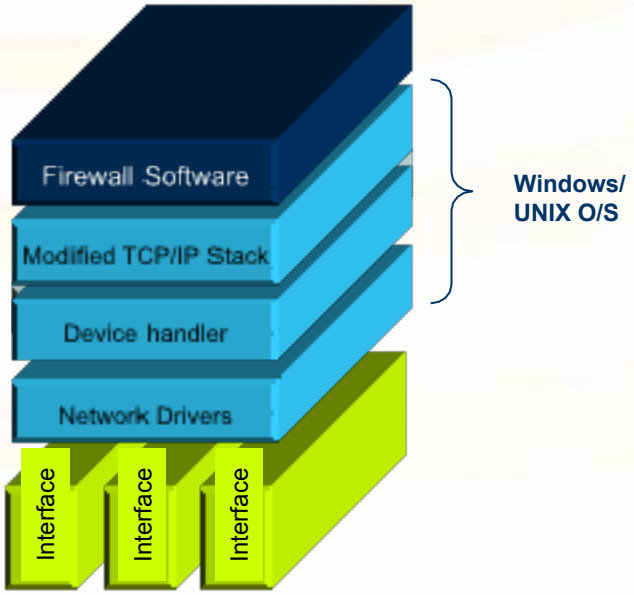
阿姆瑞特
Amaranten

Amaranten International Ltd
Operation in China

”Amaranten - Secure Net!”

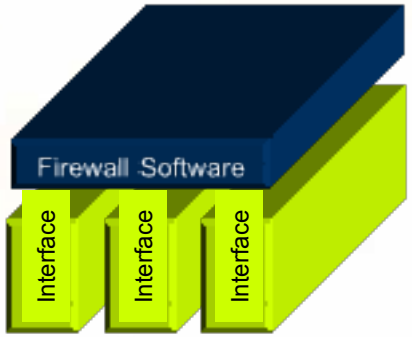
无操作系统

老式防火墙构造



- 处理速度慢
- 安全漏洞
- 操作系统和防火墙软件单独升级

阿姆瑞特防火墙构造



Security

- 无操作系统漏洞

Performance

- 防火墙内核从底层接管进出防火墙数据并进行处理 利用全部可能的硬件性能 。降低了操作系统的开销 所以能够最快的处理数据，全部产品延时不大于25us，是目前世界上延时最小的防火墙产品
- 内核开启速度快，开启时间6秒，18-20秒进入数据包转发

