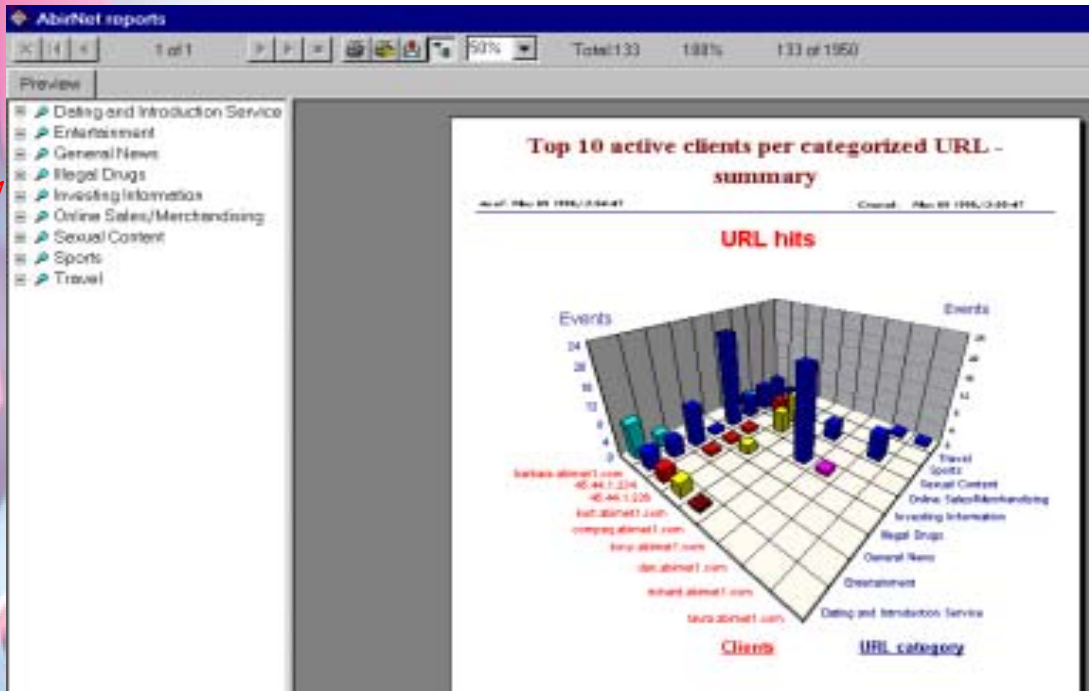
# FTP

The screenshot displays the eTrust Intrusion Detection interface. The main window shows a tree view of logs, with the 'FTP (File Transfer) Log' selected. The log content includes several entries for 'chencs14.ca.com' involving file transfers and directory listings. Below the log, there are links to 'HTTP - IDS Evasion Techniques', 'HTTP Generic Intrusions/Scans', 'http://sportz.sina.com.cn', and 'www(http) Log'. A statistics table is visible at the bottom, showing data for '用户' (User) and '总计' (Total) across various protocols.

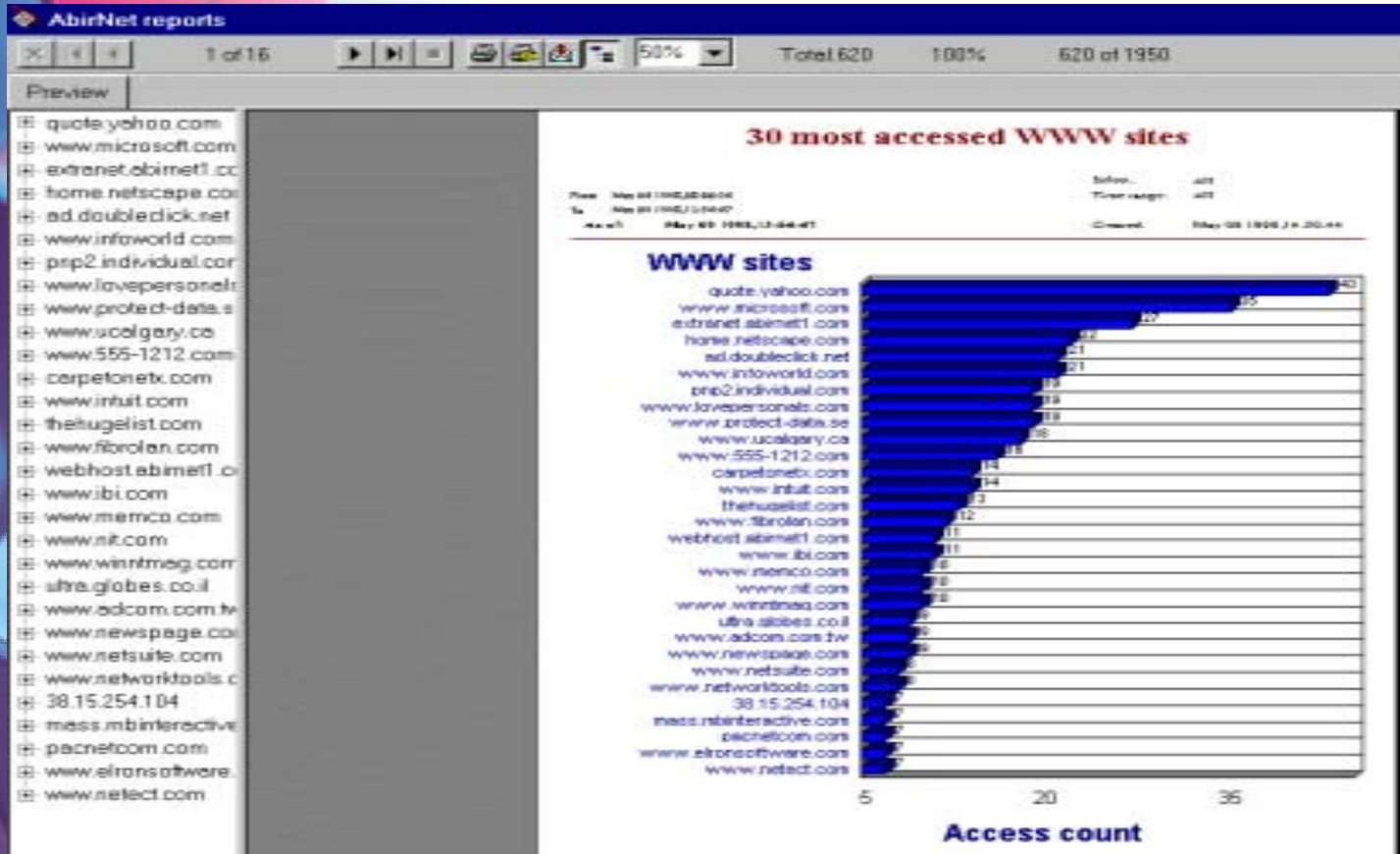
用户/总计	总计	POP (Incoming Email)	FTP	HTTP (World Wide Web)	Other
总计	4,555,529	0	0	2,315,370	2,240,159
客户	0	0	0	0	0
服务器	0	0	0	0	0
用户	0	0	0	0	0
其它服务	0	0	0	0	0

