
# 防火墙原理与设计

杭州电子科技大学
陈黎丽

# 本讲内容概要

1 防火墙概述

2 防火墙的类型和结构

3 静态包过滤器

4 动态包过滤防火墙

5 电路级网关

6 应用级网关

# 本讲内容概要

7 状态检测防火墙

8 切换代理

9 空气隙防火墙

10 分布式防火墙

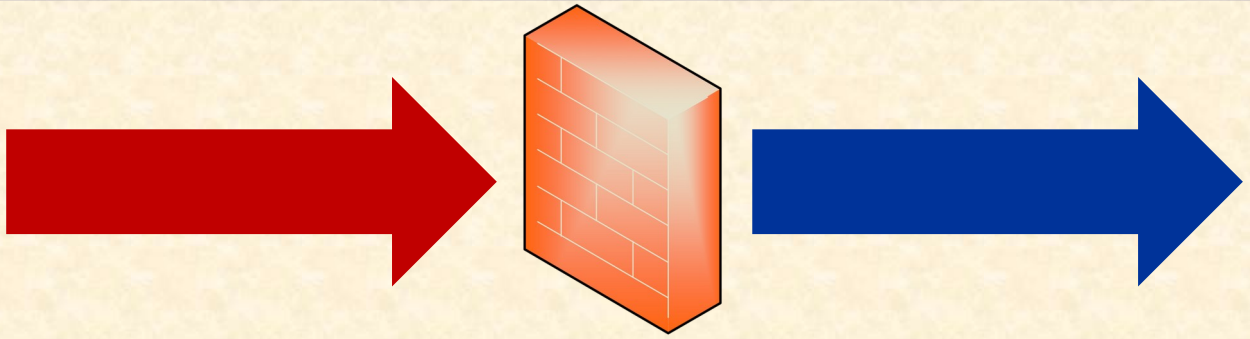
11 下一代防火墙

12 防火墙的典型产品

13 防火墙的发展趋势

# 防火墙概述

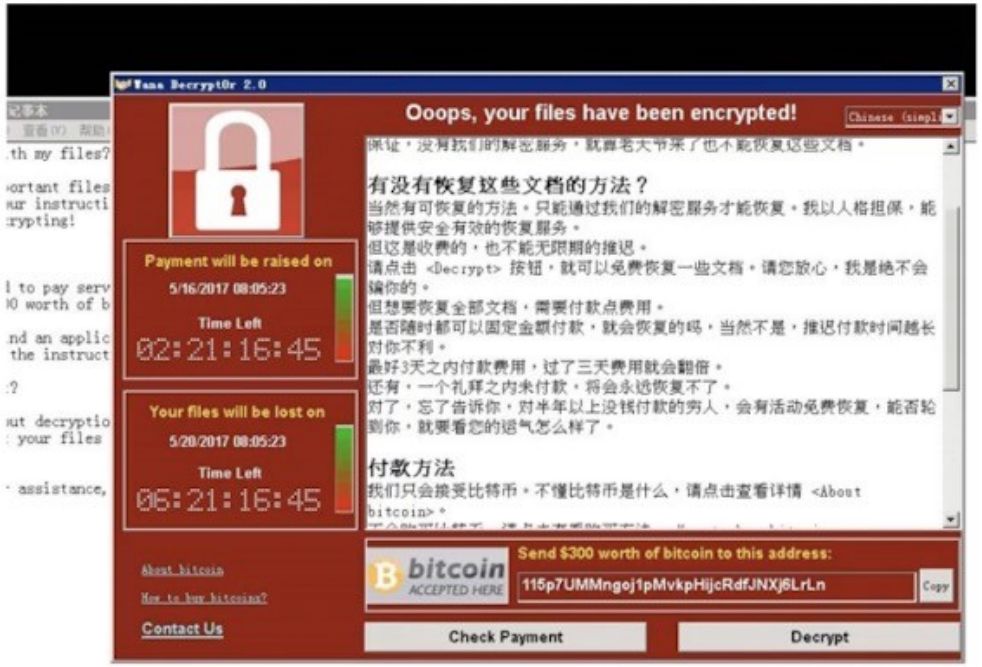
防火墙是由软件和硬件组成的系统，它处于安全的网络和不安全的网络之间，属于边界防护设备，由系统管理员设置访问控制规则，对进出网络边界的数据流进行过滤。




防火墙技术的功能主要在于及时发现并处理计算机网络运行时可能存在的安全风险、数据传输等问题，其中处理措施包括隔离与保护，同时可对计算机网络安全当中的各项操作实施记录与检测，以确保计算机网络运行的安全性，保障用户资料与信息的完整性。

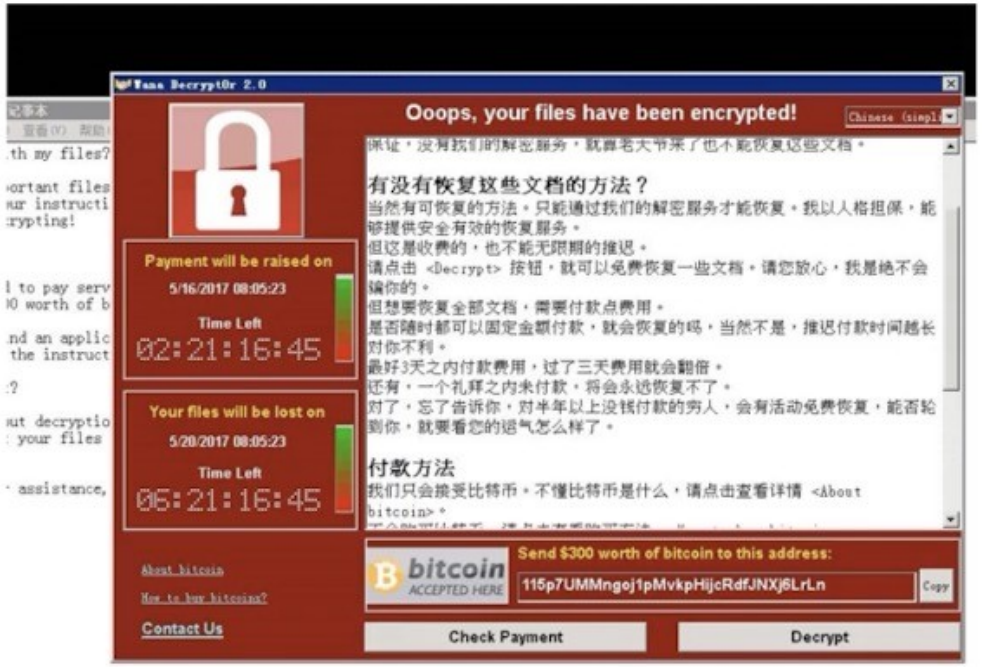
防火墙是 Internet 安全的最基本组成部分，但对于防御内部的攻击以及绕过防火墙的连接却无能为力。

# 防火墙概述


Ooops, your files have been encrypted!
Payment will be raised on
5/16/2017 08:05:23
Time Left
02:21:16:45
Your files will be lost on
5/20/2017 08:05:23
Time Left
06:21:16:45
有没有恢复这些文档的方法？
付款方法
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
About bitcoin
How to buy bitcoins?
Contact Us
Check Payment
Decrypt


DO NOT
ENTER
该内容被禁止访问

# 防火墙概述




入站流量过滤：常见病毒，网络攻击的过滤


出站流量过滤：非法网站流量，非法app应用

# 防火墙

天融信 NGFW® 下一代防火墙

华为 HiSecEngine
USG6600E 系列 AI 防火墙
（盒式）

# 防火墙对数据流的处理方式

根据安全策略，防火墙对**数据流**的处理方式分为如下三种：

- **允许**满足规则的数据流通过。 --- **访问控制**
- **拒绝**不满足规则的数据流通过，并向发送者回复一条消息，提示该数据流已被拒绝。
- 将数据流**丢弃**，不对这些数据包进行任何处理，也不会向发送者发送任何提示信息。

# 防火墙须满足的要求

| 1 | 2 | 3 |
| --- | --- | --- |
| 所有进出网络数据流都必须经过防火墙。 | 只允许经授权的数据流通过防火墙。 | 防火墙自身对入侵免疫，即确保自身安全。 |

# 本讲内容概要

1 防火墙概述

2 防火墙的类型和结构

3 静态包过滤器

4 动态包过滤防火墙

5 电路级网关

6 应用级网关

# 防火墙的发展史

| | |
|---|---|
| 第一代防火墙 | ● 1985-1988 ， Cisco 的 IOS 软件公司<br>➢ 包过滤防火墙 |
| 第二代防火墙 | ● 1989-1990 ， AT&T 贝尔实验室<br>➢ 电路级网关防火墙 |
| 第三代防火墙 | ● Purdue University ， AT&T 贝尔实验室<br>➢ 应用级网关防火墙 |
| 第四代防火墙 | ● 1991-1994 ，南加利福尼亚大学信息科学院<br>➢ 动态包过滤防火墙 |
| 第五代防火墙 | ● 1996 年，内核代理结构<br>➢ 1998 年， NAI 公司，自适应代理 |
| 第六代防火墙 | ● 2004 年， IDC 提出统一威胁管理 UTM 概念<br>➢ 将杀毒、 IDS 和防火墙安全设备划归 UTM |

# 防火墙的发展史

**第 ... 代防火墙**

- 伴随 Web 应用的发展，产生了 Web 应用防火墙（ WAF ）
- 审计设备、访问控制设备、架构 / 网络设计工具、 WEB 应用加固工具

**第 ... 代防火墙**

- 2009 年， Gartner 提出了下一代防火墙 NGFW 概念
- 下一代防火墙必须有标准的防火墙功能，如网络地址转换、状态检测、 VPN 等，以及企业所需要的 IPS 、防病毒、行为管理等功能。

**第 ... 代防火墙**

- 伴随云计算的发展，产生了云防火墙 / 云 WAF
- 统一管理互联网到业务的访问控制策略，支持全网流量可视和业务间访问关系可视。

**第 ... 代防火墙**

- 伴随人工智能的发展， 2017 年，华为推出 AI 防火墙
- 内置基于 AI 的高级威胁检测引擎，支持加密流量免解密威胁检测，联动云端

# 防火墙的发展史

2019 年，新华三集团以“主动安全，智慧驱动”为理念，推出全新变革的 AI 防火墙，应对新型网络威胁。


- 高速、稳定的海量业务处理性能；
- 智能关联分析的威胁检测引擎；
- 本地及云端的虚拟化技术；
- 快速的加密流量协议分析能力；
- 全局威胁可视的集中监控。