阿姆瑞特 Amaranten

产品线简介

F5000 Series

F3000 Series

- 高负荷的VPN网络
- 数据中心
- 电信级网络
- 电信业

F1800 Series

- 大型高校
- 数据中心，服务提供商
- 金融机构

F600 Series

- 大型VPN网关
- 企业总部/大型企业

F300 Series

- 中型企业
- 中型VPN网关
- 服务提供商

F100Series

- 中小型企业
- 中小型企业的VPN网关
- 可安全管理的CPE

F50 Series

- 远程办公/小型分支机构
- 小型企业
- 可安全管理的CPE

阿姆瑞特
Amaranten

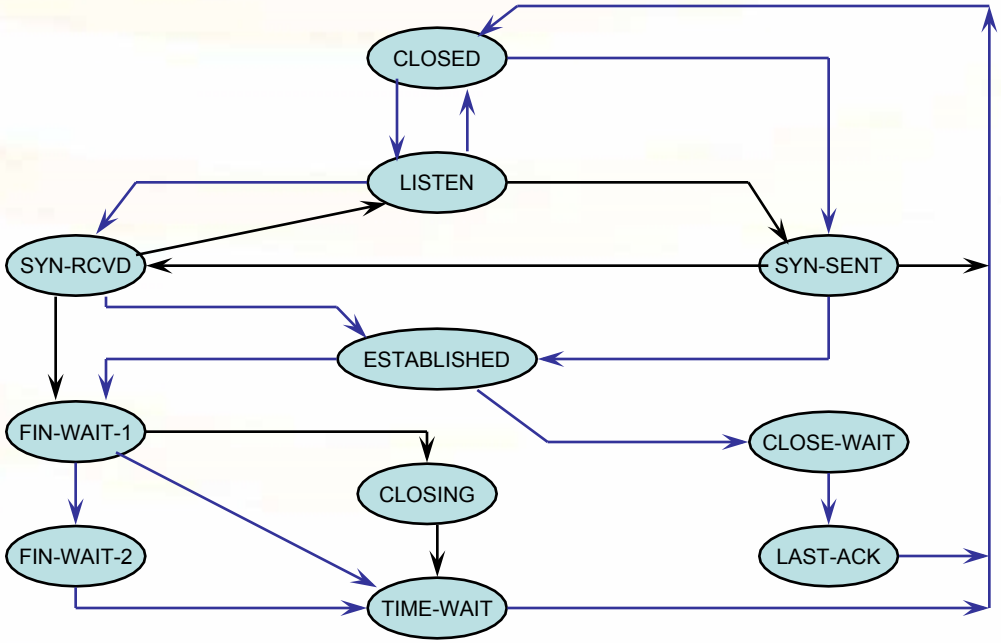
阿姆瑞特防火墙技术特点

- 全方位安全防护
- 强大的路由功能
- 专业的带宽管理
- 灵活的网络接入
- 丰富的VPN功能
- 便捷的图形管理
- 细微的网络日志

阿姆瑞特 Amaranten

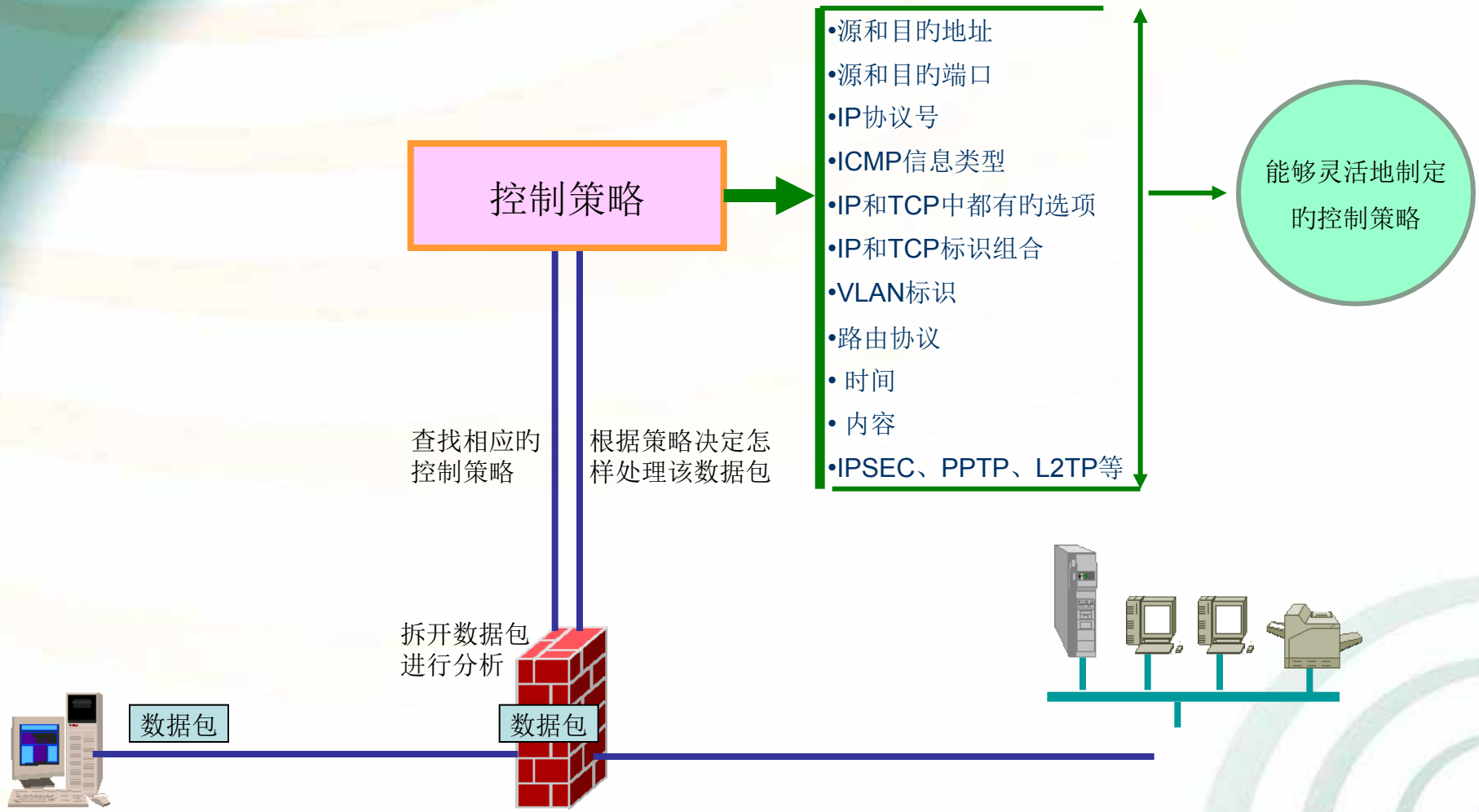
全状态检测防火墙

- 采用状态检测技术
- 数据包一致性检验
- 预防假冒IP攻击
- 放置非正常连接
- 提升工作效率

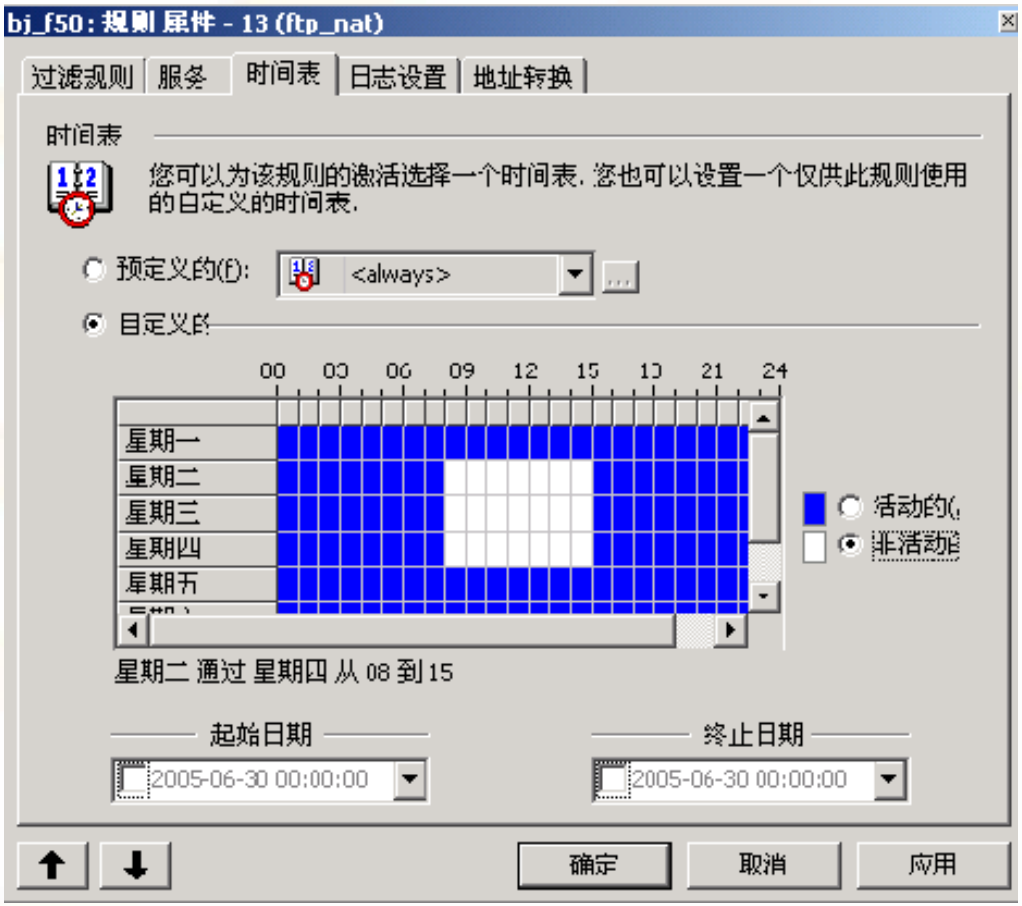


Illegal Addresses
Checksum Control
TTL Control
Layer Size Consistency
IP Option Sizes
IP Source Route
IP Timestamp
IP Bad Options
IP Reserved flag
TCP Blind Spoofing Protection
TCP Header Option Sizes
TCP MSS Control
TCP Window Scale
TCP Selective ACK
TCP Timestamp
TCP Alternate Checksum
TCP Connection Count
TCP Bad Options
TCP Flag combinations
TCP Reserved Field
TCP NULL Packets
ICMP Response Control
ARP Spoofing Protection
Strict Interface Matching
Connection Timeout Control
Payload Size Control
Reassembly Timing Control
Illegal Fragments
Duplicate Fragments
Fragmented ICMP

灵活的访问控制


控制策略
•源和目的地址
•源和目的端口
•IP协议号
•ICMP信息类型
•IP和TCP中都有的选项
•IP和TCP标识组合
•VLAN标识
•路由协议
• 时间
• 内容
•IPSEC、PPTP、L2TP等
能够灵活地制定的控制策略
查找相应的控制策略
根据策略决定怎样处理该数据包
拆开数据包进行分析
数据包
数据包