# eID - 报表形式样本1


目录



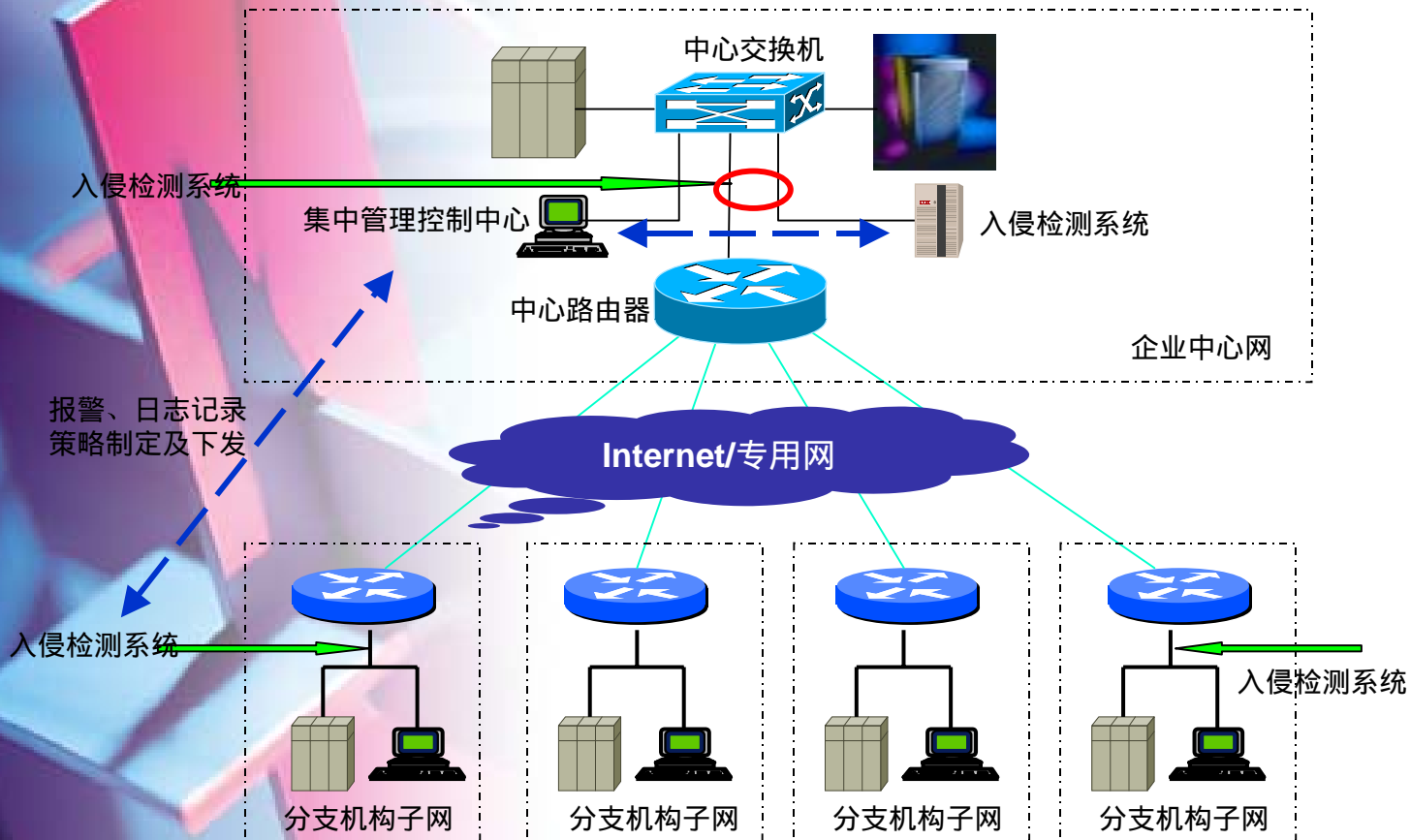
# eID - 报表形式样本2



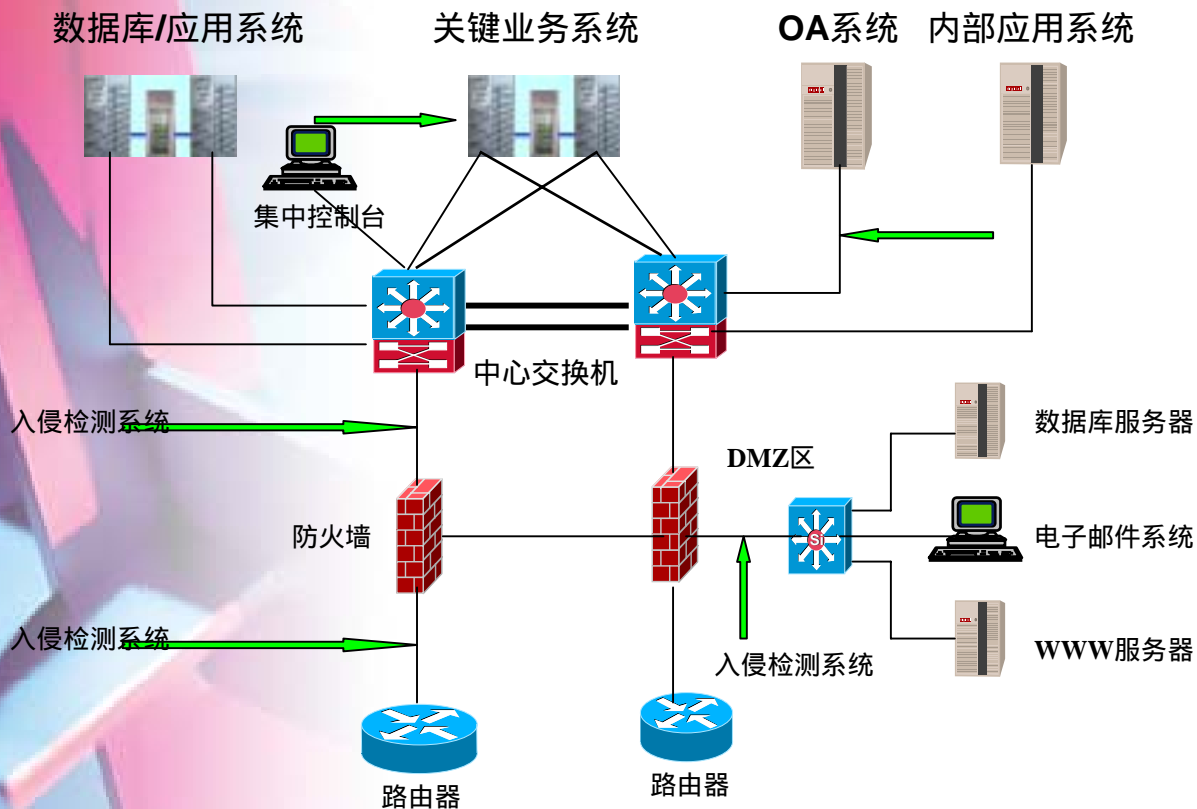
# 入侵检测系统解决方案

The background features a complex 3D geometric design. It consists of several translucent, semi-transparent planes in shades of light blue and red. These planes are arranged in a way that creates a sense of depth and perspective. Interspersed