# 防火墙产业分布

中国网络安全行业全景图
（基于 2020 年度数据）



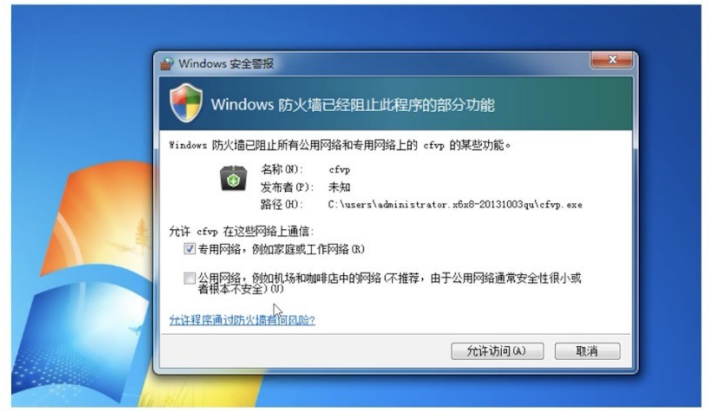
# 防火墙的分类

从逻辑上讲，防火墙可以大体分为主机防火墙和网络防火墙。

- **主机防火墙**：针对于单个主机进行防护。
- **网络防火墙**：往往处于网络入口或边缘，针对于网络入口进行防护，服务于防火墙背后的本地局域网。

从物理上讲，防火墙可以分为硬件防火墙和软件防火墙。

- **硬件防火墙**：在硬件级别实现部分防火墙功能，另一部分功能基于软件实现，性能高，成本高。
- **软件防火墙**：应用软件处理逻辑运行于通用硬件平台之上的防火墙，性能低，成本低。