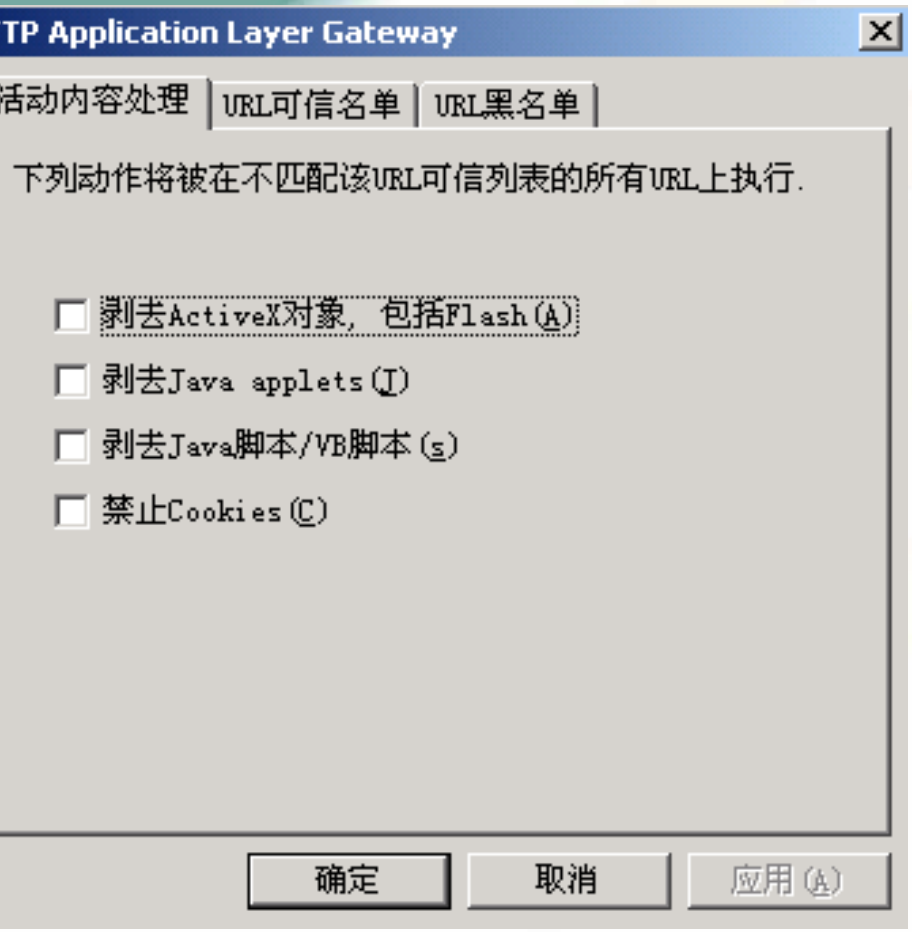
基于时间的控制

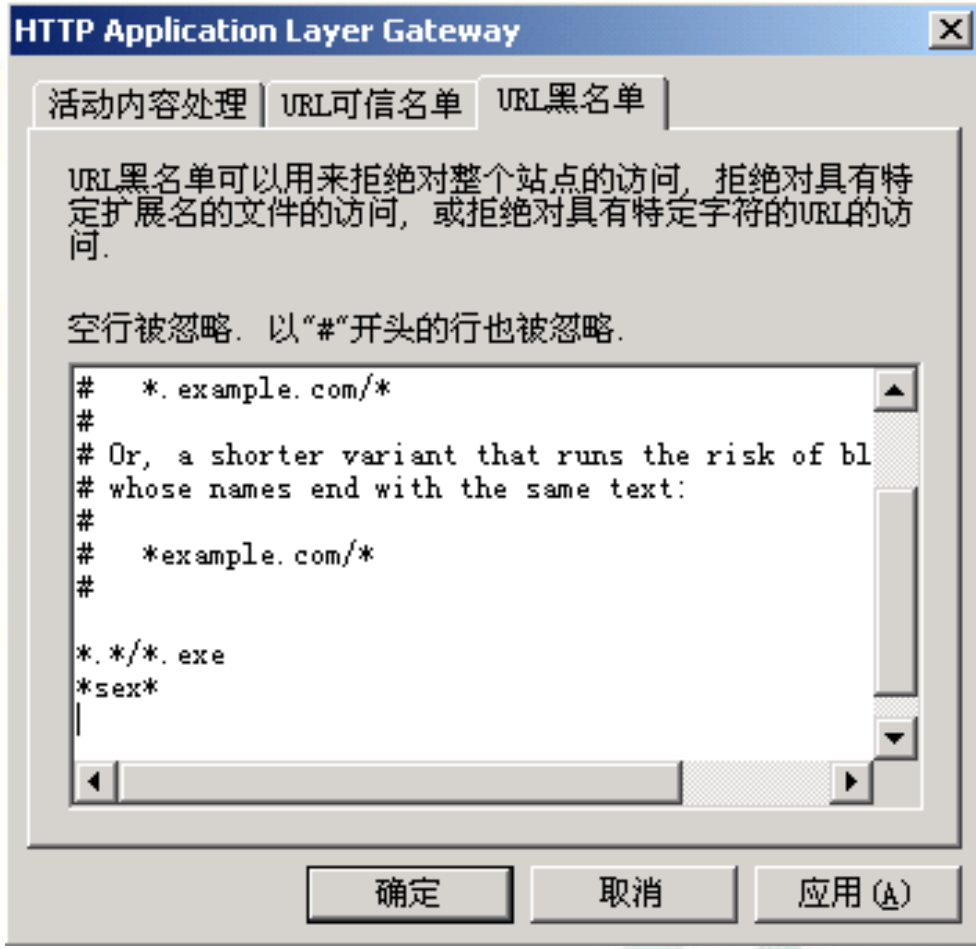


- 控制某条规则的生效时间

内容过滤

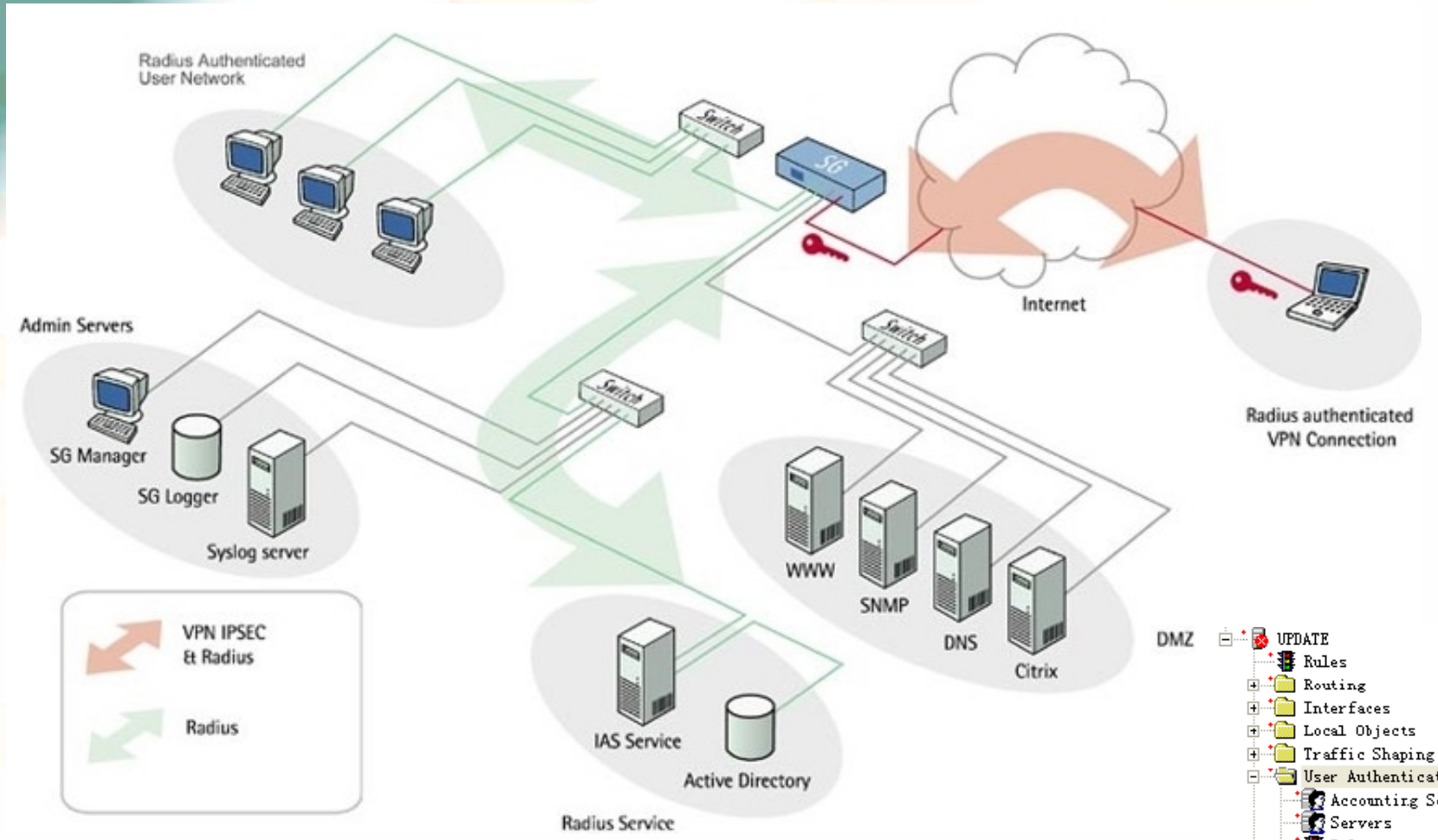
- 阿姆瑞特防火墙功能能够经过URL过滤和关键字过滤控制内部人员访问的主页或站点，防止具有恶意代码网页（网页木马、网页病毒）对网络的侵害。
- 除了内容过滤以外，还能够做到下列特征：
  - 禁止下载某种类型文件。例如：.exe
  - 针对Java脚本/VB脚本、Java applets的过滤；
  - 禁止Active-X/Flash等内容，彻底杜绝了黑客网站恶意程序对内网机器的攻击；
  - 禁止cookies，预防黑客经过cookies窃取顾客名、口令等关键信息。