among these planes are thin, white, curved lines that resemble orbits or paths in space. The overall aesthetic is clean, modern, and technical, typical of a corporate or scientific presentation.

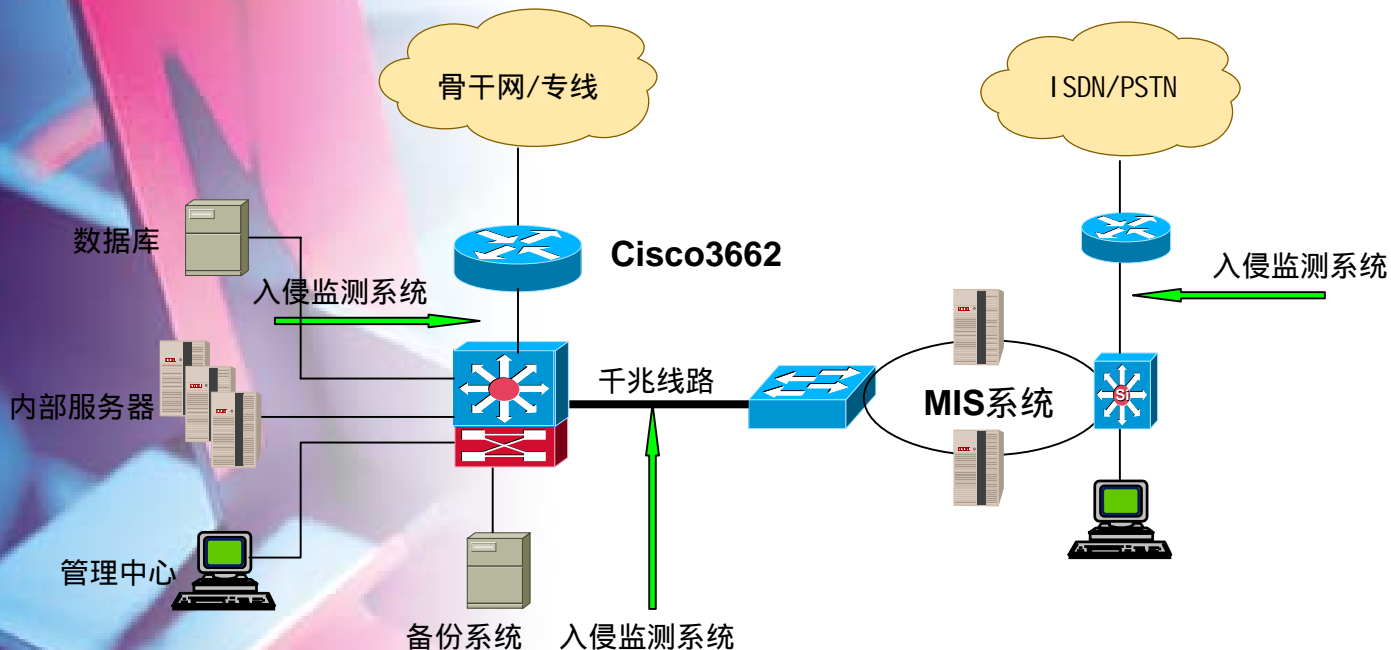
# 入侵检测系统的网络拓扑设计



# 入侵检测系统的网络拓扑设计



# 入侵检测系统的网络拓扑设计



# 金辰防火墙产品系列

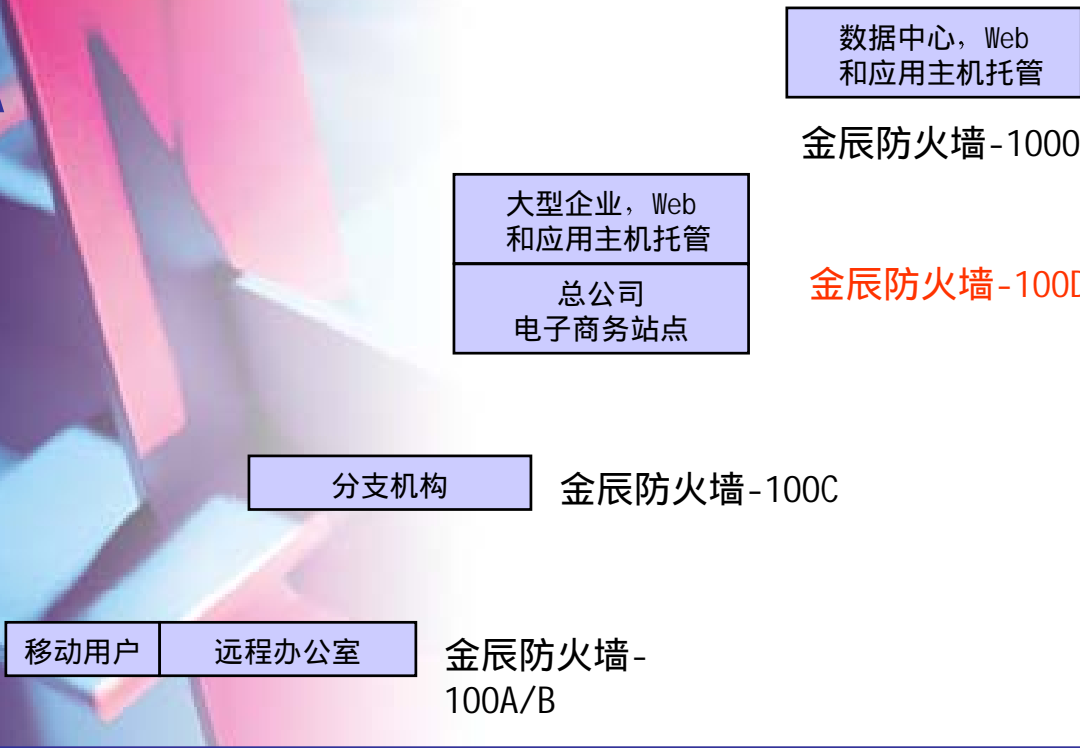
分成两个产品系列:

- SecuE-100-A、B、C、D
- SecuE-1000



# SecuE系列防火墙

性能



多站点企业和服务提供商

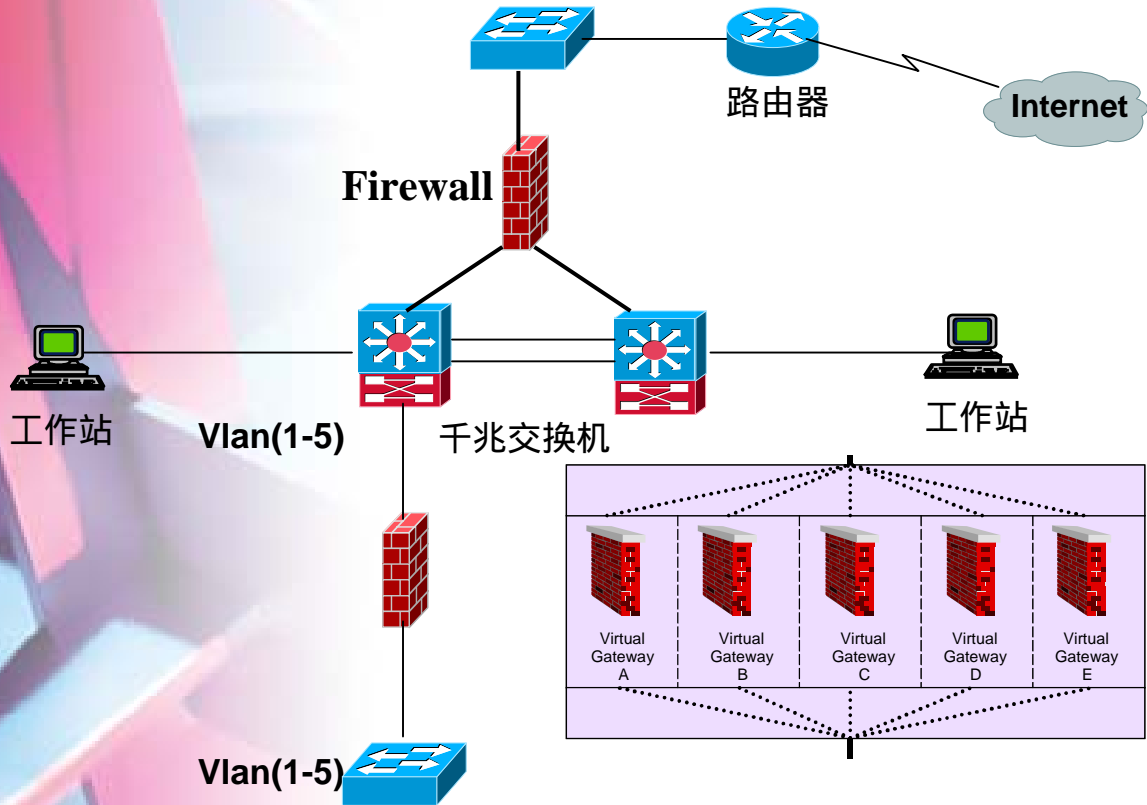
特性

(用户, 会话, 通道等.)

# SecuE系列防火墙的主要功能

- 多种操作模式
- 基于状态检测的分组过滤
- 基于时间的访问控制
- 虚拟防火墙功能
- VPN功能
- 认证功能
- 基于流量及规则的带宽管理
- 提供入侵检测功能
- URL过滤功能
- 提供WEB缓存功能
- Virus防护功能
- 双机热备功能
- 支持SSL、SSH安全管理
- 支持SNMP
- 简单方便的配置备份与恢复

