

第4章 安全防御体系

管理

架构

技术

产品



1.安全的网络架构：安全域划分

Ubiquitous Interconnectivity = Widespread Vulnerability

安全域划分和边界保护的意义就在于阻止这种无限互联，即使在内网，这种“无限互联”使得漏洞、蠕虫、病毒、内部滥用和误用等威胁防不胜防。

隔离使得风险可控。

等级划分　边界防护

节选自美国总统IT顾问委员会PITAC（President’s Information Technology Advisory Committee）报告 2005



安全域划分的原则

- 同一域内的安全属性相似，便于部署安全策略
- 数量不宜太多
- 划分原则和方法直观易部署
- 照顾现有网络架构和应用布局
- 对端的可信度是重要的参考依据
- ...

收益

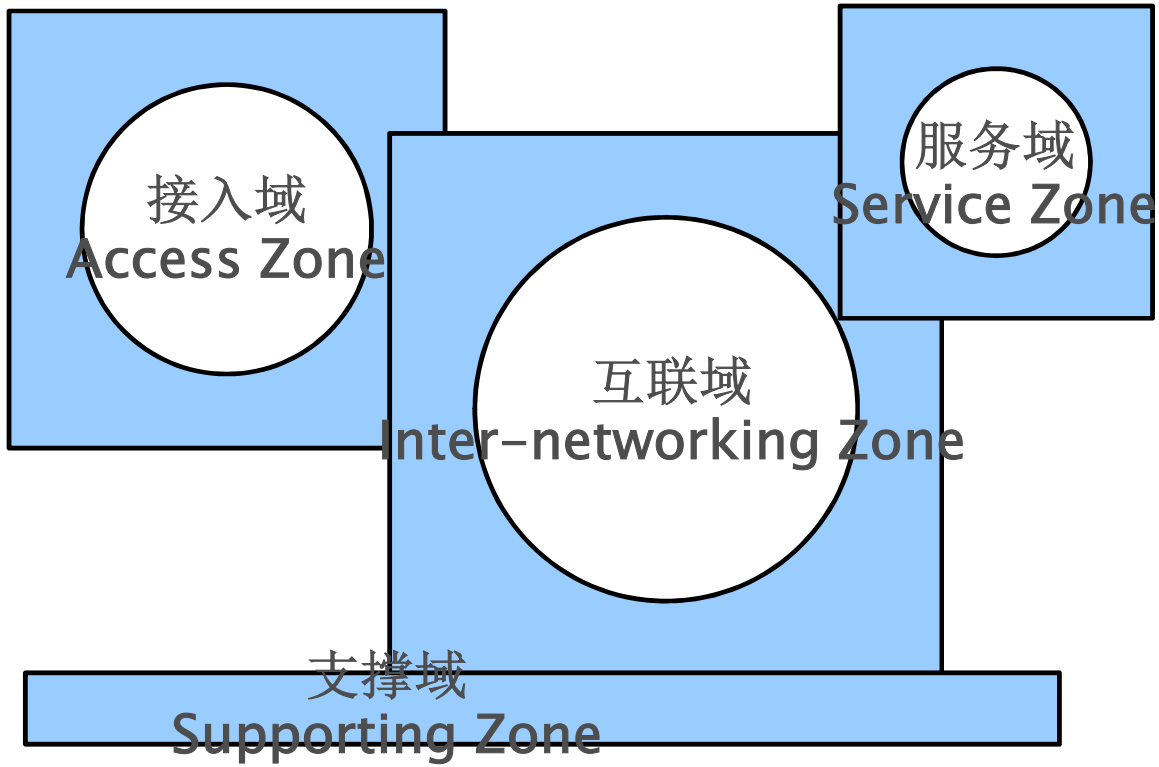
- 隔离安全风险
- 保持安全策略一致
- 便于部署安全设备
- 共享，降低安全成本



安全域示例 - 3+1

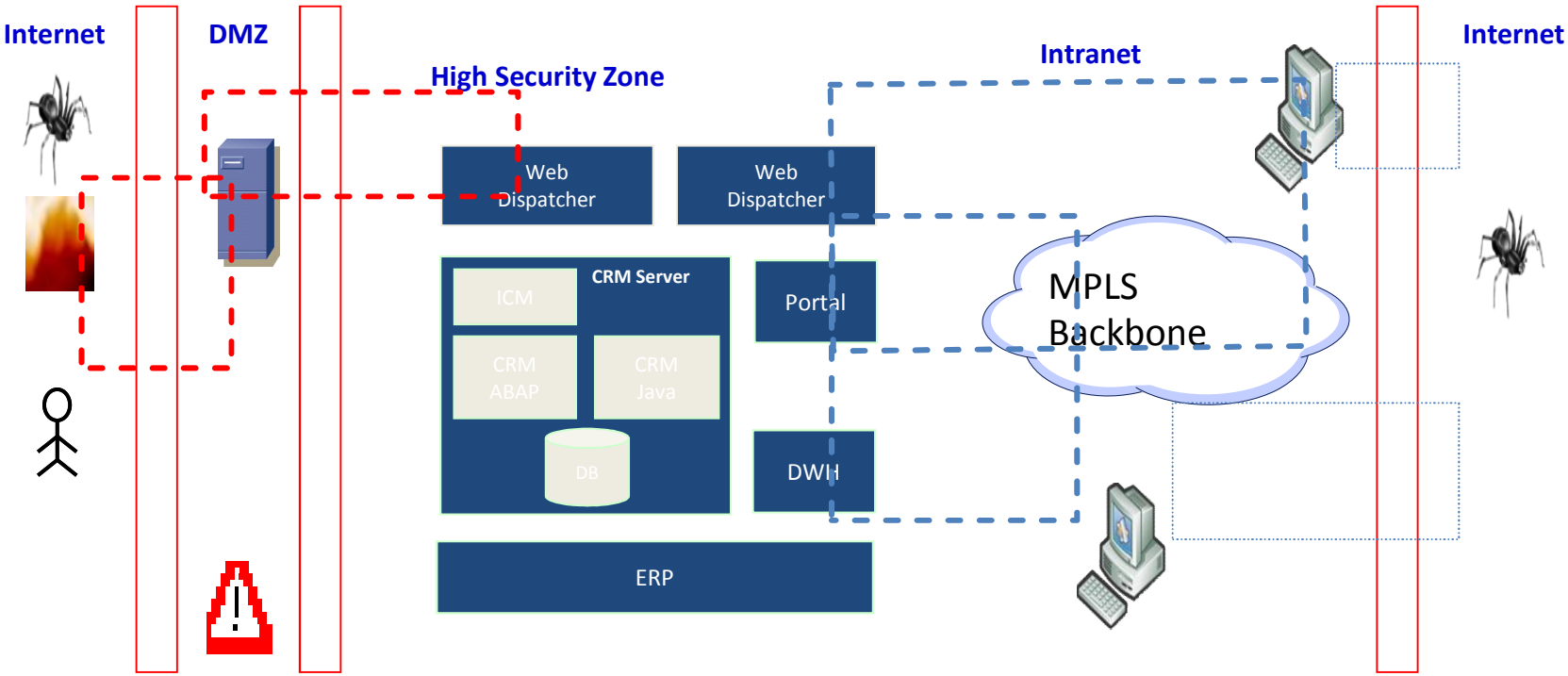
•网络和系统可以分解成4个域
•Networks and systems have 4 kinds of Zones