TP Application Layer Gateway
活动内容处理
URL可信名单
URL黑名单
下列动作将被在不匹配该URL可信列表的所有URL上执行.
剥去ActiveX对象，包括Flash(A)
剥去Java applets(J)
剥去Java脚本/VB脚本(S)
禁止Cookies(C)
确定
取消
应用(A)


HTTP Application Layer Gateway
活动内容处理
URL可信名单
URL黑名单
URL黑名单可以用来拒绝对整个站点的访问，拒绝对具有特定扩展名的文件的访问，或拒绝对具有特定字符的URL的访问.
空行被忽略. 以"#"开头的行也被忽略.
.example.com/
#
Or, a shorter variant that runs the risk of bl
whose names end with the same text:
#
example.com/
#
./*.exe
sex
确定
取消
应用(A)

阿姆瑞特 Amaranten

顾客认证



阿姆瑞特 Amaranten

顾客认证

- **深层次访问控制**
  基于顾客的信誉度，访问时间以及访问的内容，允许或拒绝访问
- **进一步增强了安全性**
- **认证方式**
  - 内部顾客数据库， Radius，微软活动目录或Xauth
- **日志**
  - 基于顾客级别的日志统计
- **优势**
  - 增长安全性的同步降低管理开销（在网络顾客数据库里面删除一种顾客也是经过网关来控制）
  - 顾客认证与策略、时间表和内容过滤等功能结合提升了防火墙使用效率（在工作时间阻止不需要的访问）
  - 支持RADIUS通用顾客数据库
  - 基于login方式的顾客身份登陆

强大的抗攻击能力

- OS Fingerprinting 和 Firewalking
- 网络的TCP/UDP端口扫描
- SYN flood
- ICMP flood攻击
- UDP flood攻击
- 死ping(Ping of death)攻击
- IP欺骗(IP spoofing)攻击
- 端口扫描(Port scan)
- 陆地攻击(Land attack)
- 撕毁攻击(Tear drop attack)
- 过滤IP源路由选项(Filter IP source route option)
- IP地址扫描攻击(IP address sweep attack)
- WinNuke attack攻击
- Java/ActiveX/Zip/EXE
- Dos & DDoS攻击
- 顾客定义的不良URL
- Per-source session limiting攻击
- Syn fragments攻击
- Syn and Fin bit set攻击
- No flags in TCP攻击
- FIN with no ACK攻击
- ICMP fragment攻击
- Large ICMP攻击
- IP record route攻击
- IP security options攻击
- IP stream攻击
- IP bad option攻击
- Unknown protocols攻击

阿姆瑞特 Amaranten

防攻击原理

- 老式的防火墙
  - 经过设定阈值进行攻击防范，例如每个IP每秒2023个SYN报文下列才以为是正常的，超出视为攻击
  - 依托通用OS，OS对攻击的抵抗能力不足；且防火墙软件与OS间必然存在开销，消耗系统资源
- 阿姆瑞特防火墙
  - 采用类似代理技术进行攻击防范，必须首先与防火墙建立起连接，防火墙才会再与主机进行连接，攻击不会经过防火墙到达主机
  - 专用内核，没有OS开销，提升了本身抵抗攻击能力
  - 设计中充分考虑了系统抗攻击的能力，预留防火墙系统资源，任何情况下CPU利用率都不会到达100%