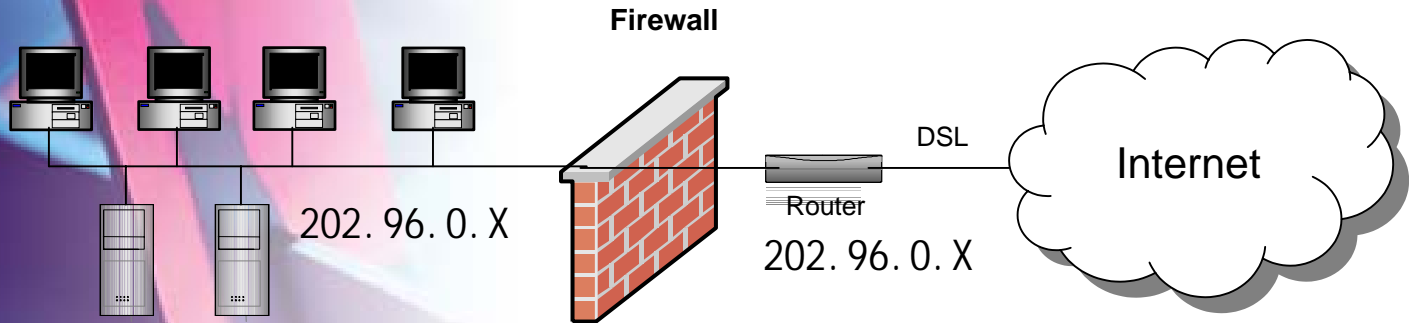
# 千兆防火墙虚拟网关概念



# 防火墙解决方案

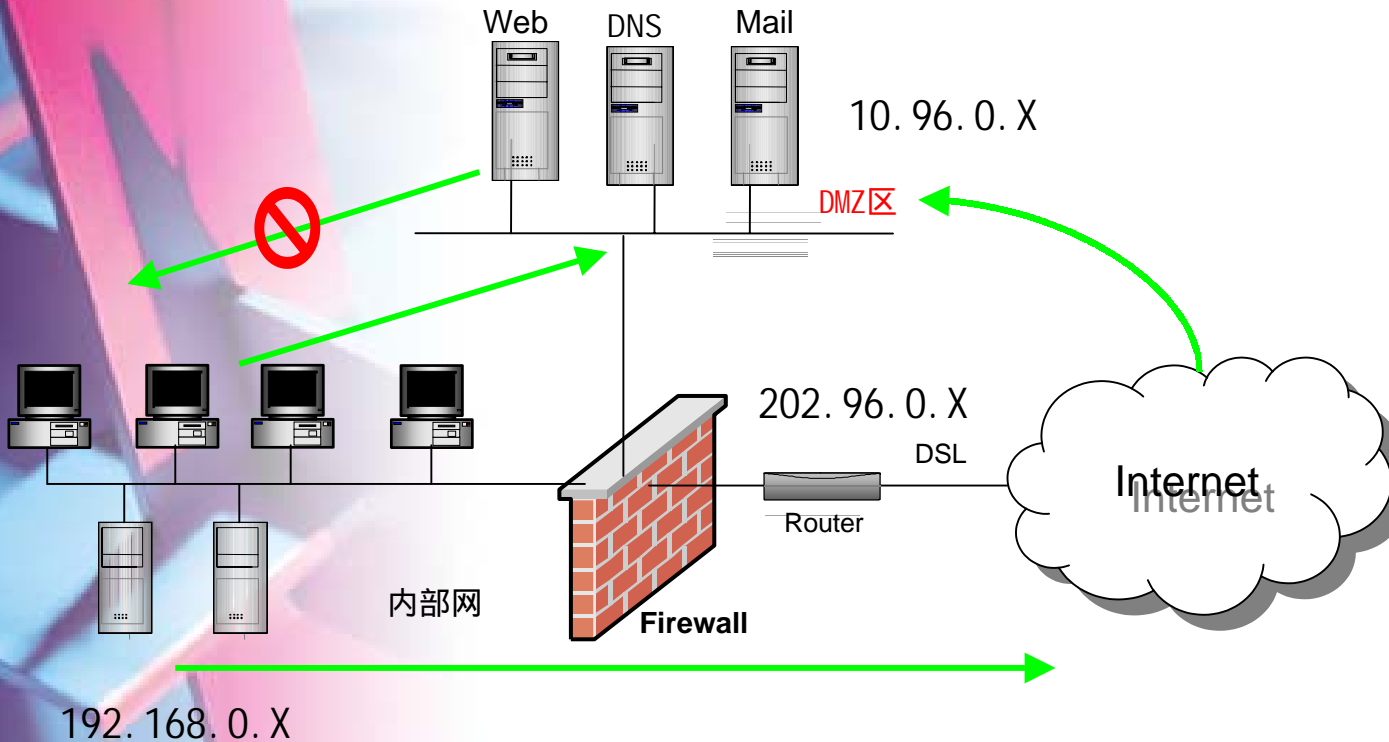
The background features a complex 3D geometric design. It consists of several translucent, semi-transparent planes in shades of light blue and reddish-pink. These planes are arranged in a way that creates a sense of depth and perspective, with some appearing to be stacked or overlapping. Interspersed among these planes are thin, glowing white lines that curve and loop through the space, adding a dynamic and futuristic feel to the overall composition. The lighting is soft and diffused, highlighting the edges and surfaces of the geometric shapes.