原则
1. 威胁的方向
2. 受到攻击后影响面的大小





安全域示例 - 数据中心安全域



按照关键度和风险分为不同的安全域

互联网 - 以及合作伙伴

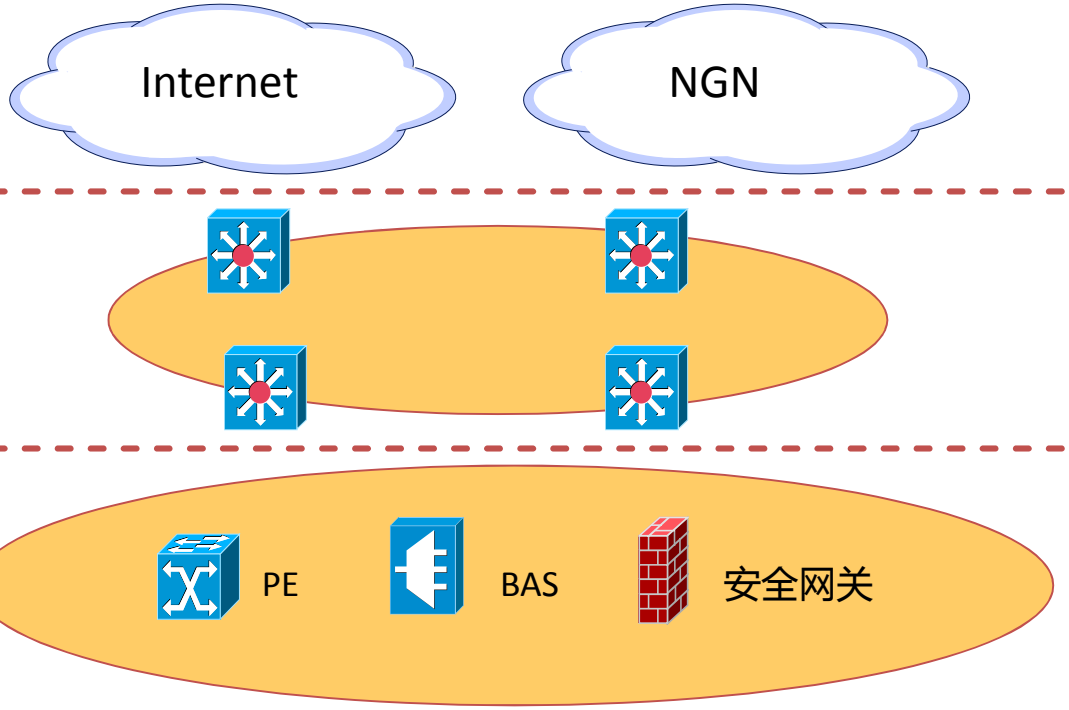
DMZ - 互联网服务

内网 - 用户、普通服务器

高安全区 - 核心区、企业关键服务器

城域网安全域的划分示例



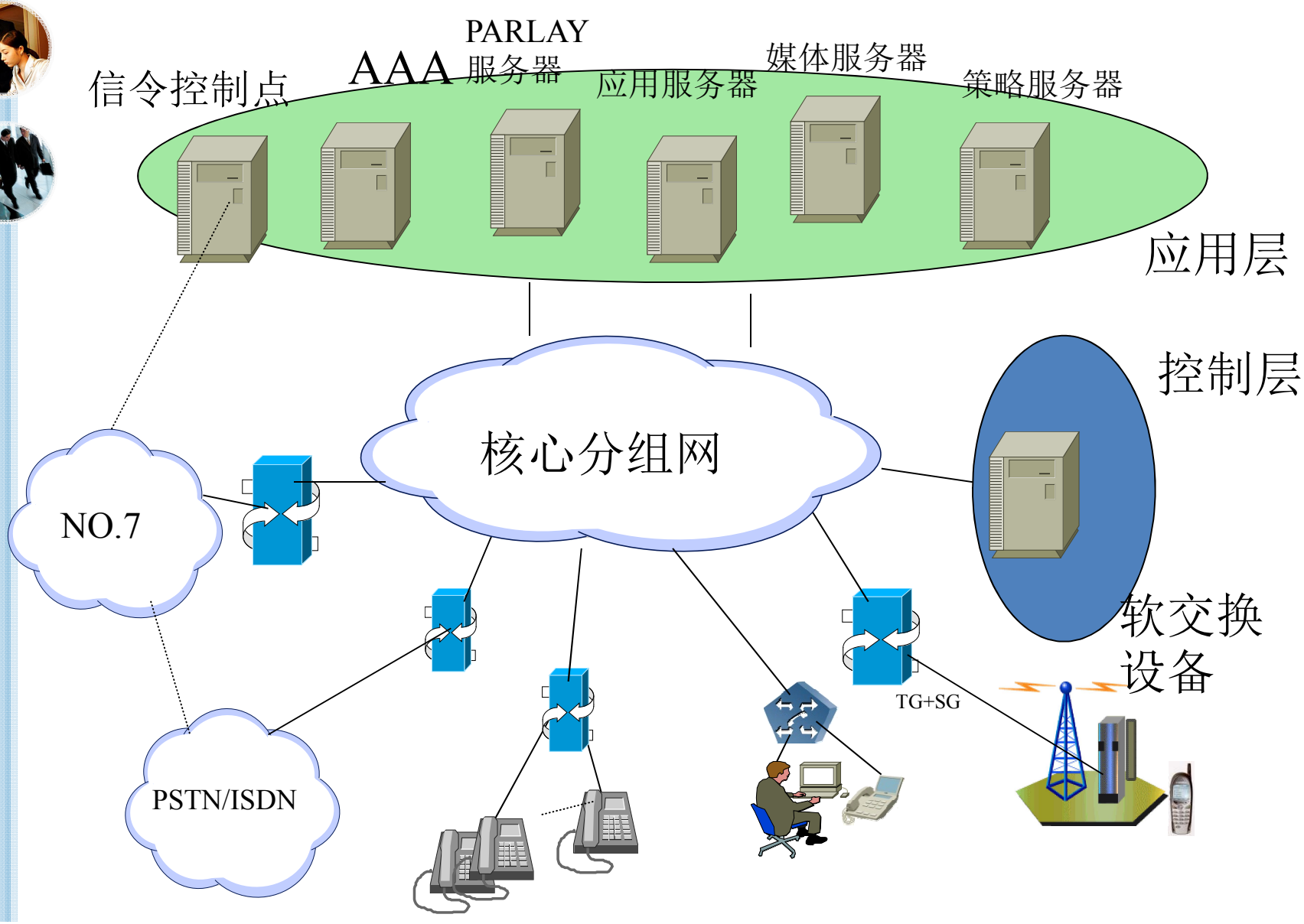


城域网核心层
不同业务分平面承载