阿姆瑞特
Amaranten

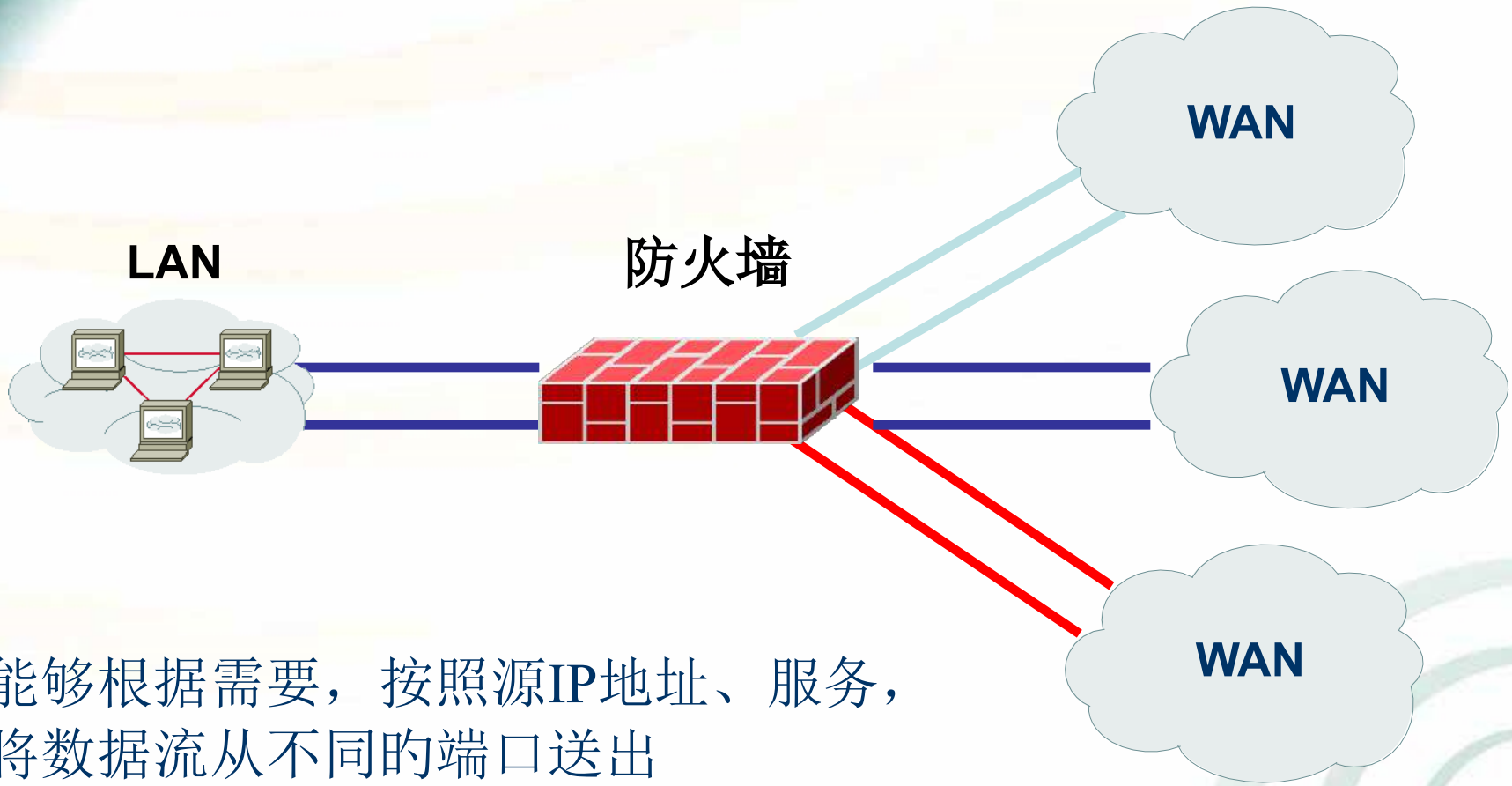
阿姆瑞特防火墙技术特点

- 全方位安全防护
- 强大的路由功能
- 专业的带宽管理
- 灵活的网络接入
- 丰富的VPN功能
- 便捷的图形管理
- 细微的网络日志

强大的路由功能

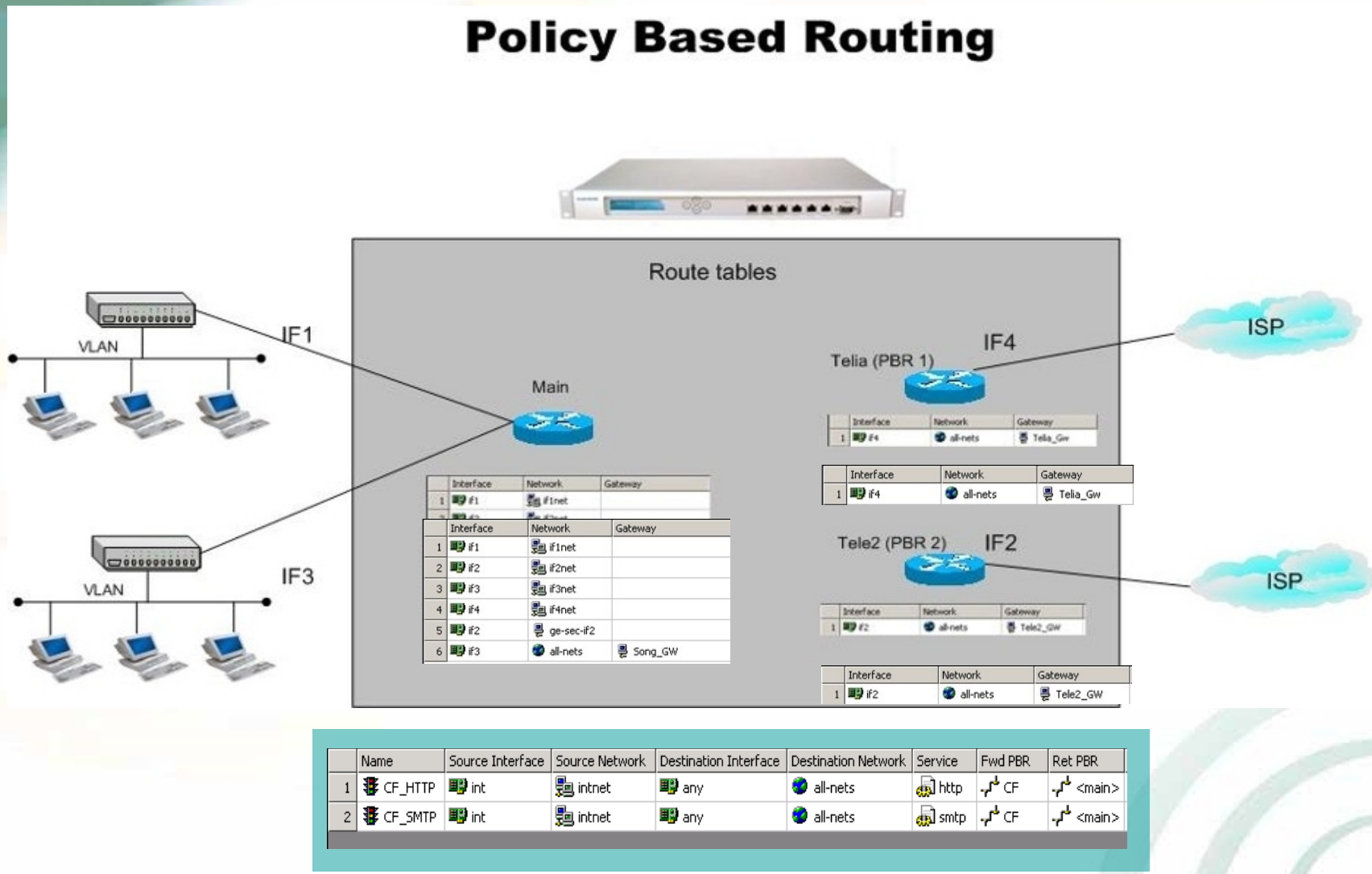
- 支持4096条静态路由
- 支持PBR（Policy Based Routing，基于策略的路由），配置主路由表和多种PBR路由表，不同的规则采用不同的路由表，支持多种缺省网关
- 支持路由备份
- 支持OSPF V2动态路由
- 支持虚拟路由器/系统
- 全方面支持802.1Q

基于策略的路由（PBR）



能够根据需要，按照源IP地址、服务，
将数据流从不同的端口送出

基于策略的路由



	Name	Source Interface	Source Network	Destination Interface	Destination Network	Service	Fwd PBR	Ret PBR
1	CF_HTTP	int	intnet	any	all-nets	http	CF	<main>
2	CF_SMTP	int	intnet	any	all-nets	smtp	CF	<main>