# 透明模式应用

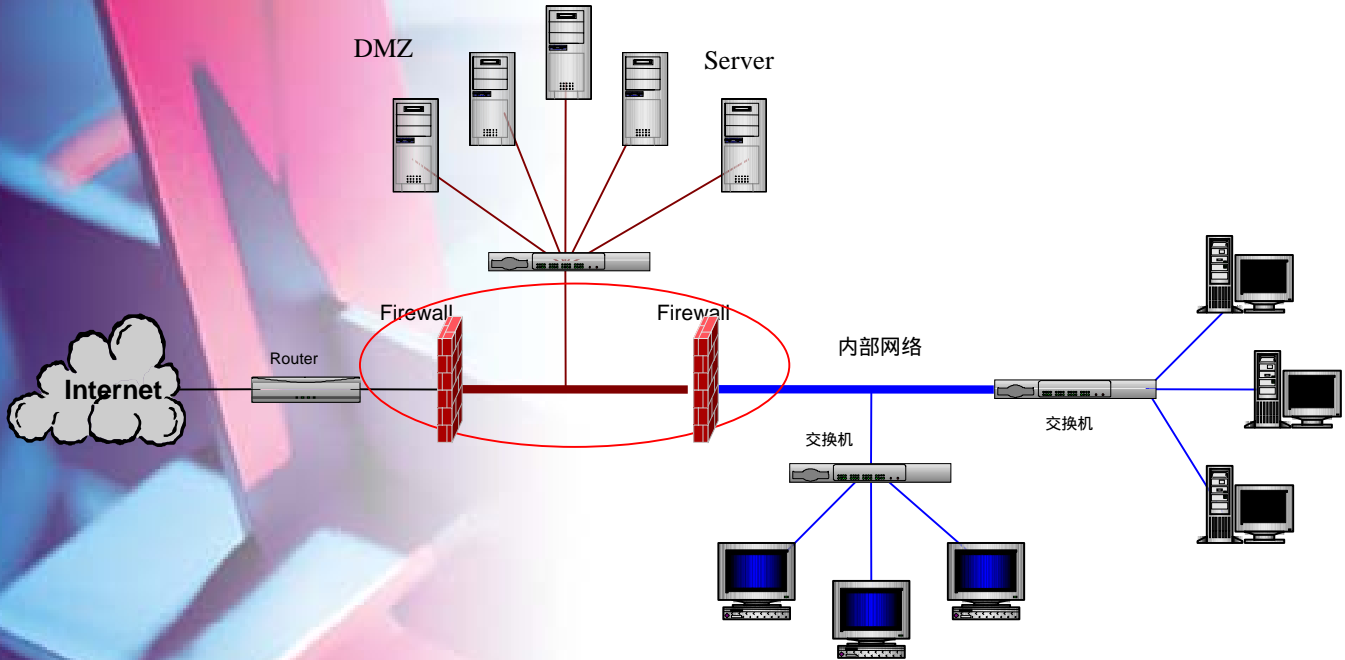


一般在安装防火墙时，需要考虑如何改动原有的网络拓扑结构或修改连接防火墙的路由表，增加了工作的复杂程度和难度  
透明模式解决此问题

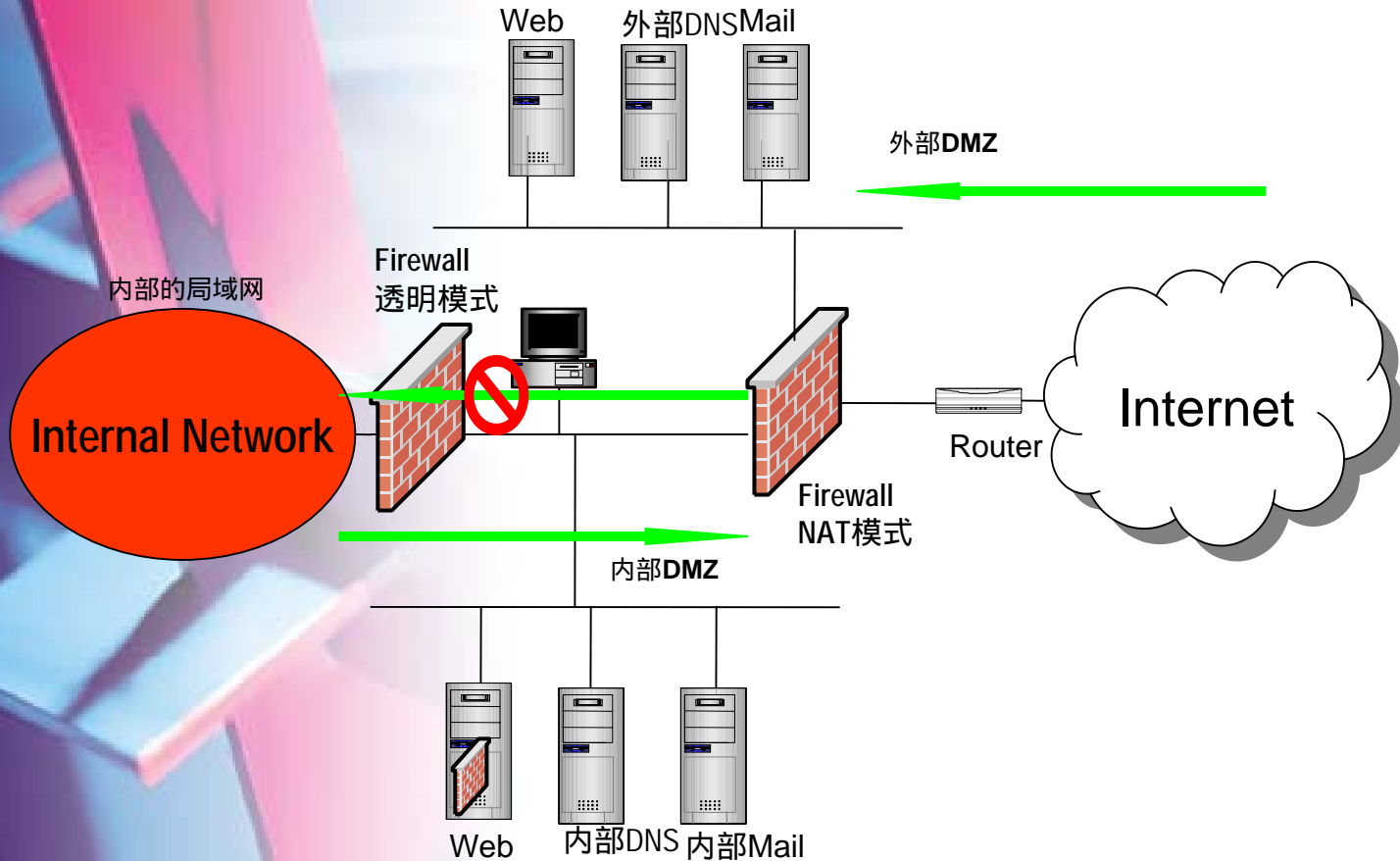
# NAT地址转换方式



# 防火墙DMZ设计



# 多层次防护设计



# 企业级的防火墙设计

总部局域网

Firewall  
透明模式



Manufacturing



Marketing



Accounting



外DMZ区

- E-Mail+IDS
- File Transfer
- Web Server
- 拨号服务器
- 外部DNS



Router

Firewall  
NAT模式



内DMZ区

- E-Mail+IDS
- 内部DNS服务器
- Web Server



Internet



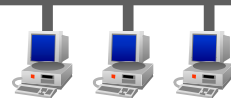
移动用户

Extranets

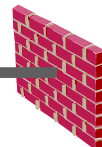
VPN



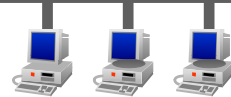
Business Partners



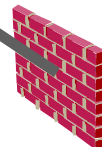
VPN



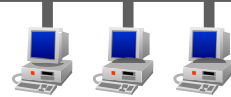
分公司



VPN



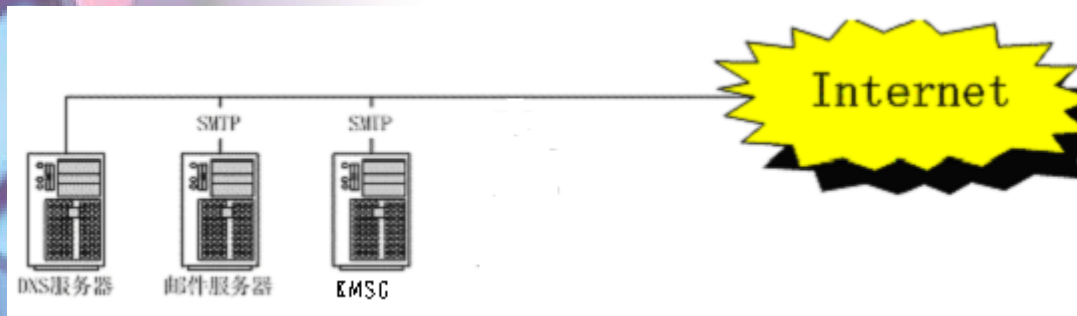
供应商



# KILL 邮件过滤网关

KILL MailShield Gateway

- 对进出系统的电子邮件进行过滤
- 与具体的邮件系统类型无关
- 使用独立加固的硬件平台



# KILL 邮件过滤网关

- 高性能
- 物理旁路接入，不影响系统可靠性
- 特征码自动升级
- 支持SMTP认证、POP认证和Windows认证
- 支持多域系统
- 容错、均衡与集群
- 未来更会
  - 病毒过滤
  - 图片过滤
  - 倾向性言论过滤
  - 垃圾邮件过滤