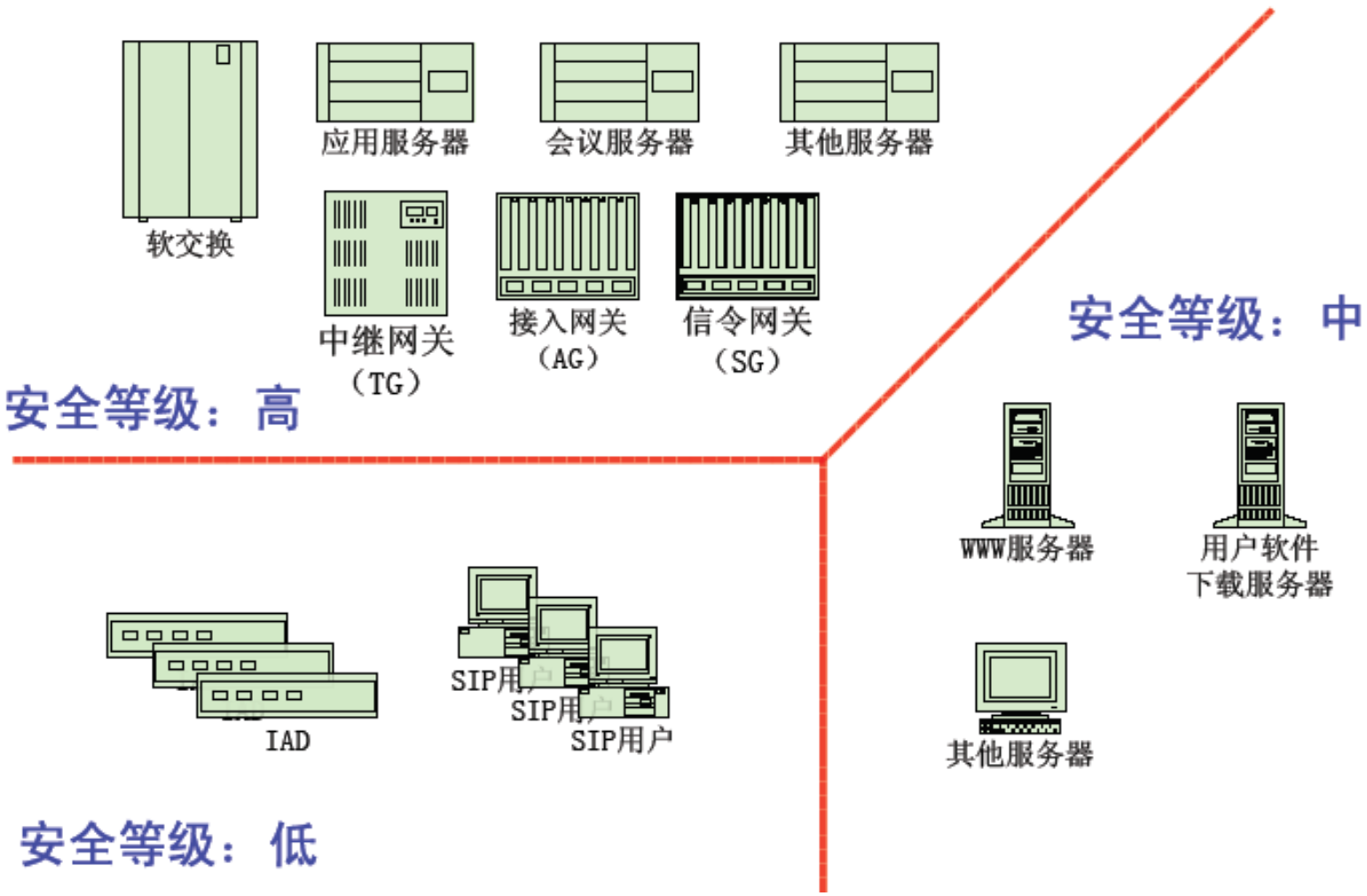
城域网汇聚层
用户认证**uRPF**

城域网接入层
提供多种接入方式
通过VLAN标识用户
支持802.1p

例:NGN与软交换应用方案



软交换网络安全域划分（示例）



网络和业务的发展vs安全的挑战

- 网络结构
  - 虚拟化（设备、拓扑、网络功能）
  - 软件定义，动态按需部署
- 挑战
  - 安全域的边界：模糊、跨边界交互增加
- 对策
  - 软件定义？对网络、计算、存储资源的感知