使用策略路由

—反垃圾邮件/抗病毒/HTTP代理

- **更安全**

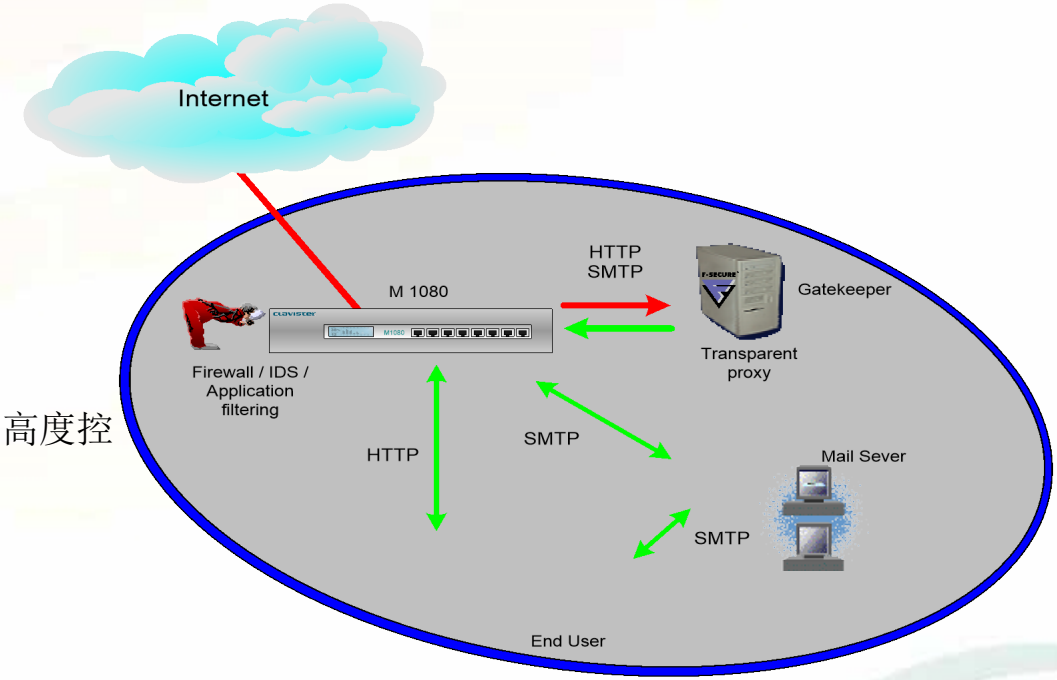
  防火墙预防了来自内外部的恶意攻击

- **更大的吞吐量**

  只有特定的网络需要经过抗病毒/垃圾扫描和HTTP代理，确保网络的吞吐量

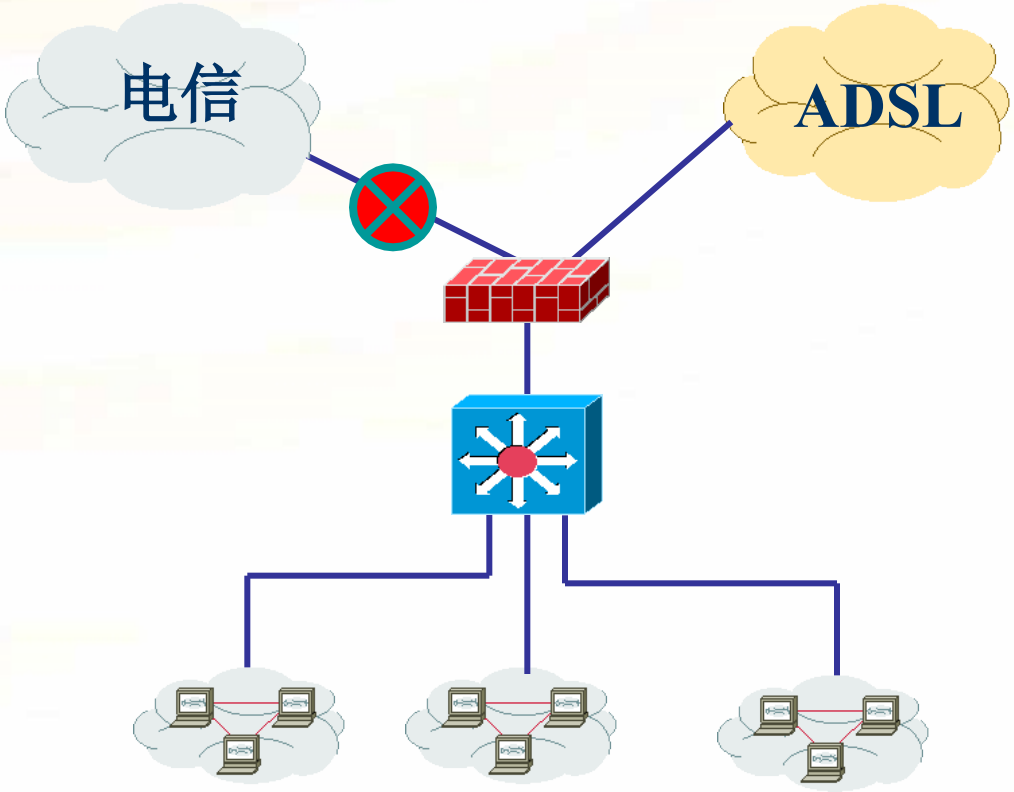
- **管理优势**

  不需要客户端的代理设置，防火墙能够高度控制信息流量

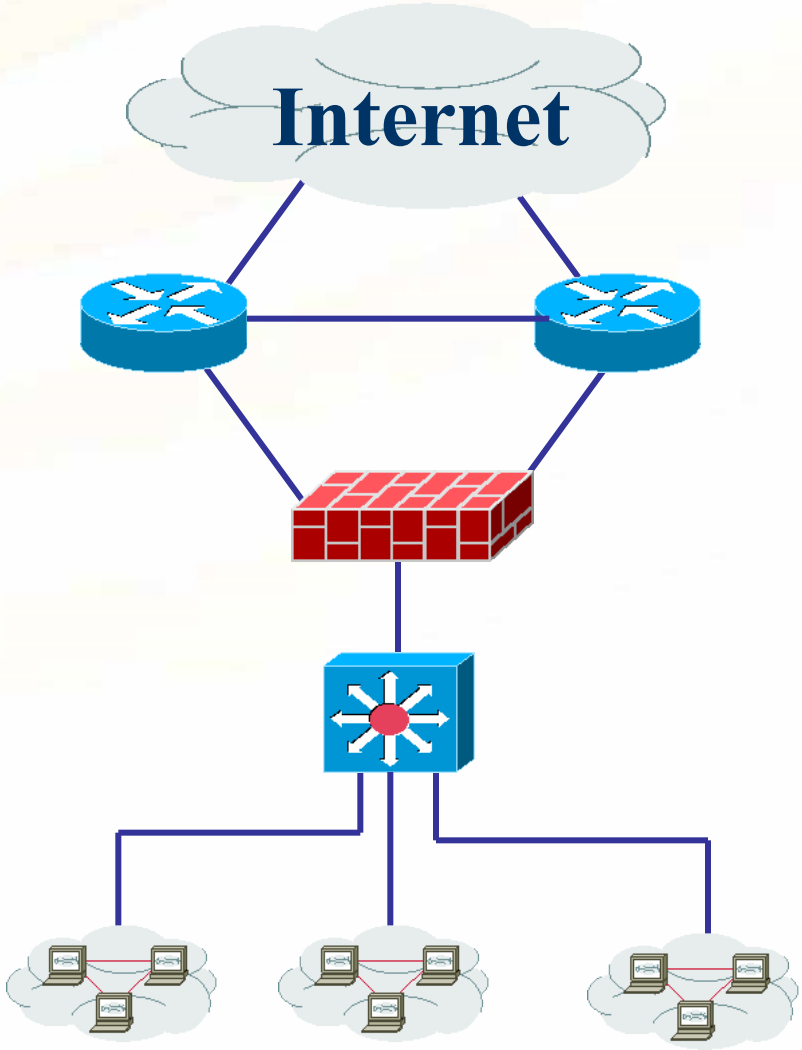


	Name	Source Interface	Source Network	Destination Interface	Destination Network	Service	Fwd PBR	Ret PBR
1	CF_HTTP	int	intnet	any	all-nets	http	CF	<main>
2	CF_SMTP	int	intnet	any	all-nets	smtp	CF	<main>