# KILL 安全胃甲

- 适应计算机病毒的网络化趋势
  - 传播网络化、攻击网络化
  - 满足广域网络环境的计算机病毒防范要求
- 适用平台:
  - 服务器
    - KILL for Windows NT/2000 Server
    - KILL for NetWare
    - KILL for Unix
    - KILL for Linux
  - 群件系统
    - KILL for Lotus Notes
    - KILL for MS Exchange
  - 客户端
    - Win95/98/Me、
    - Windows NT Workstation/ 2000 Professional、
    - Win3.X、DOS

# KILL 安全胃甲

- 企业网络杀毒工具

- 集中控管
- 策略和病毒特征码的层次化分发
- 客户端策略强制锁定
- 病毒自动隔离
- 远程自动无停机安装
- 双引擎病毒扫描
- 病毒特征码签名保护
- 自动增量升级
- 多平台支持

# 如何构建成有效的防毒环境

全方位防毒体系

防护

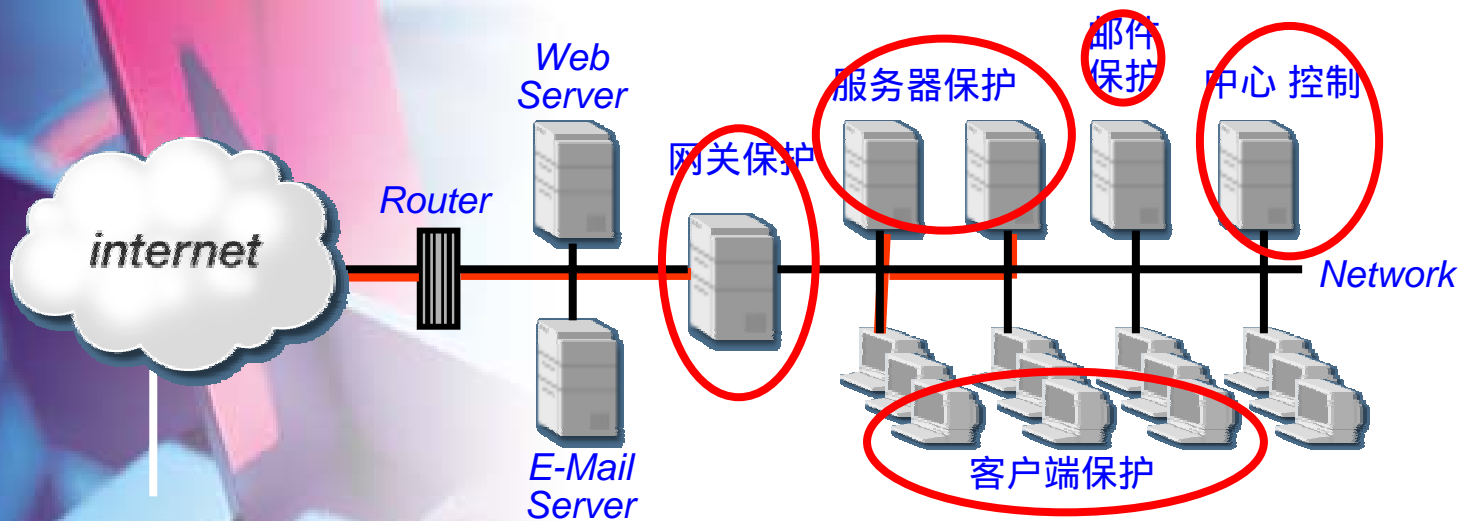
集中方便控管中心

管理

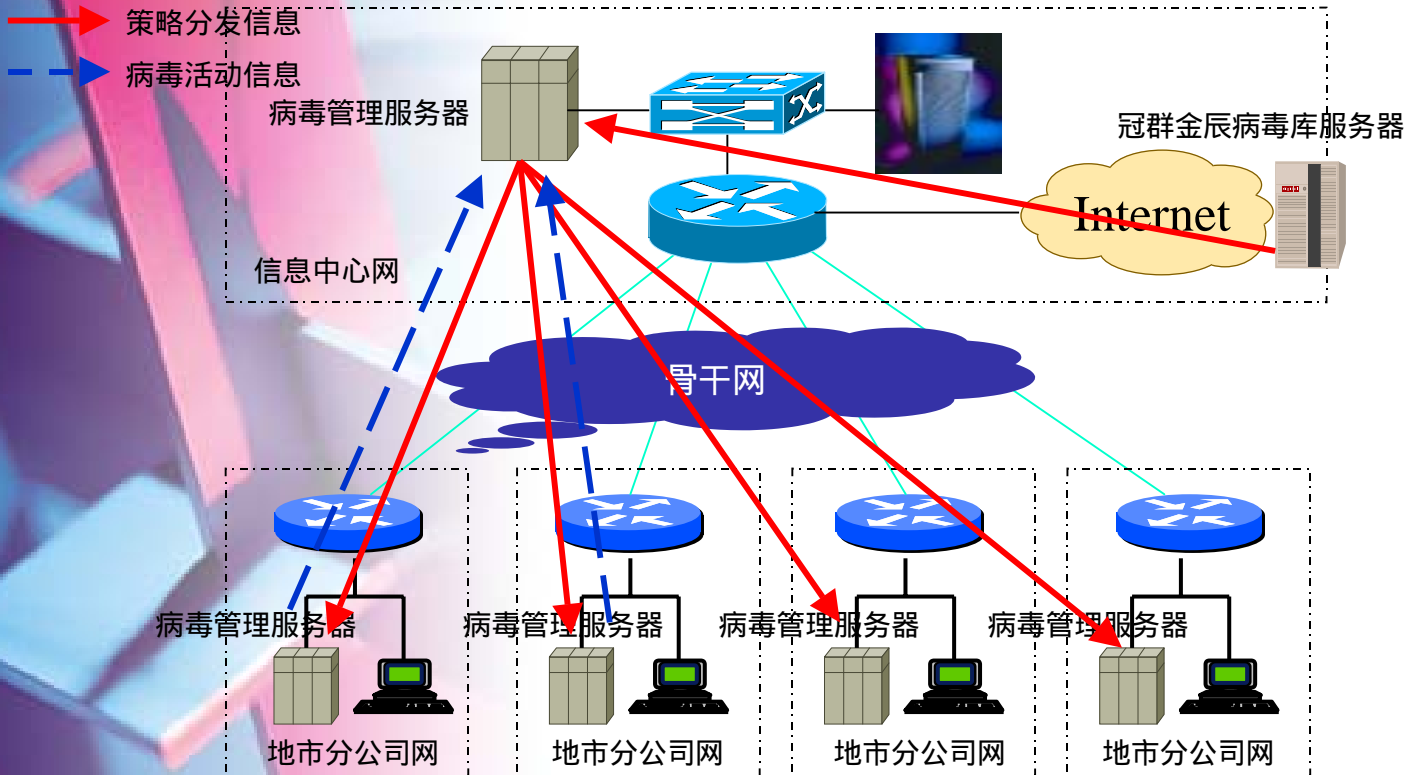
7X24小时技术支持

服务

# 冠群金辰病毒防护系统

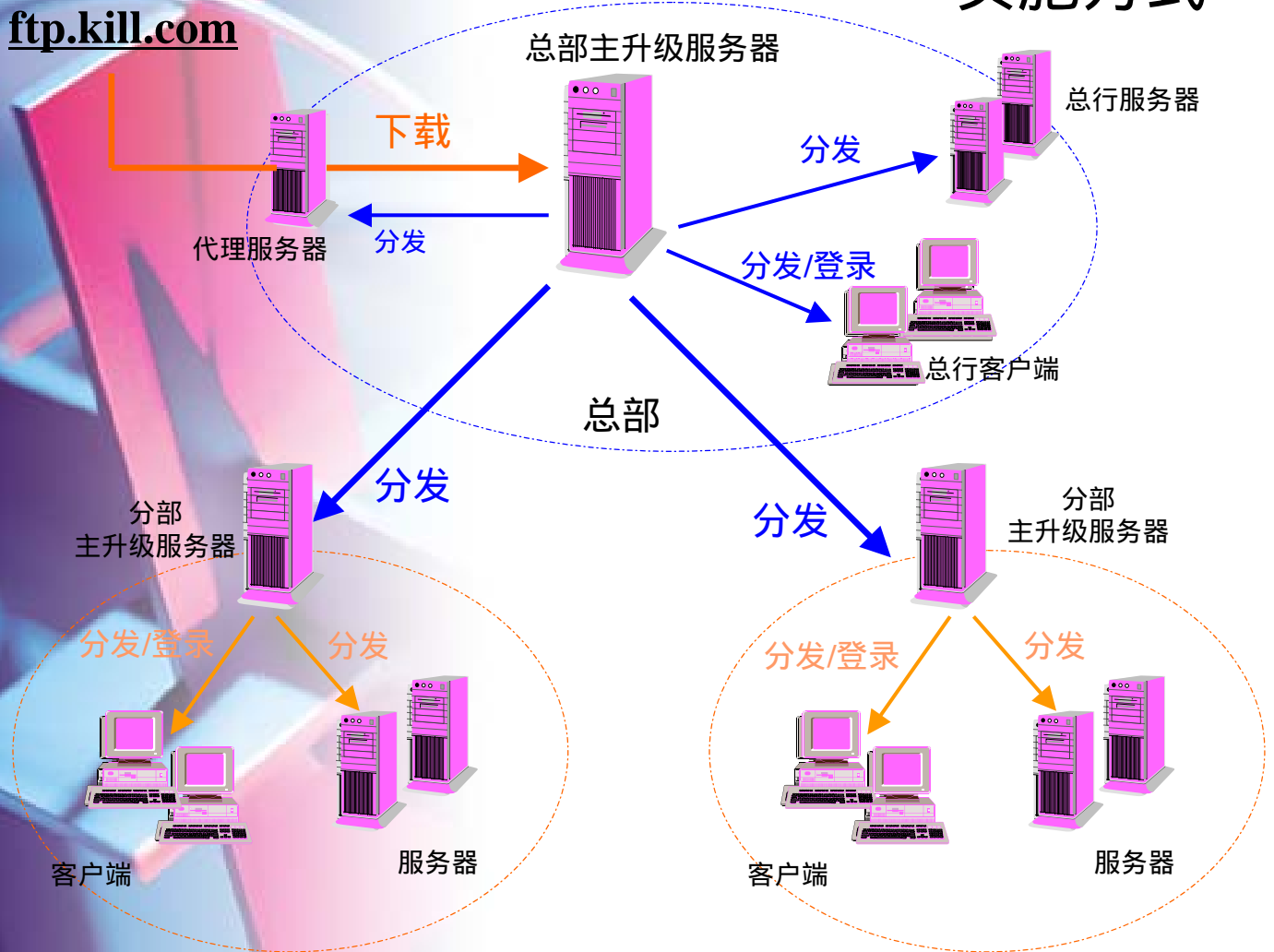


# 病毒防护体系设计



# 实施方式

[ftp.kill.com](http://ftp.kill.com)



# 冠群金辰的优质服务

## 三网一中心

- 全球病毒监测网

金辰公司国内病毒监测网和CA公司国际病毒监测网构成(43个国家170多间办事处)

- 主动服务网
- 全国授权服务网
- 本地研发中心

# 技术支持的内容

- 委派专人负责项目支持

- 技术支持与服务内容

- √ 免费800电话支持
- √ 主动邮件服务
- √ 现场技术支持，24小时到达
- √ 更新升级服务
- √ E-mail技术支持
- √ 免费技术培训

- 全国50家授权技术支持与服务中心

- 灾难数据恢复中心