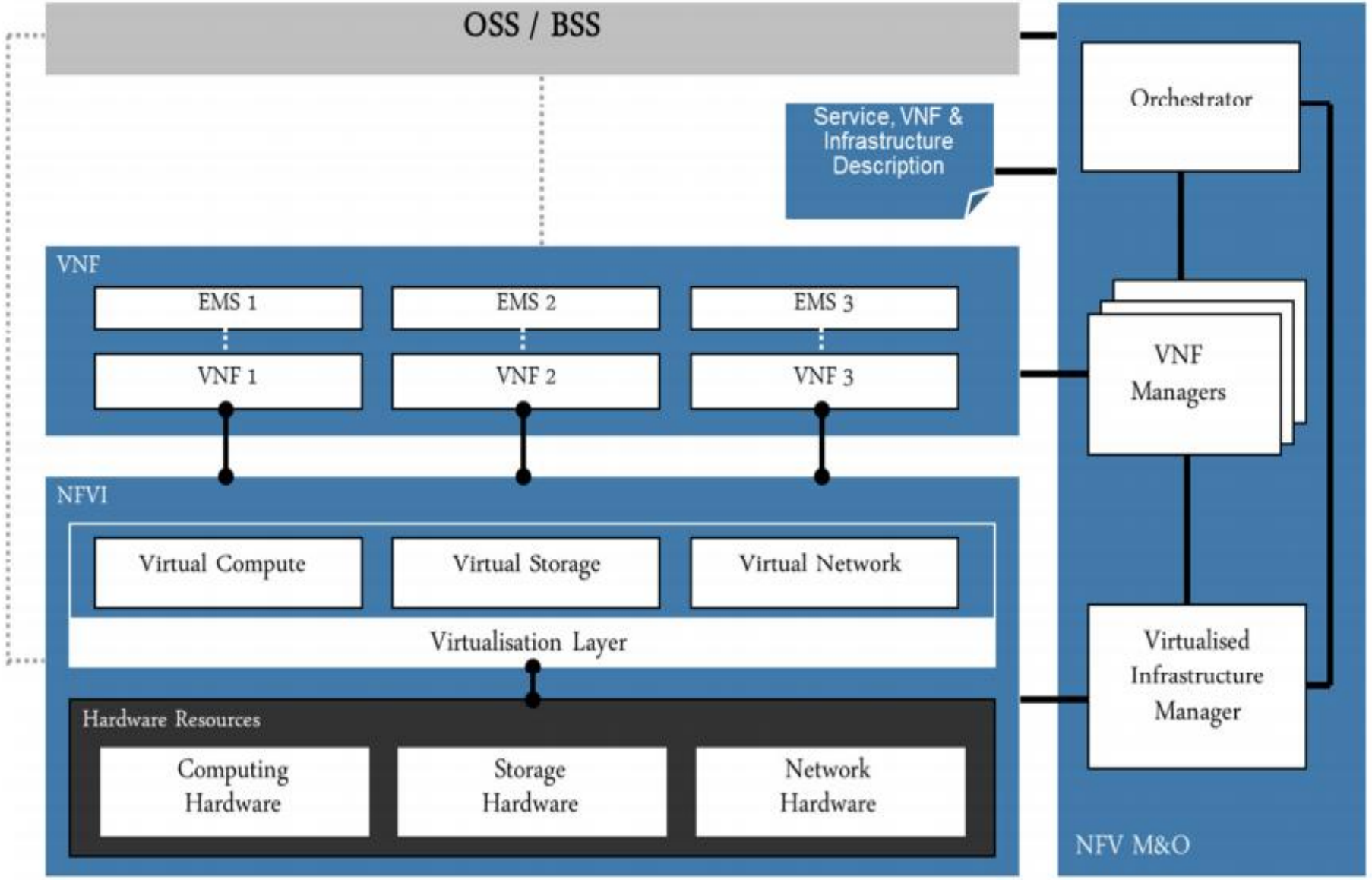


Figure 4: NFV Architectural Framework



安全防御体系

产器：服务， 设备

防恶意代码
防火墙,入侵检测
密罐
信息加密
身份管理
访问控制
日志和审计
内容安全

物理安全
风险评估
补丁管理
应急响应
容灾备份
…



2.防火墙

•防火墙是在两个网络(通常是用户内部网络和Internet)之间实施访问控制策略的一个或一组系统（硬件、软件的组合）,所有进入和离开的数据都必须经过防火墙的检查，只有符合访问控制策略的流才允许通过。

•通过它可以隔离风险区域（Internet或有一定风险的网络）与安全区域（局域网）的连接，同时不会妨碍安全区域对风险区域的访问。

★分离器：

可以隔离风险区域，同时不妨碍对风险区域的访问；

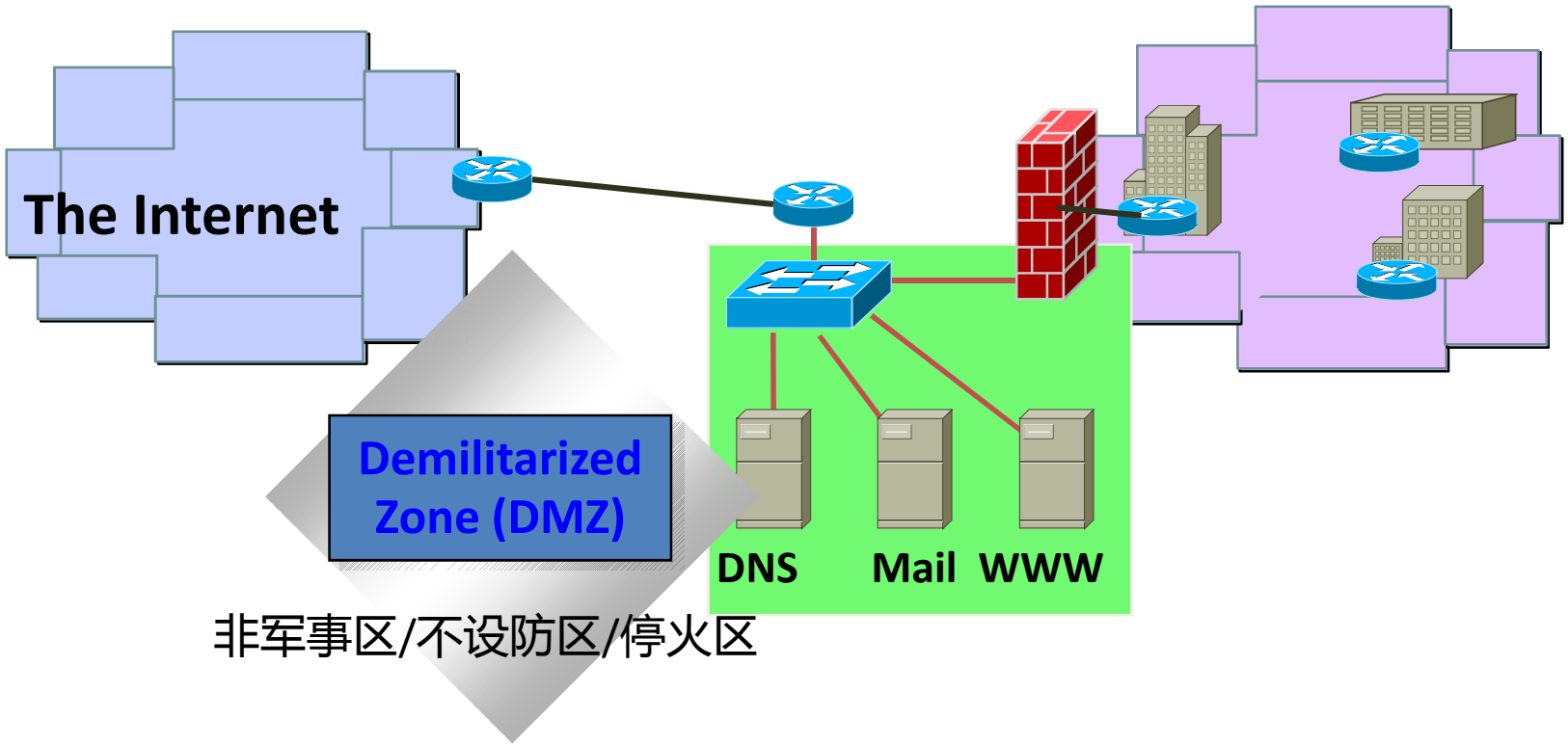
★限制器：可以作为不同网络或网络安全域之间信息的出入口并根据企业的安全策略控制出入网络的信息流；