软件防火墙：部署在用户电脑上，对个人电脑进行保护，由个人进行管理

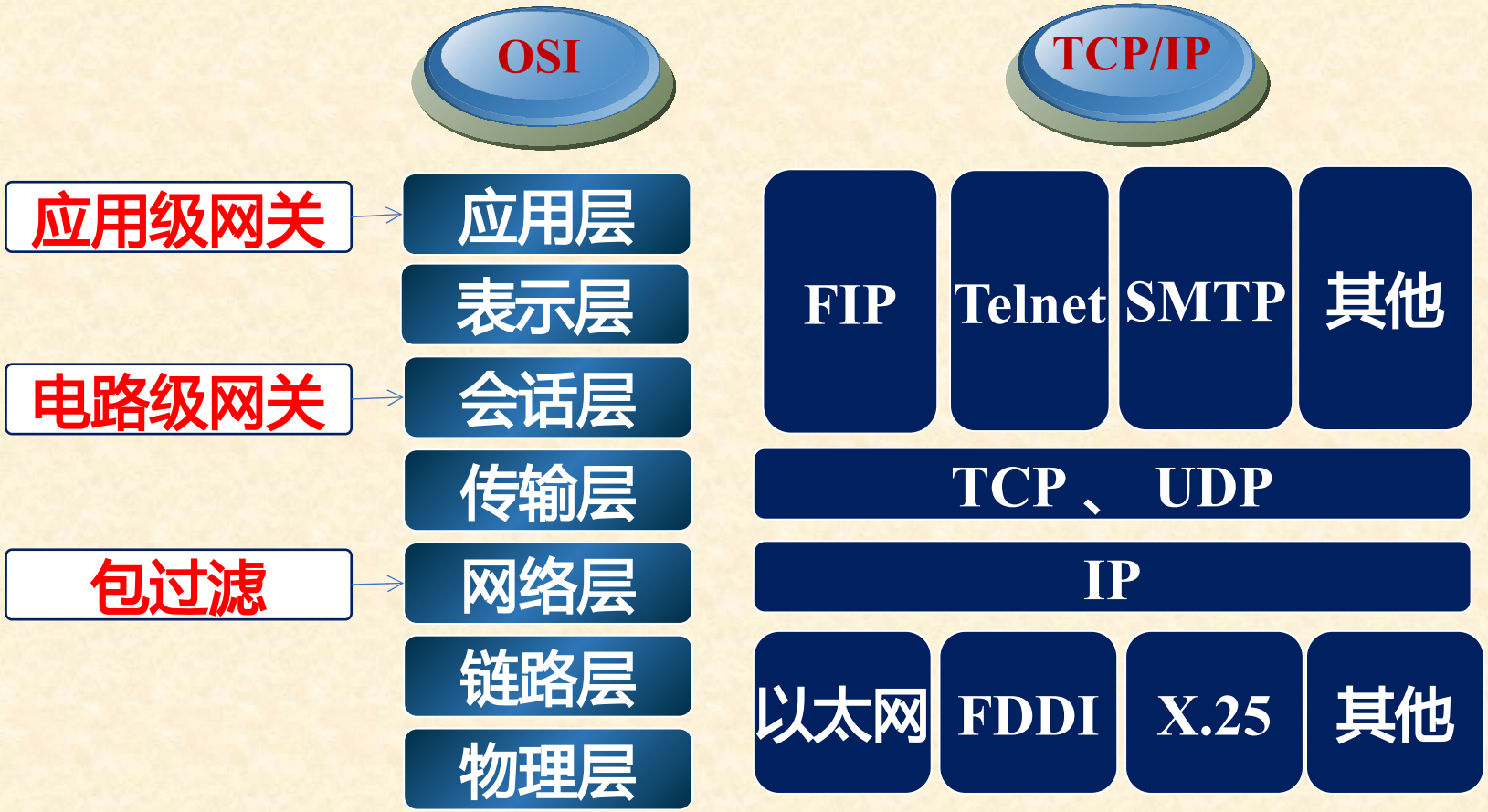

硬件防火墙：部署在网络边界，对整体网络进行保护，由专业网络工程师进行维护

# 防火墙的类型和设计结构


- 包过滤防火墙
- 电路级网关防火墙
- 应用级网关防火墙


- 静态包过滤
- 动态包过滤
- 电路级网关
- 应用层网关
- 状态检查包过滤
- 切换代理
- 空气隙（物理隔离）

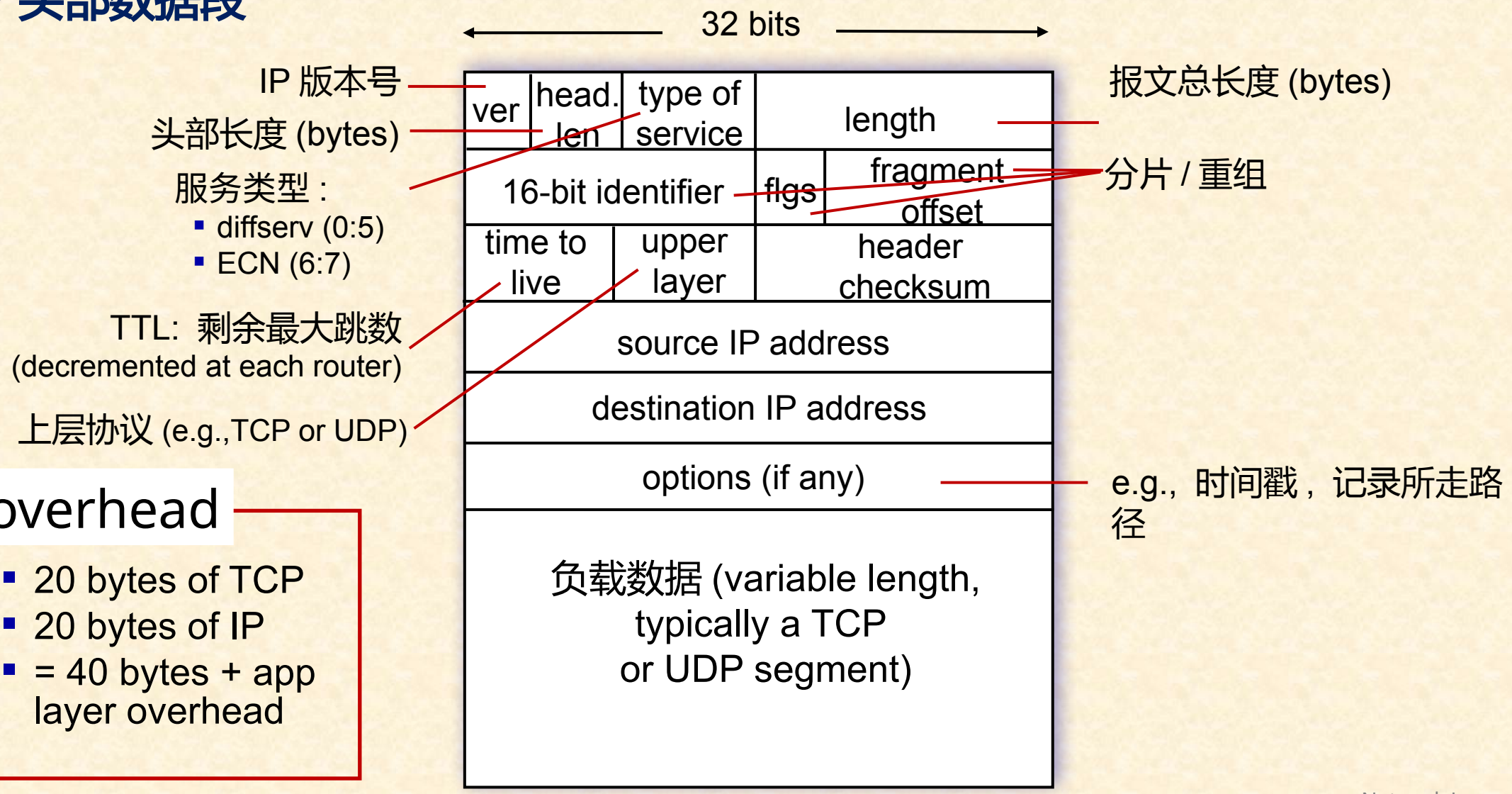
# OSI 模型与防火墙类型的关系




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

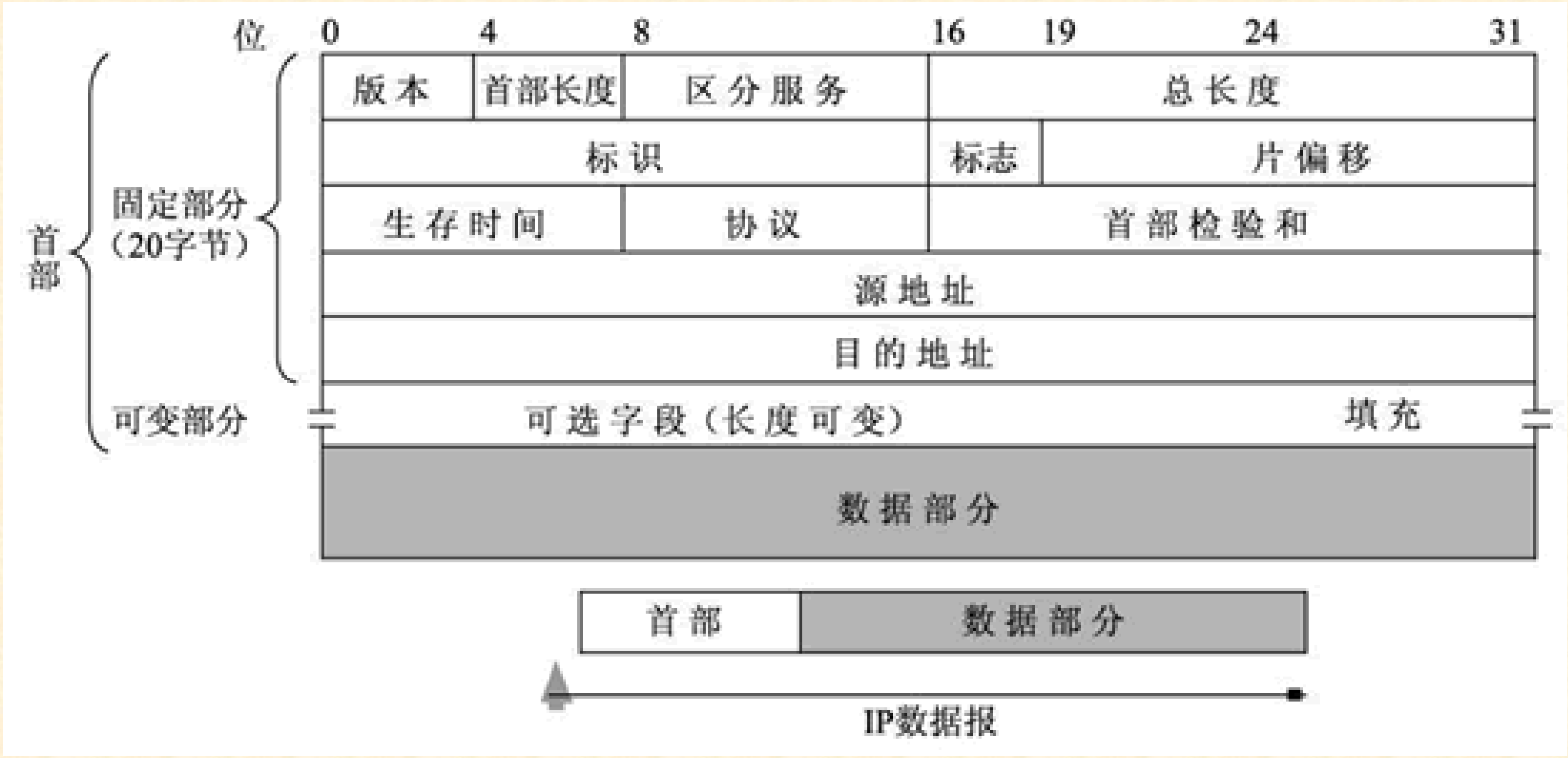
# OSI 模型与防火墙类型的关系（续）

## IP 头部数据段



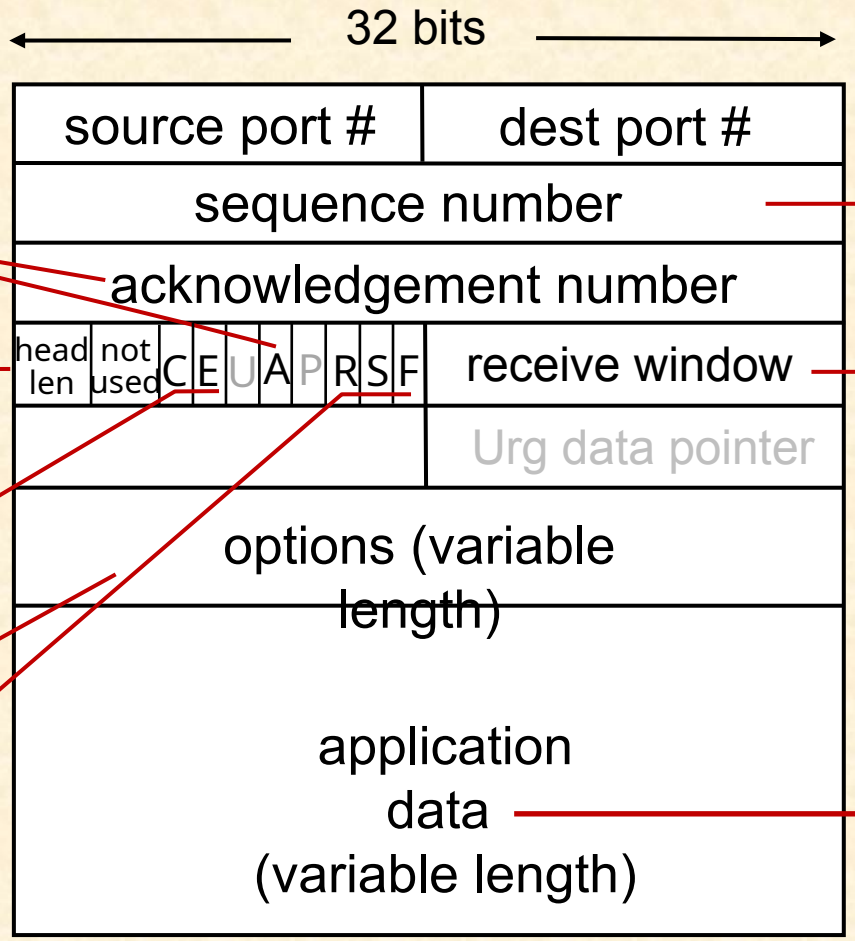

**overhead**

- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead


位
0
4
8
16
19
24
31
版本
首部长度
区分服务
总长度
标识
标志
片偏移
生存时间
协议
首部检验和
源地址
目的地址
可选字段（长度可变）
填充
数据部分
首部
固定部分
（20字节）
可变部分
数据部分
IP数据报

# OSI 模型与防火墙类型的关系（续）

- TCP 头部数据段




ACK: seq # of next expected byte; A bit: this is an ACK

length (of TCP header)

C, E: 拥塞通知

TCP options

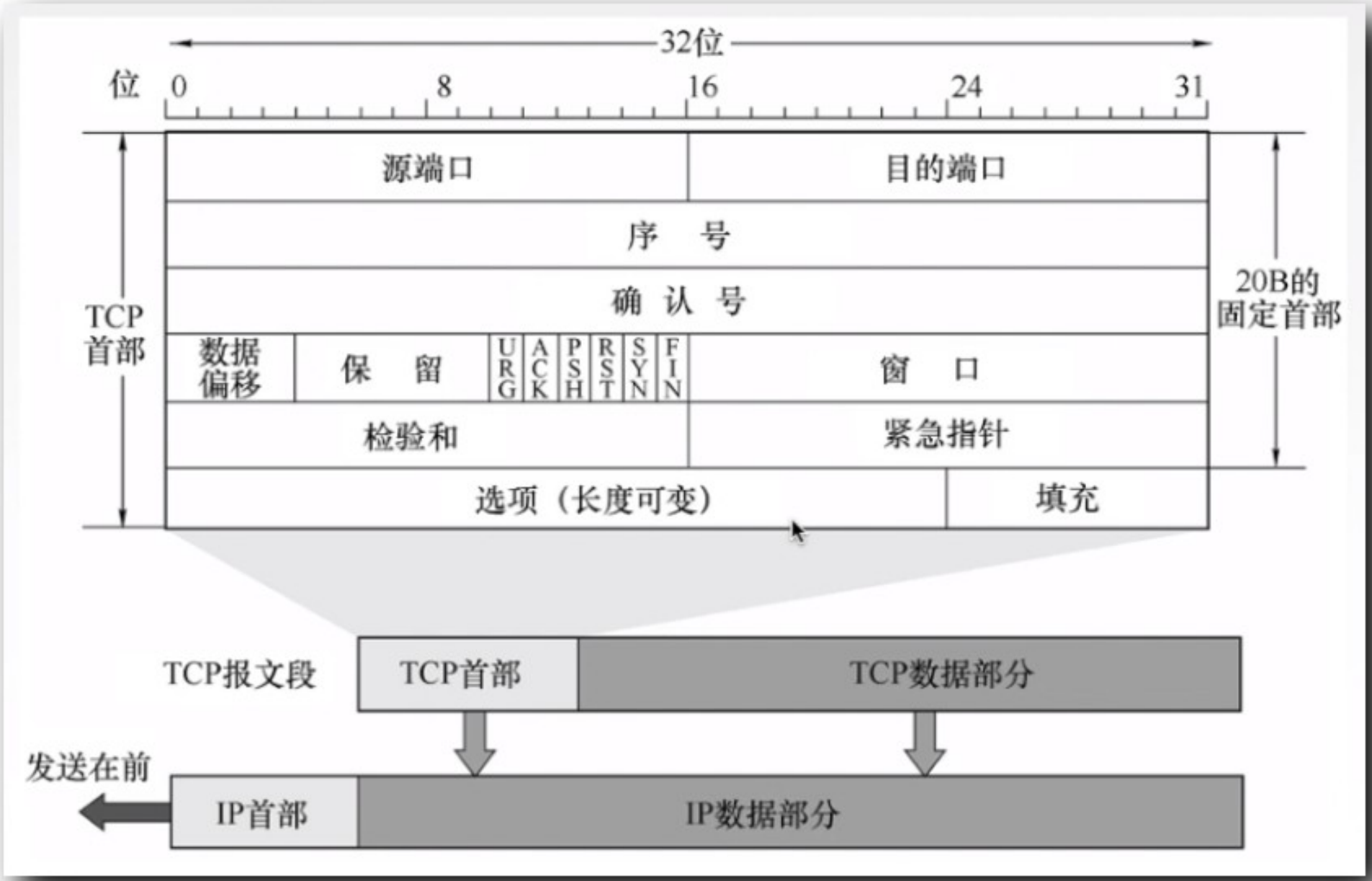
RST, SYN, FIN: connection management

报文段序号 #: counting bytes of data into bytestream (not segments!)