支持路由备份

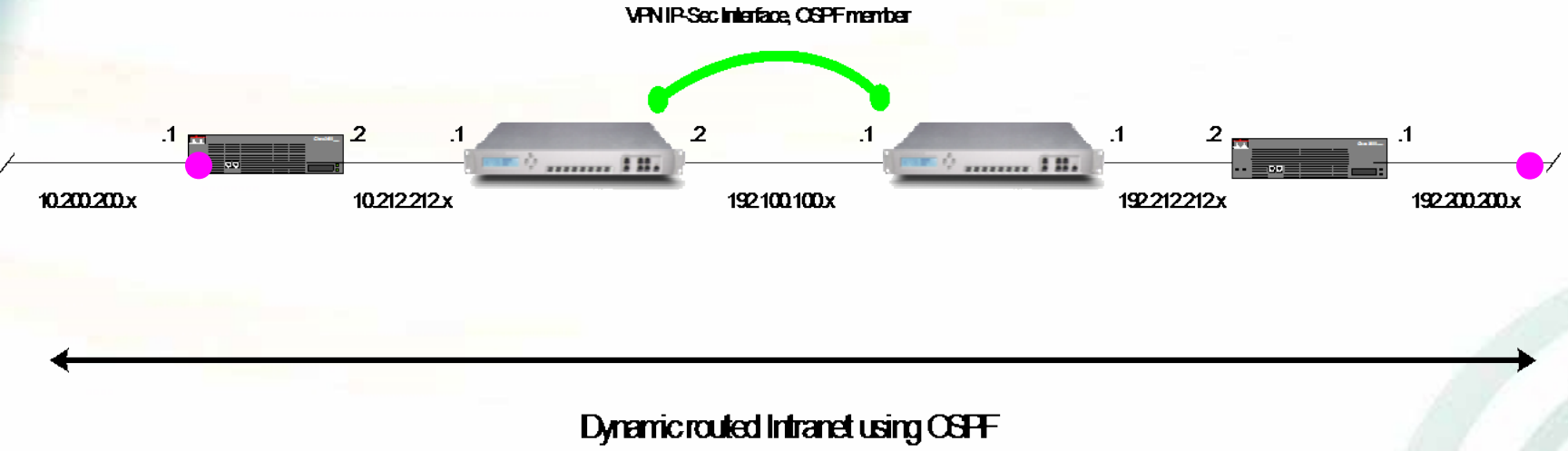


全方面支持OSPF

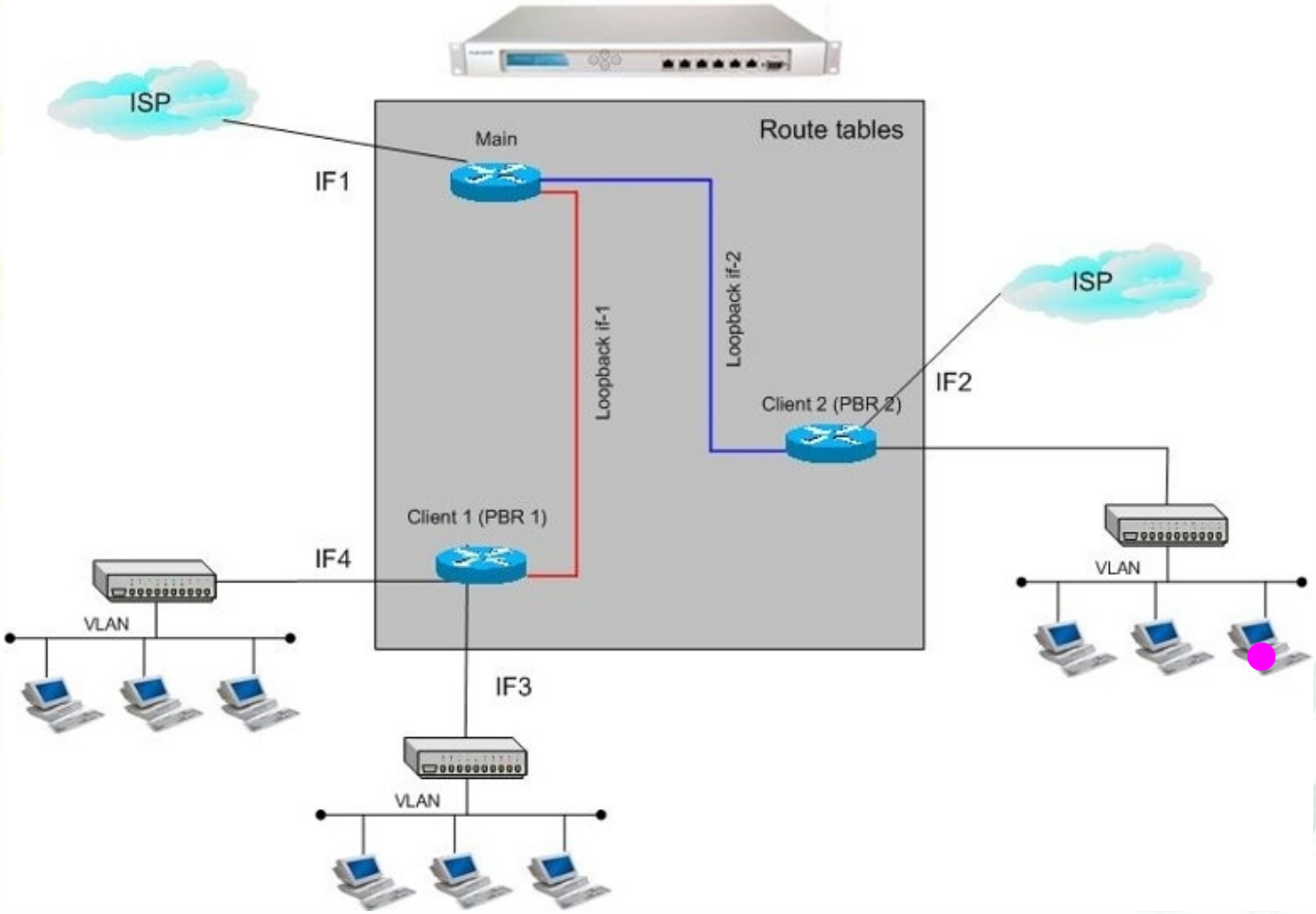


VPN接口支持动态路由

OSPF动态路由信息能够穿越VPN通道，进行传递。

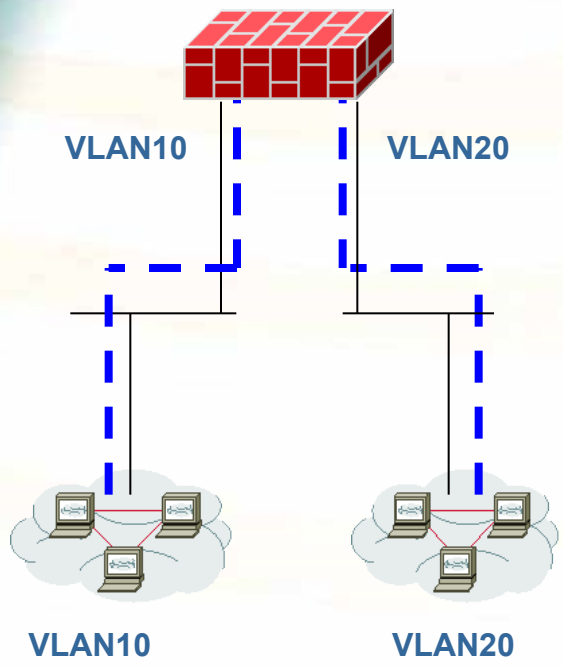


虚拟路由/系统

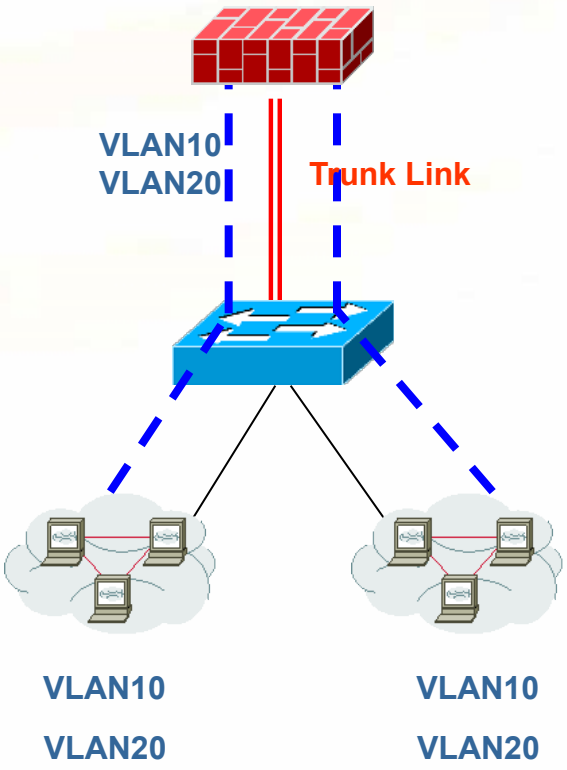

ISP
Main
Route tables
IF1
Loopback if-1
Loopback if-2
ISP
IF2
Client 2 (PBR 2)
Client 1 (PBR 1)
IF4
VLAN
VLAN
IF3
VLAN