★分析器：

它可以监控进出网络的信息流，仅让安全、核准了的信息进入，抵制对企业构成威胁的数据，从而完成看似不可能的任务。



设置防火墙



- 前端路由器使用ACL进行第一步安全防护
- 内部使用交换机进行网段隔离



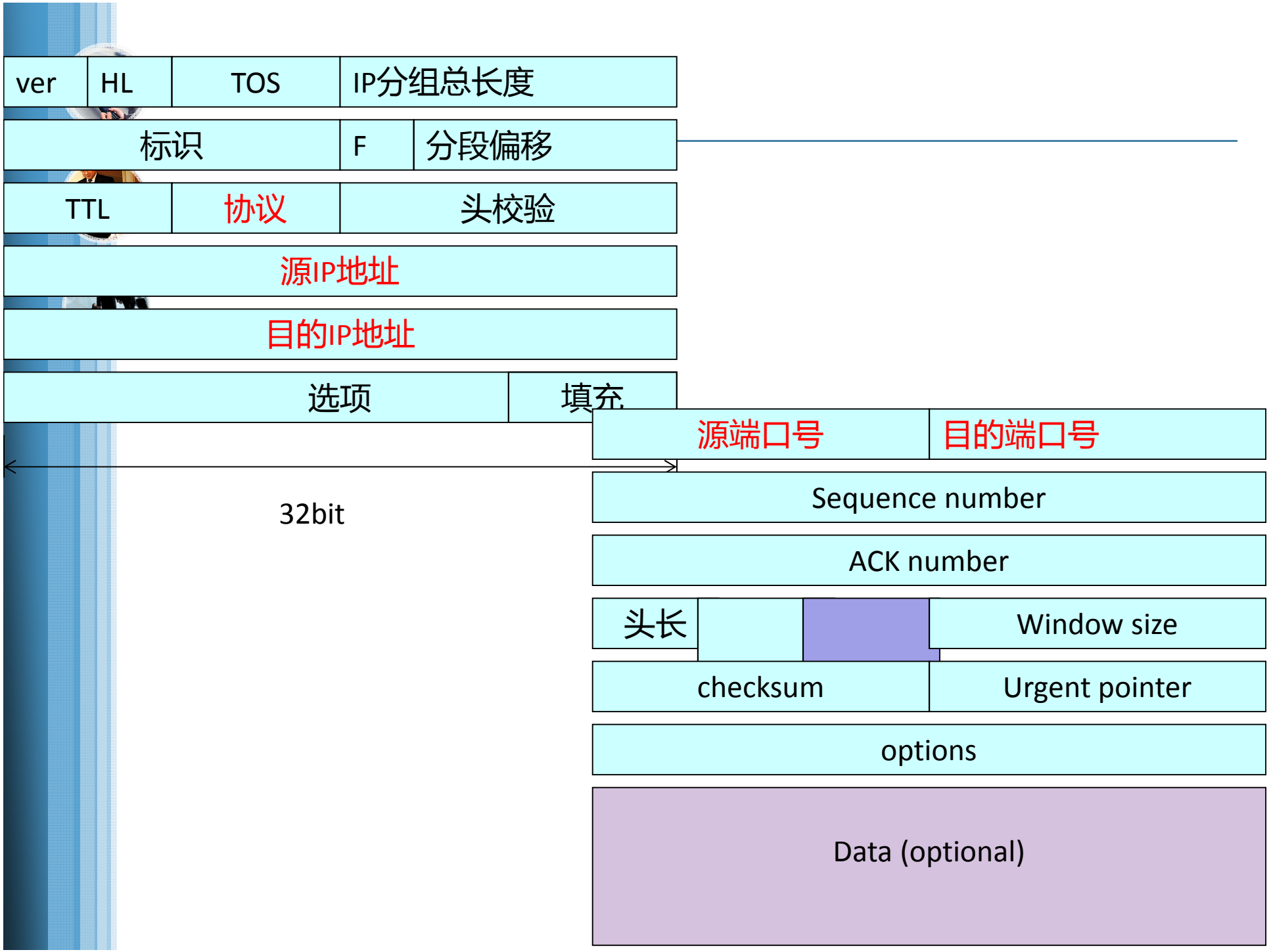
防火墙技术种类

- 包（IP分组）过滤技术（ Packet filter ）
  - –基本包过滤（静态包过滤）
  - –基于状态检测的包过滤（动态包过滤）
  - –常见包过滤设备/软件
    - 路由器访问控制表ACL
    - 硬件包过滤设备
    - 软件：ipchains / netfilter
    - netfilter/iptables ： http://www.netfilter.org/ 或者 http://www.iptables.org/
- 代理服务技术
  - –应用层网关级防火墙



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（成为访问控制表或ACL），根据对比结果的不同，决定该传输是被丢弃还是允许通过。
- 静态包过滤的依据：
  - 包的目的地址及目的端口
  - 包的源地址及源端口
  - 包的传送协议
    - 基于TCP的传输：根据TCP报头的标志字来控制传输
    - 基于UDP的传输：根据端口号来控制
  - ICMP的消息类型
  - 包的大小


ver
HL
TOS
IP分组总长度
标识
F
分段偏移
TTL
协议
头校验
源IP地址
目的IP地址
选项
填充
32bit
源端口号
目的端口号
Sequence number
ACK number
头长
Window size
checksum
Urgent pointer
options
Data (optional)

状态检测包过滤（stateful inspect)

- 状态检测防火墙是一种动态包过滤防火墙，也称为自适应防火墙，它在基本包过滤防火墙的基础增加了状态检测的功能。
- 将数据包看成一个整体的数据流，维护一份连接表来动态监视通信会话的状态，而不是简单依靠包自身所包含的信息（如源地址、目的地址、端口号、标志）。

•例：允许内网用户访问Web

In-port	out-port	in/out	action
*	80	out	permit

Stateful:
建立状态，返回的包匹配后就会被允许



- 状态检测防火墙维护用户将要使用的所有传输的状态
  - –TCP：面向连接的，可以根据SYN，ACK等识别连接状态
  - –UDP：建立虚拟会话连接
  - –ICMP的处理要难一些，但它仍然有一些信息来创建虚拟的连接，关键是有些ICMP数据包是单向的，如当TCP和UDP传 输有错误时会有一个ICMP数据包返回。对于ICMP的处理，不同的防火墙产品可能有不同的方法