流控制 # bytes receiver willing to accept

data sent by application into TCP socket

**防火墙通常建立在 TCP/IP 模型基础上， OSI 模型与 TCP/IP 模型之间并不存在一一对应的关系。**



# 本讲内容概要

1 防火墙概述

2 防火墙的类型和结构

3 静态包过滤器（分组过滤）

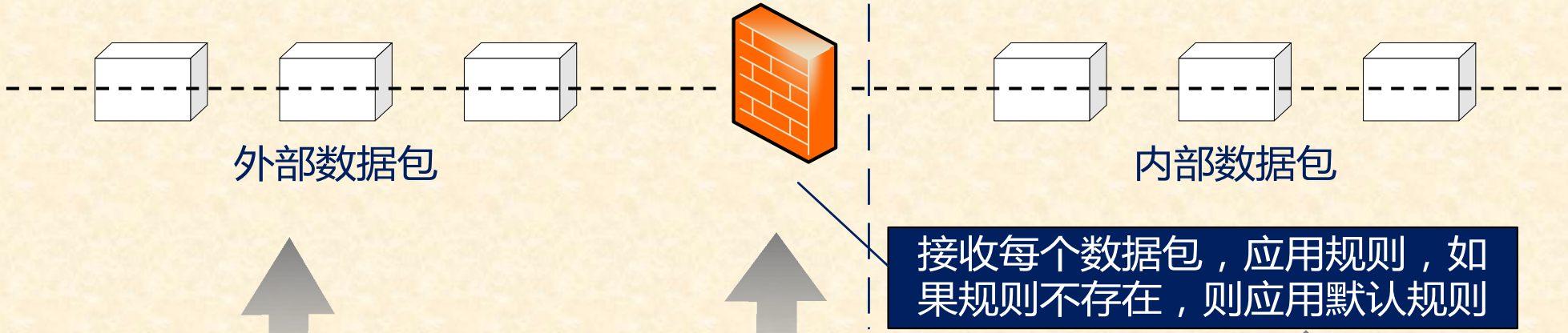
4 动态包过滤防火墙

5 电路级网关

6 应用级网关

# 静态包过滤防火墙（分组过滤）

# 静态包过滤防火墙的操作（分组过滤）




防火墙接收到从外部网络到达防火墙的数据包，对数据包过滤。

对数据包施加过滤规则，对数据包 IP 头和传输字段内容进行检查。

如果没有规则与数据包头信息匹配，则对数据包施加默认规则。

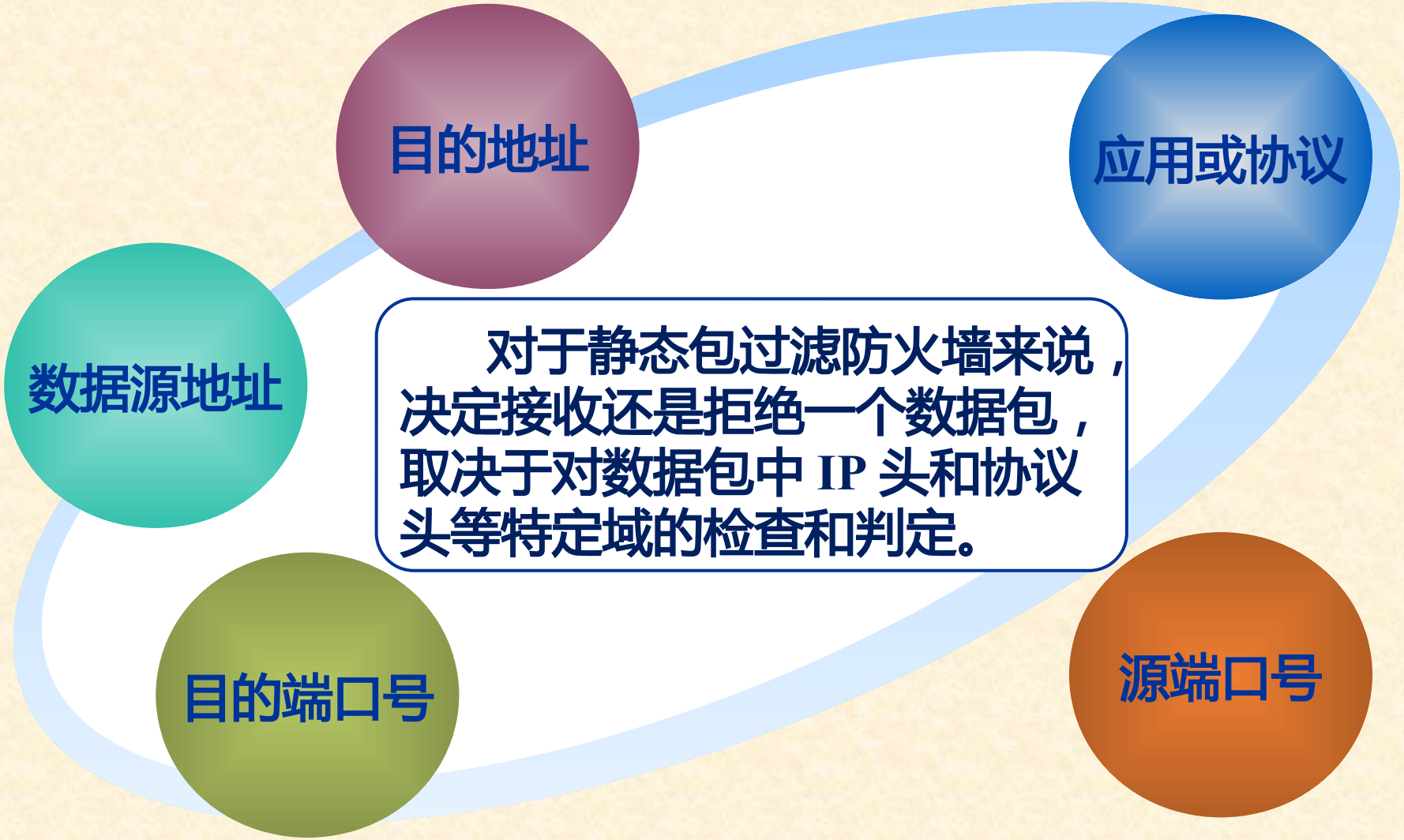
# 过滤规则

规则由一组属性值和操作组成，如果某个 IP 分组携带的信息和构成规则的一组属性值匹配，意味着该 IP 分组和该规则匹配，对该 IP 分组实施规则指定的操作。

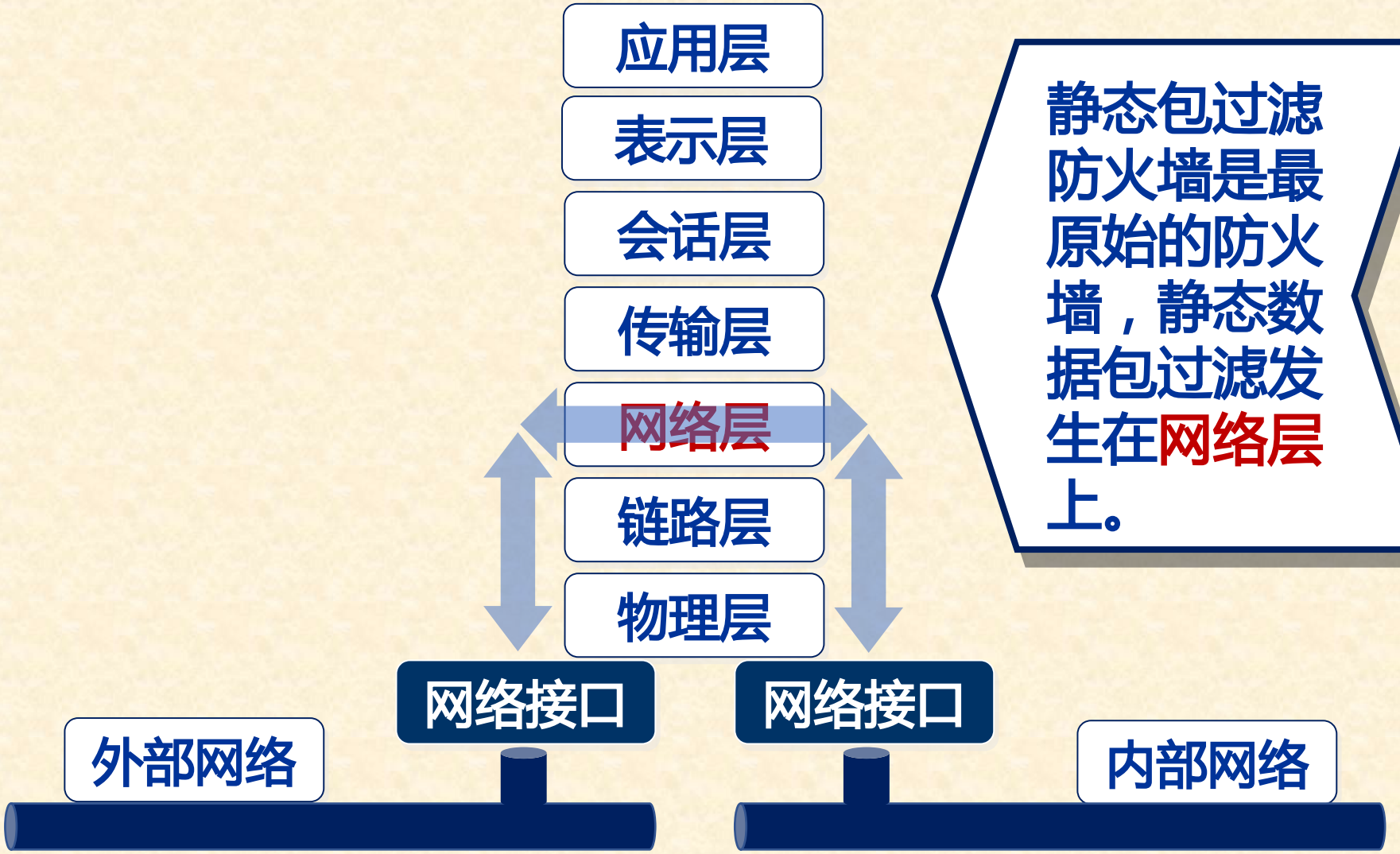
构成规则的属性值通常由下述字段组成：

- 源 IP 地址，用于匹配 IP 分组 IP 首部中的源 IP 地址字段值。
- 目的 IP 地址，用于匹配 IP 分组 IP 首部中的目的 IP 地址字段值。
- 源和目的端口号，用于匹配作为 IP 分组净荷的传输层报文首部中源和目的端口号字段值。
- 协议类型，用于匹配 IP 分组首部中的协议字段值。