对VLAN（802.1Q）的支持

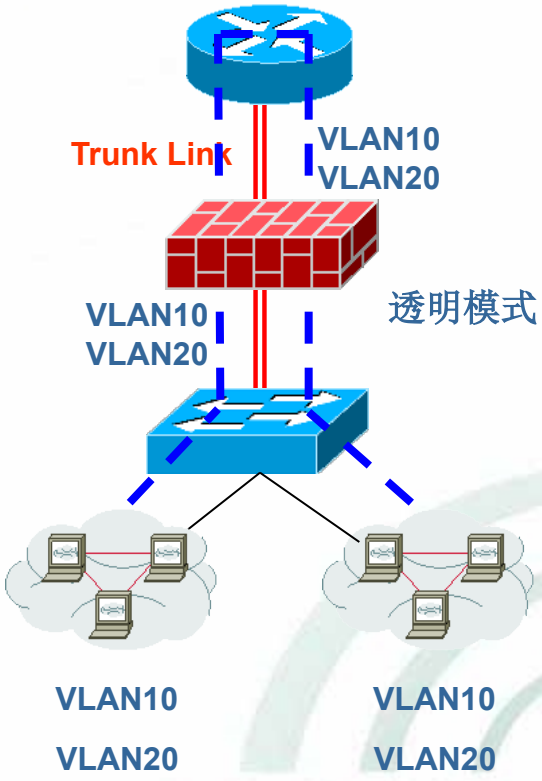
VLAN间路由



Trunk扩展端口



Trunk穿越



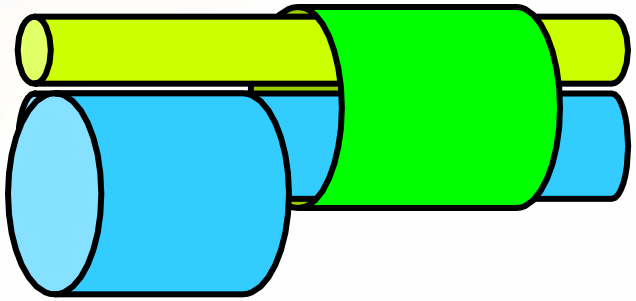
阿姆瑞特
Amaranten

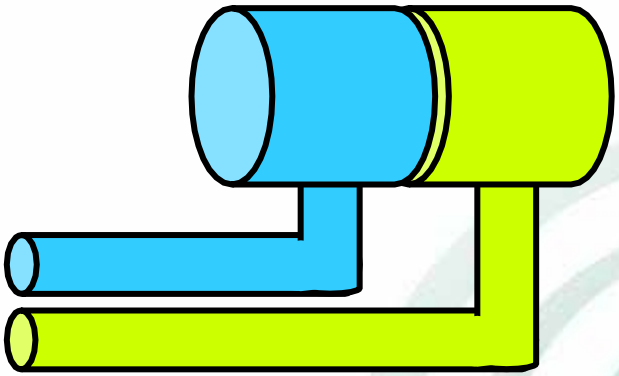
阿姆瑞特防火墙技术特点

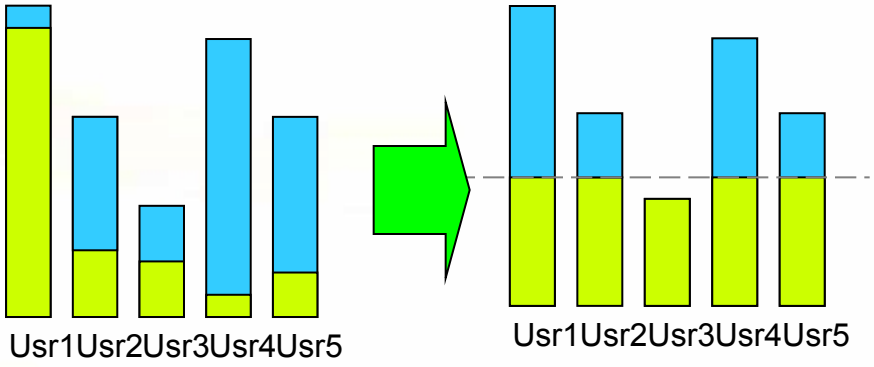
- 全方位安全防护
- 强大的路由功能
- 专业的带宽管理
- 灵活的网络接入
- 丰富的VPN功能
- 便捷的图形管理
- 细微的网络日志

带宽管理

- 最大带宽限制
- 带宽确保
- 传播优先控制
- 动态流量均衡
- 传播平衡控制

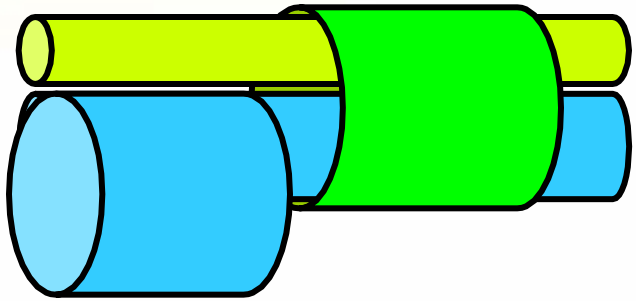






带宽控制

- 能够对顾客IP地址、服务等经过防火墙的带宽进行限制，例如：限制某个顾客对外访问最大带宽，或者访问某种服务的最大带宽。



带宽确保

- 确保网络中主要服务或者主要顾客的带宽不被其他服务或者顾客占用，从而确保了主要数据优先经过网络。

优先级控制

- 经过定义管道的方式提供CoS/QoS功能，而且管道没有数量的限制，也就是说优先级控制的等级没有数量的限制，同步可在每一种管道中，能够设定8个优先级（0-7），从而能够进行愈加细致的流量控制。

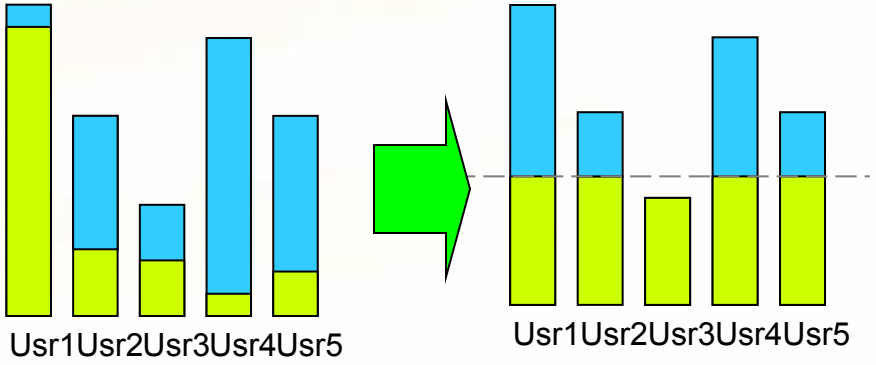
阿姆瑞特 Amaranten

动态流量均衡

- 为了确保网络中的全部带宽都得到合理的应用，防火墙提供动态流量均衡功能。
- 例如：假如某网络带宽为256k，设定主机A的带宽为100k，主机B带宽为156k。假如主机B目前只用到120k，而主机A100k的带宽不够用，此时主机A能够动态取得主机B剩余的36K带宽。假如主机B某一时刻的突发速率到156K，他会动态的从主机A那里取得属于他的36K带宽，从而确保主要服务或者顾客优先进行数据传播。

传播平衡控制

- 可根据需要进行设置，确保内网各顾客分配带宽趋于平衡，不致出现“贫富分化”的现象。



阿姆瑞特防火墙带宽管理特点

- 经过定义管道的方式提供CoS/QoS功能
- 管道没有数量的限制
- 设置精度为1Kbps，偏差率不超出5%
- 可进行带宽限制、带宽确保、动态均衡带宽
- 大差别带宽管理时，不存在“饿死”现象
- 可对上传和下载数据分别进行带宽管理
- 明通、密通数据均能够作带宽管理
- 带宽管理可基于接口、VLAN、IP地址、服务、时间等设定

阿姆瑞特
Amaranten

阿姆瑞特防火墙技术特点

- 全方位安全防护
- 强大的路由功能
- 专业的带宽管理
- 灵活的网络接入
- 便捷的图形管理
- 细微的网络日志

灵活的网络接入

- 透明、路由、混合接入
- 同一接口下的透明+NAT
- 源地址、目的地址同步转换
- 对称式接口设计