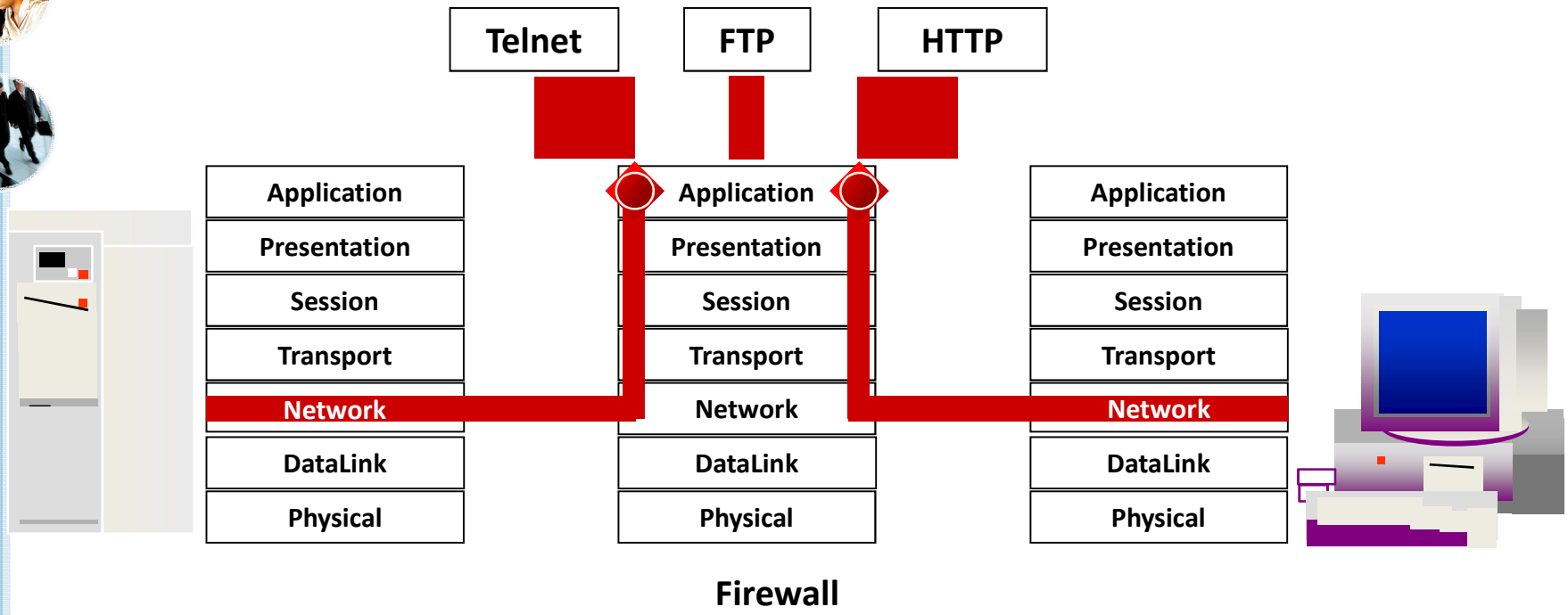
应用代理防火墙

- 应用代理防火墙工作在应用层，它针对专门的应用层协议制定数据过滤和转发规则，其核心技术是代理服务器技术。
- 应用代理防火墙的实现是基于软件的，主要包含三个模块：
  - 客户代理模块
  - 服务器代理
  - 过滤模块
- 客户代理模块负责处理客户的访问请求，由过滤模块分析和决定是否接受该请求；如果允许，则由服务器代理模块建立与服务器的连接，转发请求；服务器代理模块将服务器的应答传递给客户代理模块，再转发给客户。

常用软件：squid , wingate, MS ISA 等



应用层代理服务器(Proxy)



Firewall

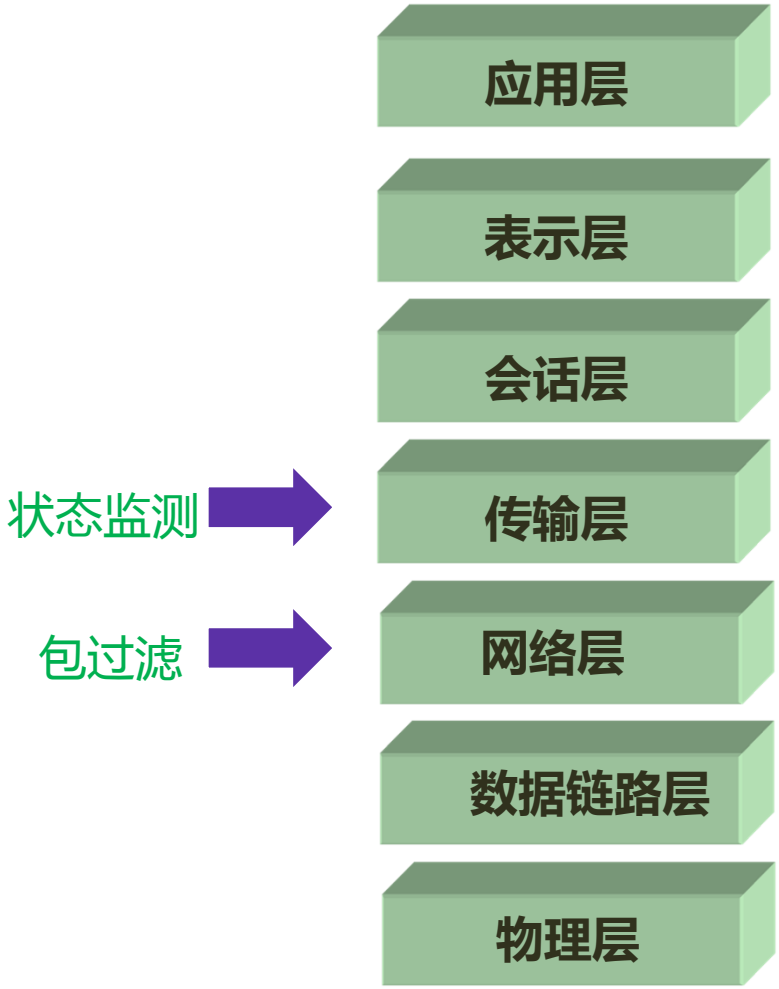
优点：
相对较高的安全性
可以实现访问的身份认证
可以在应用层控制服务的等级，权限

缺点：
性能较差，速度慢
每种访问服务需要单独的代理服务器
用户不透明

小结：传统防火墙工作模式



- **包过滤防火墙**
  - 路由器实现包过滤功能
- **应用代理防火墙**
  - 协议过于单一
- **基于状态监测的包过滤防火墙**
  - 主流技术
  - 主要工作在4层





防火墙的局限性

How to defeat firewalls

Take over the firewall.

Get packets through the firewall.

Get the information without going through the firewall.

- 防火墙不能防范未知的攻击方式
  - 关注TCP/IP攻击技术的发展
- 防火墙不能防范不经过防火墙的攻击
  - 确认防火墙是对外的唯一连接
  - 不能对付内部攻击
- 防火墙访问控制的粒度不够细
  - 对关键资源需要进一步的主机访问控制
- 防火墙自身不能防范病毒
  - 可以配合其他病毒监测设备实施病毒扫描和清除
- 可能带来内部的松懈心理
- 需要用户正确的配置

Unusual firewall bypassing techniques:
http://gray-world.net/

防火墙破坏了Internet端到端的特性，阻碍了新的应用的发展



防火墙发展

1. 虚拟防火墙:
CISCO使用Security Context建立虚拟防火墙
从PIX7.0和FWSM 2.2(1)开始，可以把物理的一个防火墙配置出多个虚拟的防火墙，每个防火墙称为context

2. **NGFW:**
Gartner认为下一 代防火墙有三个特征:

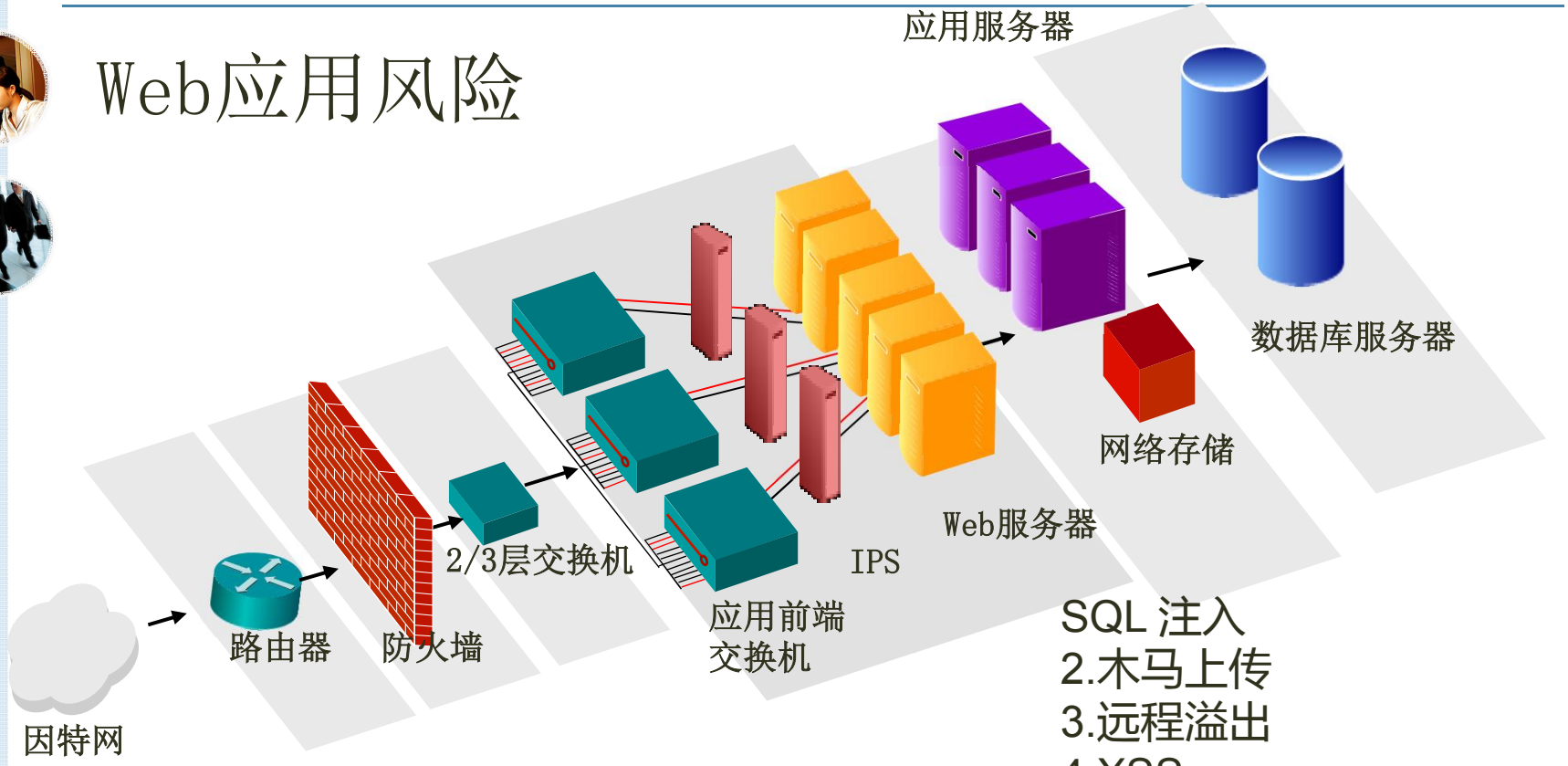
第一，下一代防火墙是基于角色和应用的管理设备;
第二，它具有传统防火墙的所有功能;
第三，具备智能的流量管理控制和策略配合。

基于策略的应用级管理软件，如：
网 管人员有哪些权限
财务系统人员可以访问财务的系统，其他人不能访问，
有些员工可以上外网有些不可以上



3.Web应用防火墙

Web应用风险



SQL 注入
2.木马上传
3.远程溢出
4.XSS
5.本地、远程包含漏洞利用
6.重要信息窃取
7.验证、认证绕过
8.Cookie、Session 劫持
9.网站挂马
10.应用层 DOS 攻击



3.WAF

Web应用防火墙工作在应用层，对HTTP(S)进行双向深层次检测： 对于来自Internet 的攻击进行实时防护， 避免黑客利
用应用层漏洞非法获取或破坏网站数据，

Web 应用漏洞扫描（安全评估）	SQL 注入、跨站脚本（XSS）漏洞扫描
网页挂马检测	网页挂马主动检测
Web 基础架构防护	蠕虫、缓冲区溢出、CGI 信息扫描、目录遍历等 Web 通用攻击防护
Web 应用安全防护	SQL 注入及 XSS 攻击防护
	跨站请求伪造（CSRF）攻击防护
	爬虫防护
	盗链防护
	恶意扫描防护
	Cookie 安全
	服务器信息伪装/过滤
	URL ACL
网页篡改防护	页面预取功能
	视觉恢复功能
	缓存更新时间设置
内容安全	恶意代码过滤
	敏感关键字自定义
抗拒绝服务攻击	TCP Flood 防护
	HTTP Flood 防护
网络层安全	ARP 欺骗防护
	L4 ACL
主动阻断方式	丢弃数据包、阻断 TCP 连接