# 工作于网络层的静态包过滤（续）（分组过滤）

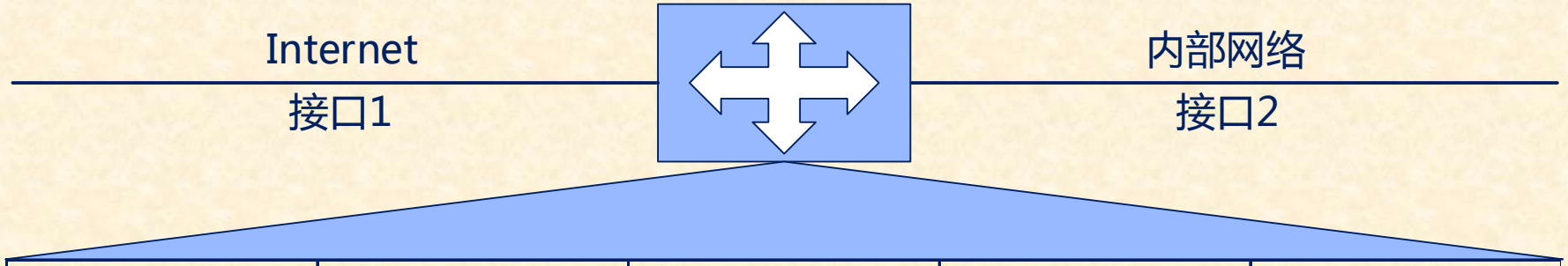


# 工作于网络层的静态包过滤（分组过滤）




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。

# 静态包过滤防火墙实例（分组过滤）




| Interface | Source IP | Source port | Destination IP | Destination port |
|---|---|---|---|---|
| 1 | 130.33.0.0 | * | * | * |
| 1 | * | * | * | 23 |
| 1 | * | * | 193.77.21.9 | * |
| 2 | * | * | * | 80 |

- 拒绝来自 130.33.0.0 的数据包，这是一种保守策略。
- 拒绝来自外部网络的 Telnet 服务（端口号为 23 ）的数据包。
- 拒绝试图访问内网主机 193.77.21.9 的数据包。
- 禁止 HTTP 服务（端口号为 80 ）的数据包通过防火墙。

# 包过滤器的工作原理（分组过滤）

**过滤规则**

防火墙可根据数据包的

- 源地址
- 目的地址
- 端口号

确定是否允许和丢弃数据包：符合，则允许；不符合，丢弃。

**过滤位置**

- 可以在网络入口处过滤
- 也可在网络出口处过滤
- 入口和出口同时对数据包进行过滤

**访问控制策略**

- 网管需预先编写一访问控制列表
- 需明确规定哪些主机或服务可接受，哪些主机或服务不接受

# 过滤规则系列

一个过滤器可以由多个规则构成，IP 分组只有和当前规则不匹配时，才继续和后续规则进行匹配操作，如果和过滤器中的所有规则都不匹配，对 IP 分组进行默认操作。一旦和某个规则匹配，则对其进行规则指定的操作，不再和其他规则进行匹配操作。

# 过滤规则集形式

## 两种过滤规则集设置方法

（1）黑名单

黑名单方法是列出所有禁止传输的IP分组类型，没有明确禁止的IP分组类型都是允许传输的。

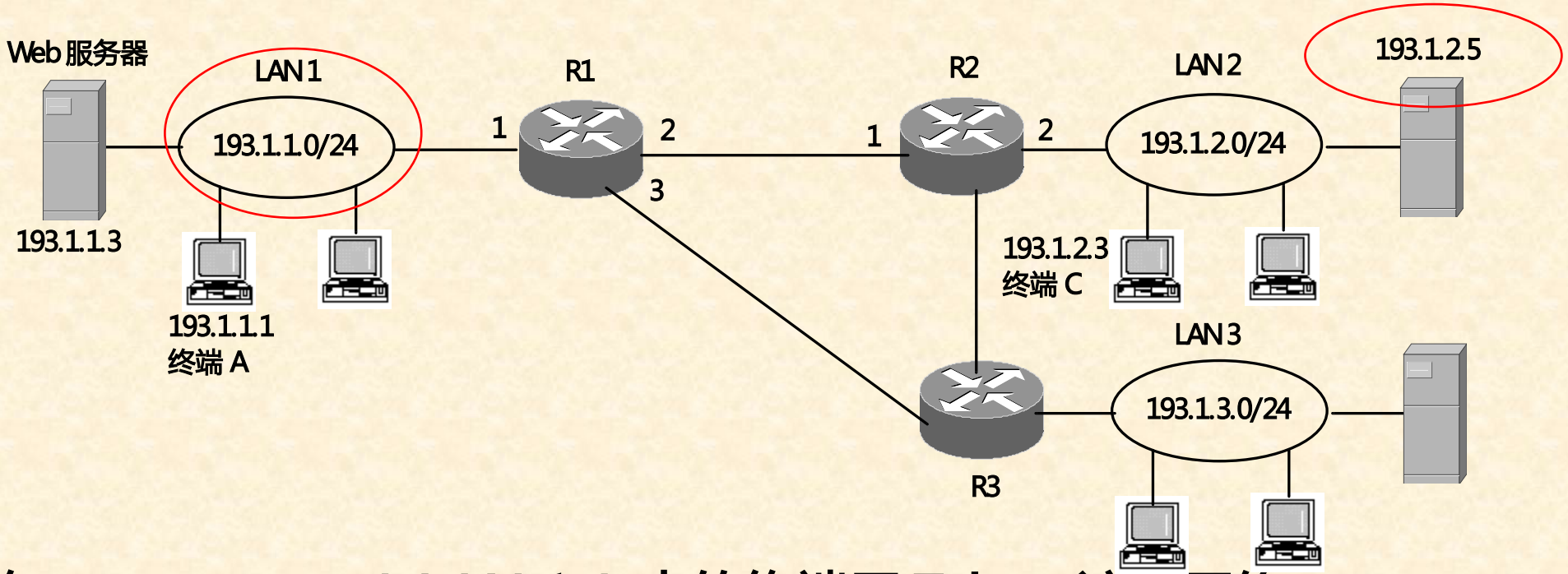
（2）白名单

白名单方法与黑名单方法相反，列出所有允许传输的IP分组类型，没有明确允许传输的IP分组类型都是禁止传输的。

# 分组过滤器

- 无状态是指实施筛选和控制操作时，每一个 IP 分组都是独立的，不考虑 IP 分组之间的关联性。
- 有状态是指将属于同一连接的所有包作为一个整体的数据流看待，对接收到的数据包进行分析，判断其是否属于当前合法连接，从而进行动态地过滤

# 无状态分组过滤器（实例1）




禁止网络 193.1.1.0/24（ LAN 1 ）中的终端用 Telnet 访问网络 193.1.2.0/24（ LAN 2 ）中 IP 地址为 193.1.2.5 的服务器。

路由器 R1 接口 1 输入方向上的分组过滤器的规则是：

- 协议类型 =TCP ；
- 源 IP 地址 =193.1.1.0/24 ；
- 目的 IP 地址 =193.1.2.5/32 ；
- 目的端口号 =23 ；
- 对和规则匹配的 IP 分组采取的动作是：丢弃。

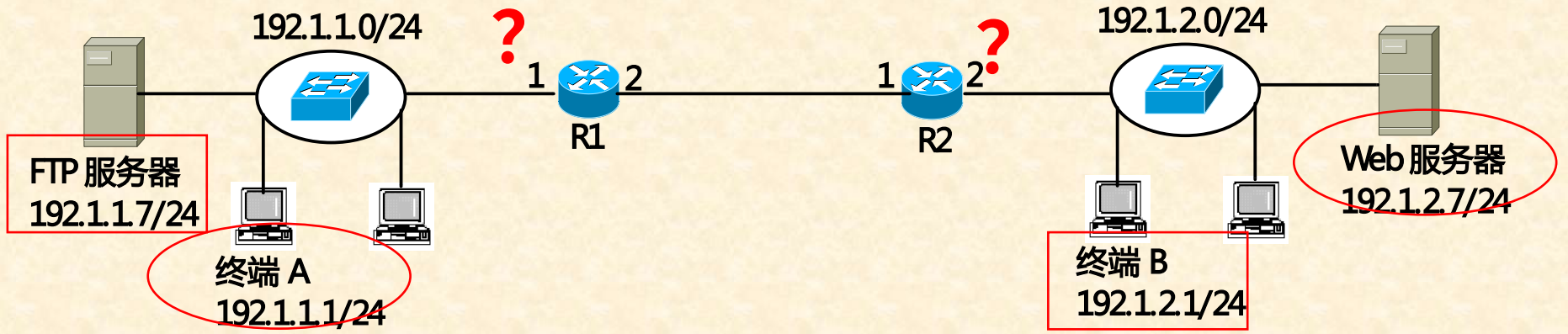
# 无状态分组过滤器（实例 1 ）

如果只是需要过滤掉所有与 LAN 1 中的终端用 Telnet 访问 LAN 2 中的服务器的操作相关的 IP 分组，允许其他 IP 分组继续传输，则完整的过滤器如下：

协议类型 =TCP ，源 IP 地址 =193.1.1.0/24 ，目的 IP 地址 =193.1.2.5/32 ，目的端口号 =23 ；丢弃。

协议类型 =* ，源 IP 地址 =any ，目的 IP 地址 =any ；正常转发。

# 无状态分组过滤器（实例 2 ）




写出作用于路由器 R1 接口 1 输入方向，路由器 R2 接口 2 输入方向，实现只允许终端 A 访问 Web 服务器，终端 B 访问 FTP 服务器，禁止其他一切网络间通信过程的安全策略的过滤规则集。

# 无状态分组过滤器（实例 2 ）

**路由器 R1 接口 1 输入方向的过滤规则集**如下。

① 协议类型 = TCP ，源 IP 地址 = 192.1.1.1/32 ，源端口号 = * ，目的 IP 地址 = 192.1.2.7/32 ，目的端口号 = 80 ；正常转发。

② 协议类型 = TCP ，源 IP 地址 = 192.1.1.7/32 ，源端口号 = 21 ，目的 IP 地址 = 192.1.2.1/32 ，目的端口号 = * ；正常转发。

③ 协议类型 = TCP ，源 IP 地址 = 192.1.1.7/32 ，源端口号 = 20 ，目的 IP 地址 = 192.1.2.1/32 ，目的端口号 = * ；正常转发。