# 金辰漏洞扫描器

## • 网络系统安全漏洞扫描工具

- 扫描多种目标对象，包括：

- 操作系统(Windows系列, Linux系列)
- 网络设备(Router等)
- 应用程序(Web, DBMS)
- 安全产品(Firewall, VPN 等)

- 并发扫描

- 同时可以并发扫描100台主机系统，从而提高扫描效率
- 可以设置多种网络服务相关扫描选项(WWW, SMTP, FTP 等)

- 多种报表形式

- 漏洞库自动升级功能

# 企业虚拟专用网（eTrust VPN）

- 满足中小企业用户需求，软件实现
- 支持平台：
  - Windows 95/98/NT4.0
  - Solaris 2.6+
  - AIX 4.3.3+
  - HP-UX 11+

# 企业虚拟专用网（eTrust VPN）

- 工作模式:

- 点到点
- 点到网络
- 网络到网络

- 特点:

- 3DES/DES
- 多种认证方式，包括：NT Domain、Novell NDS、SecureID2/3、RADIUS、DCE/ Kerberos、X.509v3

An abstract 3D composition of geometric shapes. A large, semi-transparent blue question mark is centered in the foreground. Behind it, there are several rectangular blocks in shades of red, pink, and light blue, some standing upright and others lying flat. The background is a soft, out-of-focus gradient of light blue and purple, with faint, glowing circular lines that suggest a sphere or a complex geometric structure. The overall aesthetic is clean, modern, and mysterious.

?