网页篡改防护

网页篡改采用的主要手段
- **缓存溢出**
- **跨站脚本**
- **SQL注入**
- **已知WEB服务软件漏洞利用**

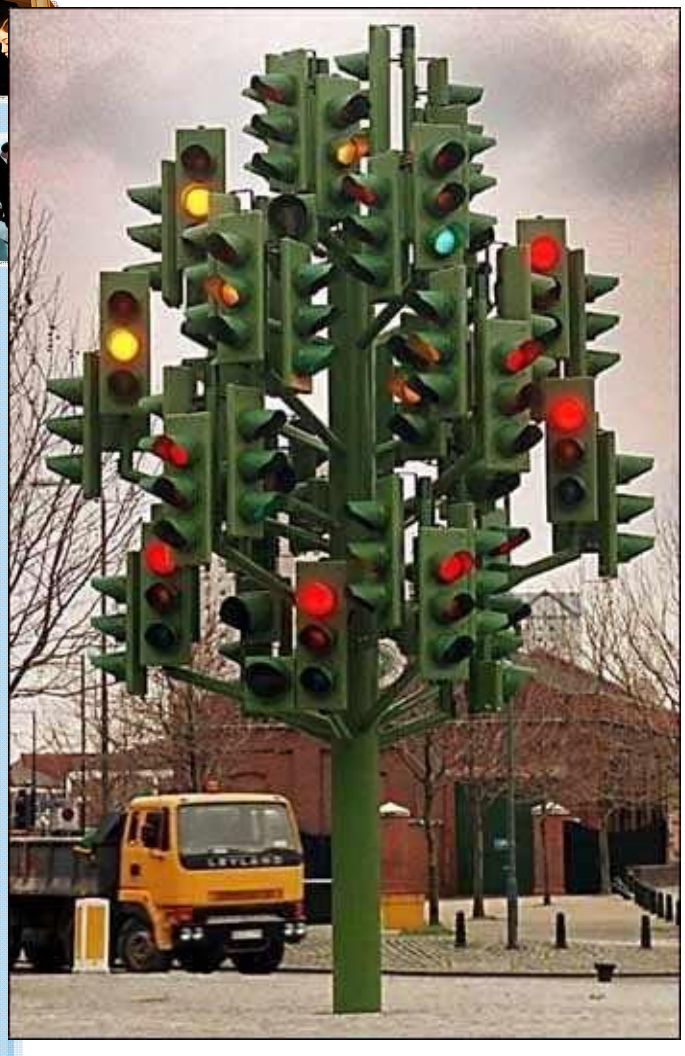
Web安全 › 规则配置 › 内容防护规则

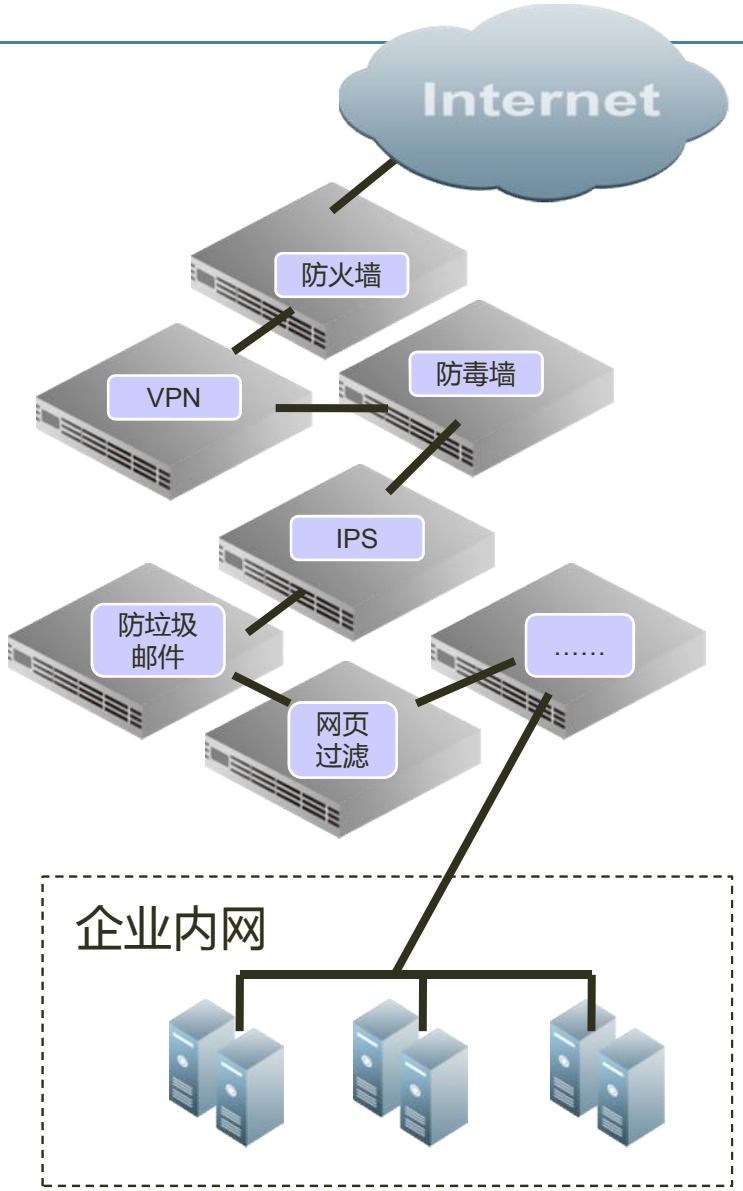
规则集 | 内置规则 | 自定义规则

ID	名称	描述
21757952	ms06-014-name	ms06-014
21757953	ms06-014-clsid	ms06-01
21757954	RealPlayer6_name_Trojan_horse	RealPlayer 6(IERPCtl.IERPCtl.1)
21757955	RealPlayer6_clsid_Trojan_horse	RealPlayer 6(IERPCtl.IERPCtl.1)
21757956	RealPlayer_11_name_Trojan_horse	RealPlayer 11
21757957	RealPlayer_11_clsid_Trojan_horse	RealPlayer 11
21757958	GLWorld_GLIEDown2_name	GLWorld GLIEDown2
21757959	GLWorld_GLIEDown2_name_clsid	GLWorld GLIEDown2
21757960	GLWorld_GLCHAT.GLChatCtrl.1_name	GLWorld GLCHAT.GLChatCtrl.1
21757961	GLWorld_GLCHAT.GLChatCtrl.1_clsid	GLWorld GLCHAT.GLChatCtrl.1
21757962	Thunder_DPClient.Vod_name	Thunder DPClient.Vod

NSFocus

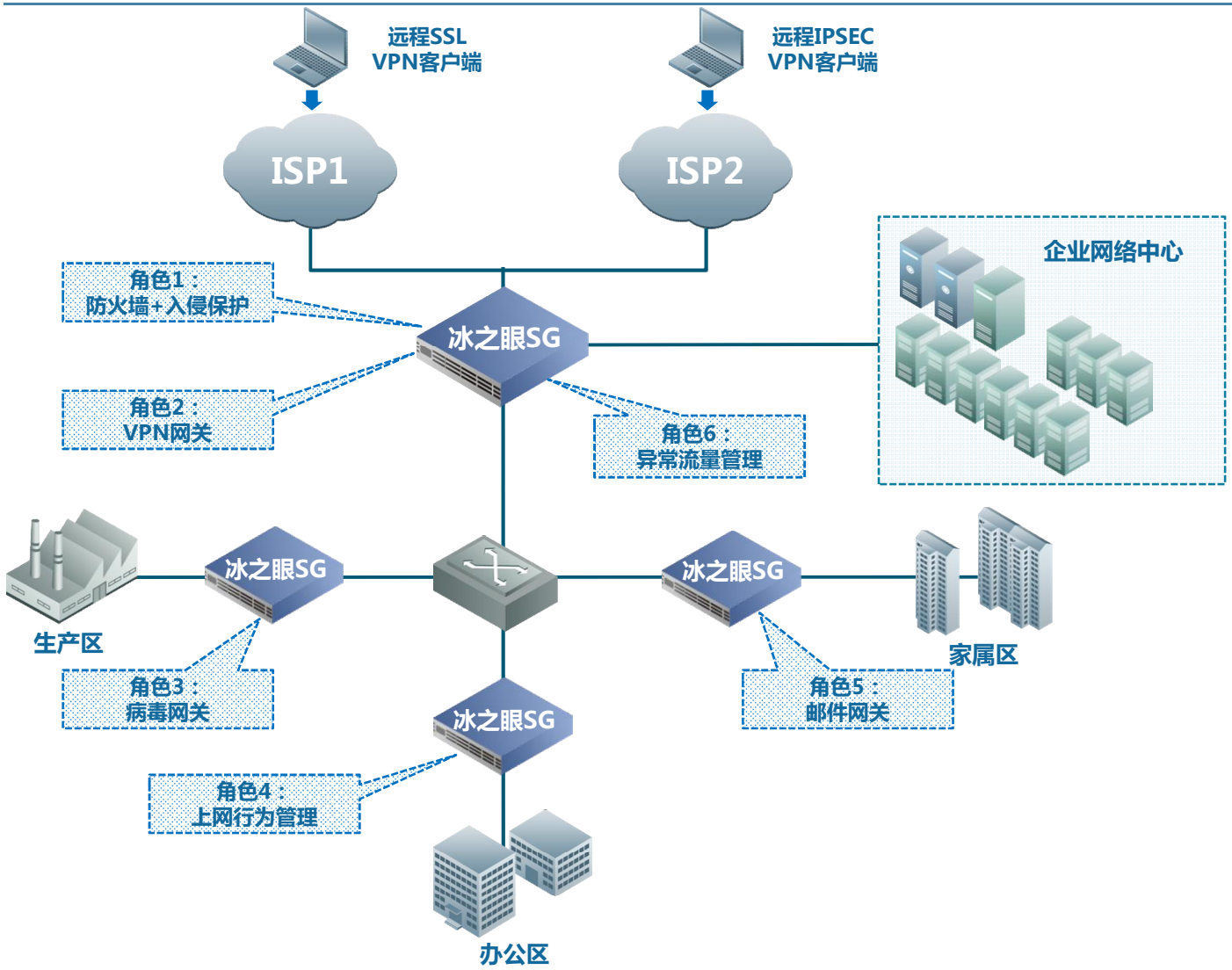
4. 安全网关SG(security gateway)







典型应用



冰之眼SG在某大型企业典型部署