④ 协议类型 = * ，源 IP 地址 = any ，目的 IP 地址 = any ；丢弃。

# 无状态分组过滤器（实例 2 ）

**路由器 R2 接口 2 输入方向的过滤规则集**如下。

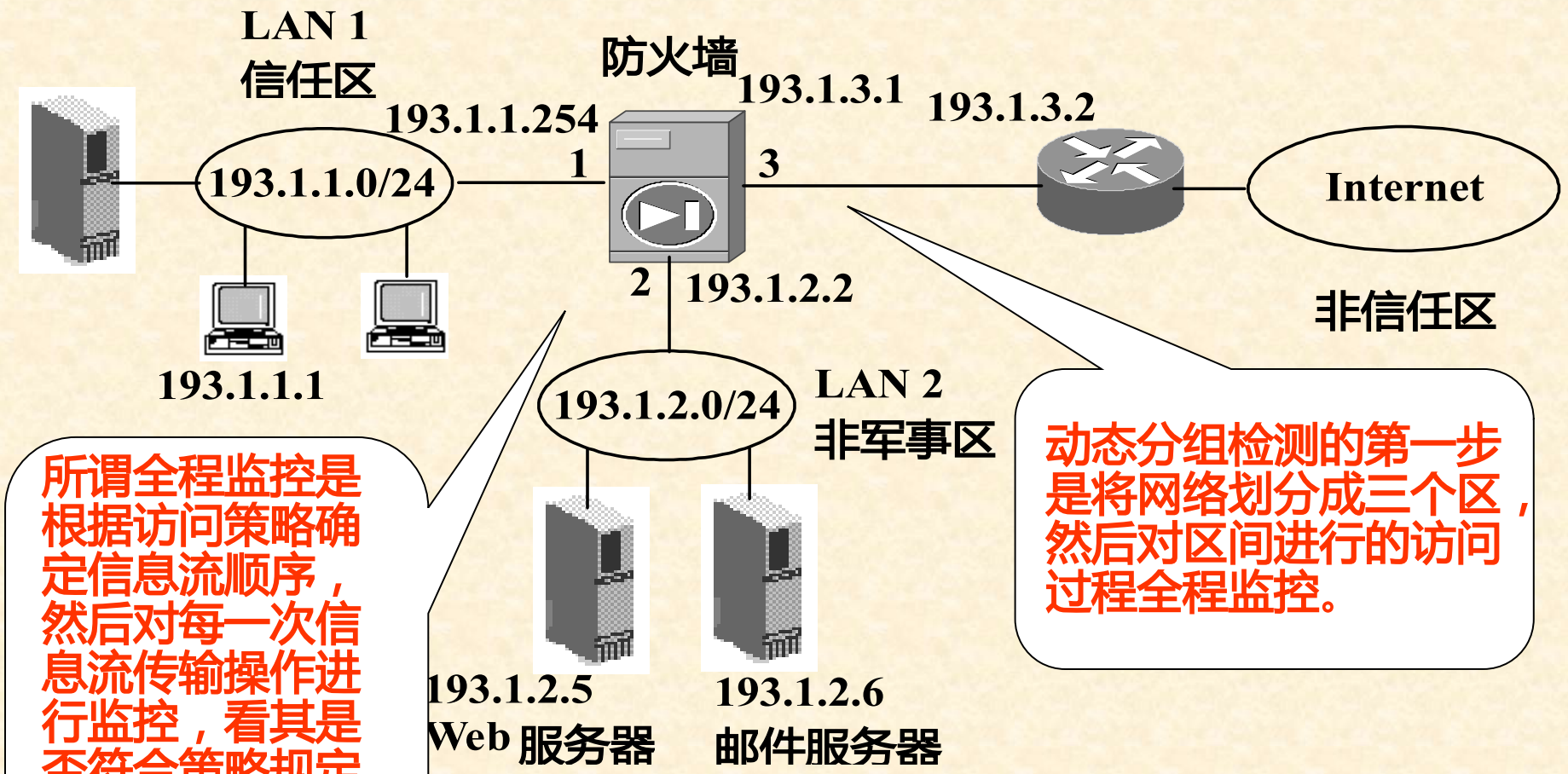
① 协议类型 = TCP ，源 IP 地址 = 192.1.2.1/32 ，源端口号 = * ，目的 IP 地址 = 192.1.1.7/32 ，目的端口号 = 21 ；正常转发。

② 协议类型 = TCP ，源 IP 地址 = 192.1.2.1/32 ，源端口号 = * ，目的 IP 地址 = 192.1.1.7/32 ，目的端口号 = 20 ；正常转发。

③ 协议类型 = TCP ，源 IP 地址 = 192.1.2.7/32 ，源端口号 = 80 ，目的 IP 地址 = 192.1.1.1/32 ，目的端口号 = * ；正常转发。

④ 协议类型 = * ，源 IP 地址 = any ，目的 IP 地址 = any ；丢弃。

# 基于分区防火墙


LAN 1
信任区
防火墙
193.1.3.1
193.1.3.2
193.1.1.254
193.1.1.0/24
1
3
Internet
2
193.1.2.2
非信任区
193.1.1.1
193.1.2.0/24
LAN 2
非军事区
所谓全程监控是根据访问策略确定信息流顺序，然后对每一次信息流传输操作进行监控，看其是否符合策略规定的顺序和动作。
动态分组检测的第一步是将网络划分成三个区，然后对区间进行的访问过程全程监控。
193.1.2.5
Web 服务器
193.1.2.6
邮件服务器

# 基于分区防火墙

访问策略

1．从信任区到非军事区　源 IP 地址 =193.1.1.0/24　目的 IP 地址 =193.1.2.5/32　HTTP 服务；

2．从信任区到非军事区　源 IP 地址 =193.1.1.0/24　目的 IP 地址 =193.1.2.6　SMTP+POP3 服务；

3．从信任区到非信任区　源 IP 地址 =193.1.1.0/24　目的 IP 地址 =0.0.0.0　HTTP+FTP　GET 服务；

4．从非军事区到非信任区　源 IP 地址 =193.1.2.6/32　目的 IP 地址 =0.0.0.0　SMTP 服务；

5．从非信任区到非军事区　源 IP 地址 =0.0.0.0　目的 IP 地址 =193.1.2.5/32　HTTP　GET 服务；

6．从非信任区到非军事区　源 IP 地址 =0.0.0.0　目的 IP 地址 =193.1.2.6/32　SMTP 服务。

# 基于分区防火墙

访问策略

1．从信任区到非军事区　源 IP 地址 =193.1.1.0/24　　目的 IP 地址 =193.1.2.5/32　FTP 服务；

2．从信任区到非军事区　源 IP 地址 =193.1.1.0/24　　目的 IP 地址 =193.1.2.6

3．从信任区　IP 地址 =0.0.0.0　HTTP+FTP　G

4．从非军　2　目的 IP 地址 =0.0.0.0

5．从非信　目的 IP 地址 =193.1.2.5/32　HTTP　GET 服务；

6．从非信任区到非军事区　源 IP 地址 =0.0.0.0　目的 IP 地址 =193.1.2.6/32　SMTP 服务。

访问策略和分组过滤不同，不是定义了允许或不允许传输的 IP 分组，而是定义了整个服务过程。如第一项策略表示允许进行由信任区中终端发起的，对非军事区中的 WEB 服务器的访问。它允许符合这个访问过程的 IP 分组在信任区和非军事区之间传输。

# 某大学的防火墙过滤规则设置

| 动　作 | 源 | 端　口 | 目　的 | 端　口 | 标　志 | 解 释 |
|---|---|---|---|---|---|---|
| allow | secondary | * | our-dns | 53 | TCP | allow secondary nameserver access |
| block | * | * | * | 53 | TCP | no other DNS zone transfers |
| allow | * | * | * | 53 | UDP | permit UDP DNS queries |
| allow | ntp.outside | 123 | ntp.inside | 123 | UDP | ntp time access |
| block | * | * | * | 69 | UDP | no access to our tftpd |
| block | * | * | * | 87 | TCP | the link service is often misused |
| block | * | * | * | 111 | TCP | no TCP RPC and ... |
| block | * | * | * | 111 | UDP | no UDP RPC and no ... |
| block | * | * | * | 2049 | UDP | NFS. This is hardly a guarantee |
| block | * | * | * | 2049 | TCP | TCP NFS is coming: exclude it |
| block | * | * | * | 512 | TCP | no incoming “r” commands... |
| block | * | * | * | 513 | TCP | ... |
| block | * | * | * | 515 | TCP | no external lpr |
| block | * | * | * | 540 | TCP | uucpd |
| block | * | * | * | 6000-6100 | TCP | no incoming X |
| allow | * | * | adminnet | 443 | TCP | encrypted access to transcript mgr |
| block | pclab-net | * | adminnet | * | TCP | nothing else |
| block | pclab-net | * | * | * | TCP | anon. students in pclab can’t go outside |
| block | * | * | * | * | UDP | ... not even with TFTP and the |
| allow | * | * | * | | TCP | |

以上规则设置部分来自美国计算机应急响应中心的建议书

# 某公司的防火墙过滤规则设置

| 动　作 | 源 | 端　口 | 目　的 | 端　口 | 标　志 | 解　释 |
|---|---|---|---|---|---|---|
| allow | * | * | mailgate | 25 | TCP | inbound mail access |
| allow | * | * | mailgate | 53 | UDP | access to our DNS |
| allow | secondary | * | mailgate | 53 | TCP | secondary nameserver access |
| block | * | * | mailgate | 23 | TCP | block incoming telnet access |
| allow | ntp.outside | 123 | ntp.inside | 123 | UDP | external time source |
| allow | inside-net | * | * | * | TCP | outgoing TCP packets are OK |
| allow | * | * | inside-net | * | ACK | return ACK packets are OK |
| block | * | * | * | * | TCP | nothing else is OK |
| Block | * | * | * | * | UDP | block other UDP, too |

以上规则设置部分来自美国计算机应急响应中心的建议书

# 静态包过滤防火墙优缺点

## 优点

- 对网络性能影响较小
- 成本较低

## 缺点

- 安全性较低
- 缺少状态感知能力
- 容易遭受 IP 欺骗攻击
- 创建访问控制规则比较困难

# 本讲内容概要

1 防火墙概述

2 防火墙的类型和结构

3 静态包过滤器

4 动态包过滤防火墙

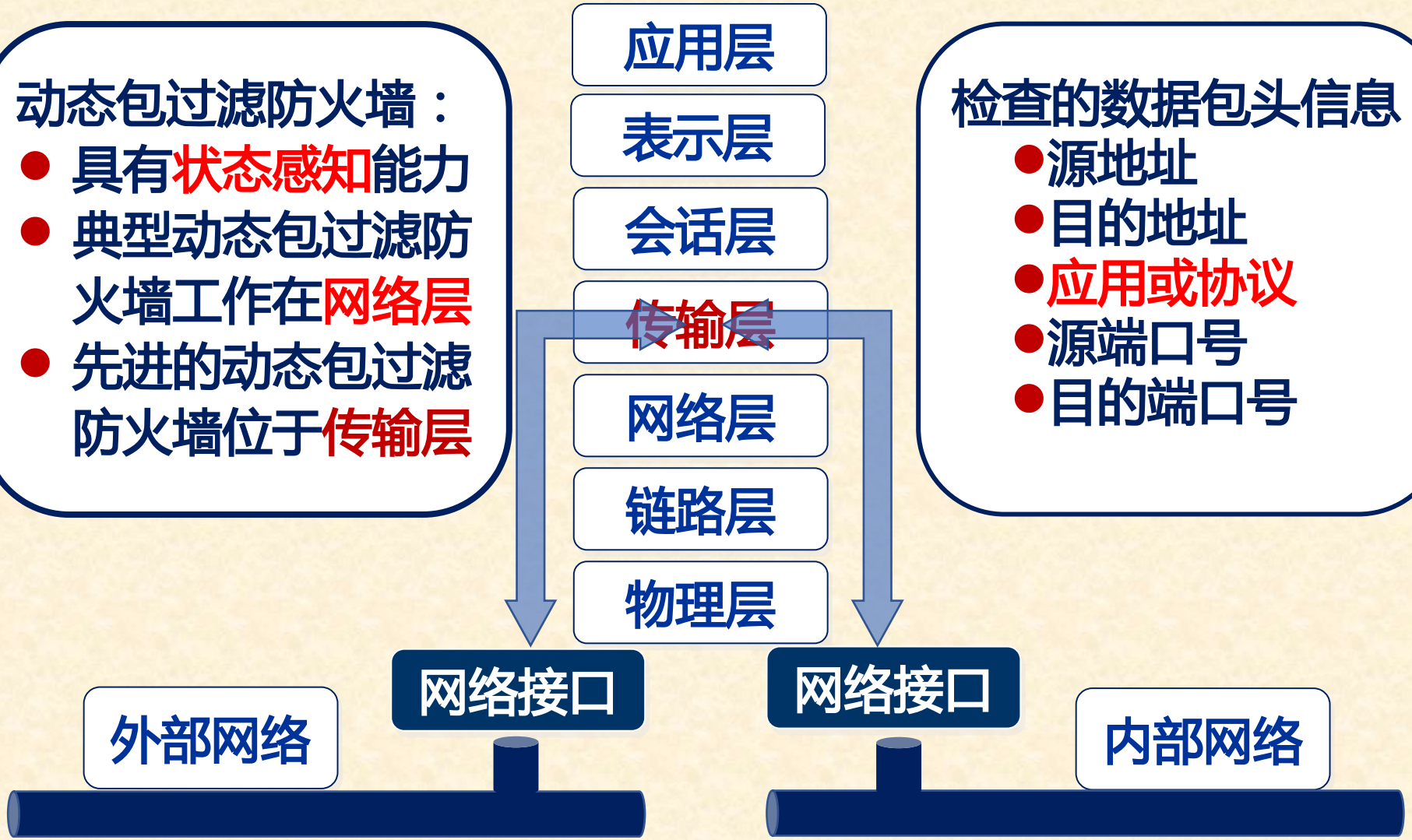
5 电路级网关

6 应用级网关

# 工作于传输层的动态包过滤防火墙

动态包过滤防火墙：

- 具有状态感知能力
- 典型动态包过滤防火墙工作在网络层
- 先进的动态包过滤防火墙位于传输层




检查的数据包头信息：

- 源地址
- 目的地址
- 应用或协议
- 源端口号
- 目的端口号

# 动态包过滤防火墙的工作原理

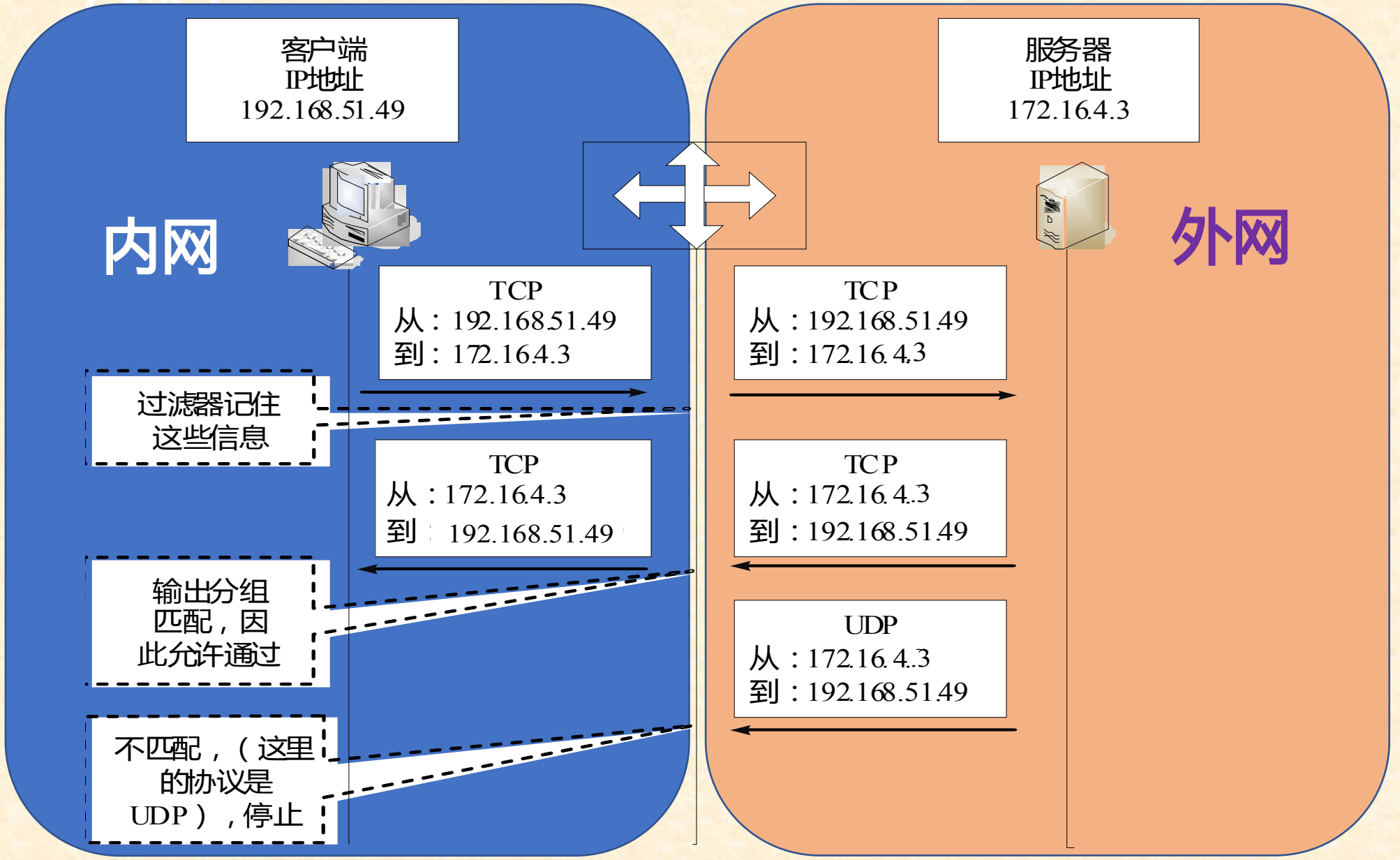
- 与普通包过滤防火墙相似，大部分工作于网络层。有些安全性高的动态包过滤防火墙，则工作于传输层。
- 动态包过滤防火墙的不同点：对外出数据包进行身份记录，便于下次让具有相同连接的数据包通过。
- 动态包过滤防火墙需要对已建连接和规则表进行动态维护，因此是动态的和有状态的。
- 典型的动态包过滤防火墙能够感觉到新建连接与已建连接之间的差别。

实现动态包过滤器有两种主要的方式：

1、实时地改变普通包过滤器的规则集

2、采用类似电路级网关的方式转发数据包

# 动态包过滤防火墙的工作原理（续）



# 动态包过滤防火墙的优缺点

| 优 点 | 缺 点 |
| --- | --- |
| 采用 SMP 技术时，对网络性能的影响非常小。 | 仅工作于网络层，仅检查 IP 头和 TCP 头。 |
| 动态包过滤防火墙的安全性优于静态包过滤防火墙。 | 没过滤数据包的净荷部分，仍具有较低的安全性。 |
| “状态感知”能力使其性能得到了显著提高。 | 容易遭受 IP 欺骗攻击。 |
| 如果不考虑操作系统成本，成本会很低。 | 难于创建规则，管理员创建时必须要考虑规则的先后次序。 |
| | 如果在建立连接时没有遵循三步握手协议，会引入风险。 |

# Linux 的 iptables 防火墙

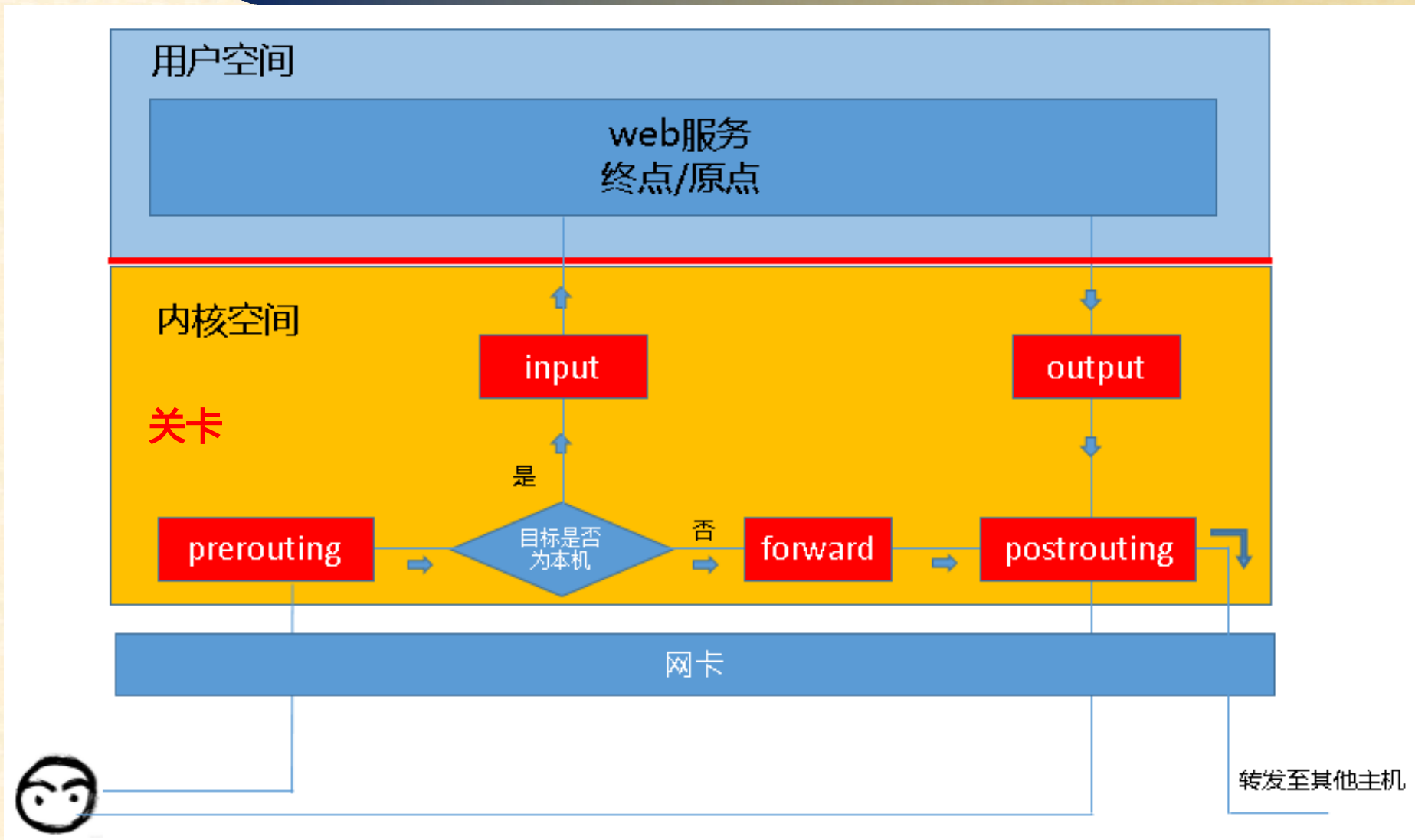
iptables 其实不是真正的防火墙，我们可以把它理解成一个客户端代理，用户通过 iptables 这个代理，将用户的安全设定执行到对应的 " 安全框架 " 中，这个 " 安全框架 " 才是真正的防火墙，这个框架的名字叫 netfilter 。

netfilter/iptables （下文中简称为 iptables ）组成 Linux 平台下的包过滤防火墙。

具有如下功能：

- 网络地址转换 (NAT)
- 数据包内容修改
- 以及数据包过滤的防火墙功能

# netfilter/iptables 原理




报文的流向：

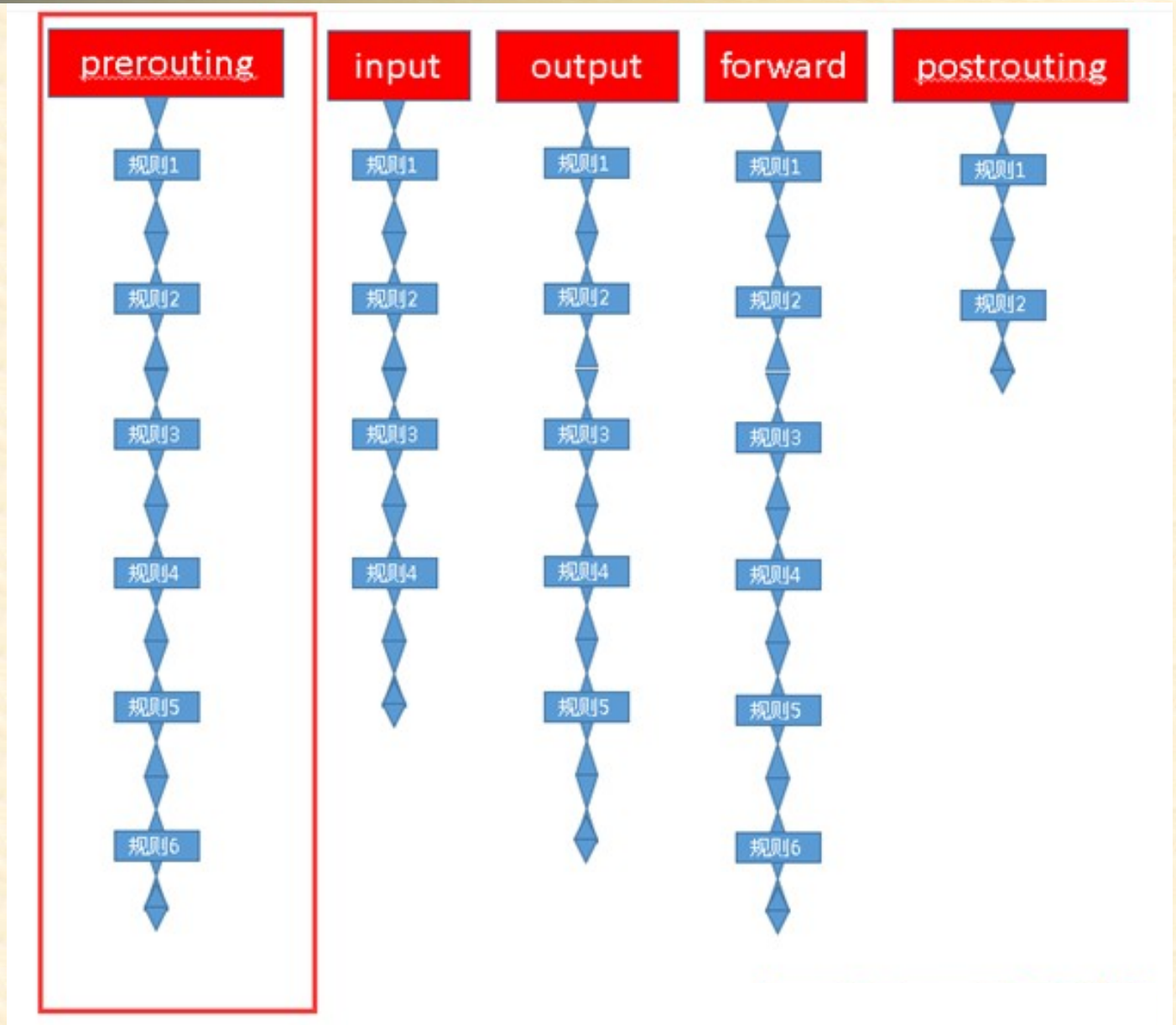
到本机某进程的报文：
PREROUTING -->
INPUT

由本机转发的报文：
PREROUTING -->
FORWARD -->
POSTROUTING

由本机的某进程发出报文（通常为响应报文）：OUTPUT -->
POSTROUTING

# netfilter/iptables 链式规则

防火墙的作用就在于对经过的报文匹配"规则"，然后执行对应的"动作",所以，当报文经过这些关卡的时候，则必须匹配这个关卡上的规则，但是，这个关卡上可能不止有一条规则，而是有很多条规则，当把这些规则串到一个链条上的时候，就形成了"链"。



# netfilter/iptables 规则表

对每个 " 链 " 上都放置了一串规则，但是这些规则有些很相似，比如， A 类规则都是对 IP 或者端口的过滤， B 类规则是修改报文，那么这个时候，可以把实现相同功能的规则放在一起，形成表。

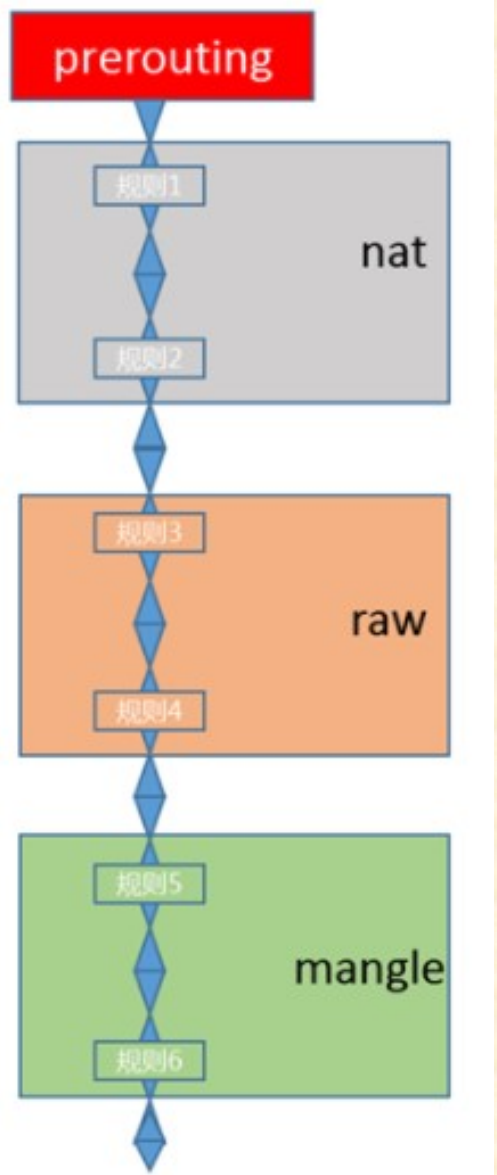
netfilter/iptables 定义了 4 种表

- filter 表：负责过滤功能，防火墙；内核模块： iptables_filter
- nat 表： network address translation ，网络地址转换功能；内核模块： iptable_nat
- mangle 表：拆解报文，做出修改，并重新封装 的功能； iptable_mangle
- raw 表：关闭 nat 表上启用的连接追踪机制； iptable_raw

# netfilter/iptables 表链关系

每个 " 链 " 中的规则都存在于哪些 " 表 " 中。

- PREROUTING 的规则可以存在于： raw 表， mangle 表， nat 表。
- INPUT 的规则可以存在于： mangle 表， filter 表，（ centos7 中还有 nat 表， centos6 中没有 ）。
- FORWARD 的规则可以存在于： mangle 表， filter 表。
- OUTPUT 的规则可以存在于： raw 表， mangle 表， nat 表， filter 表。
- POSTROUTING 的规则可以存在于： mangle 表， nat 表。



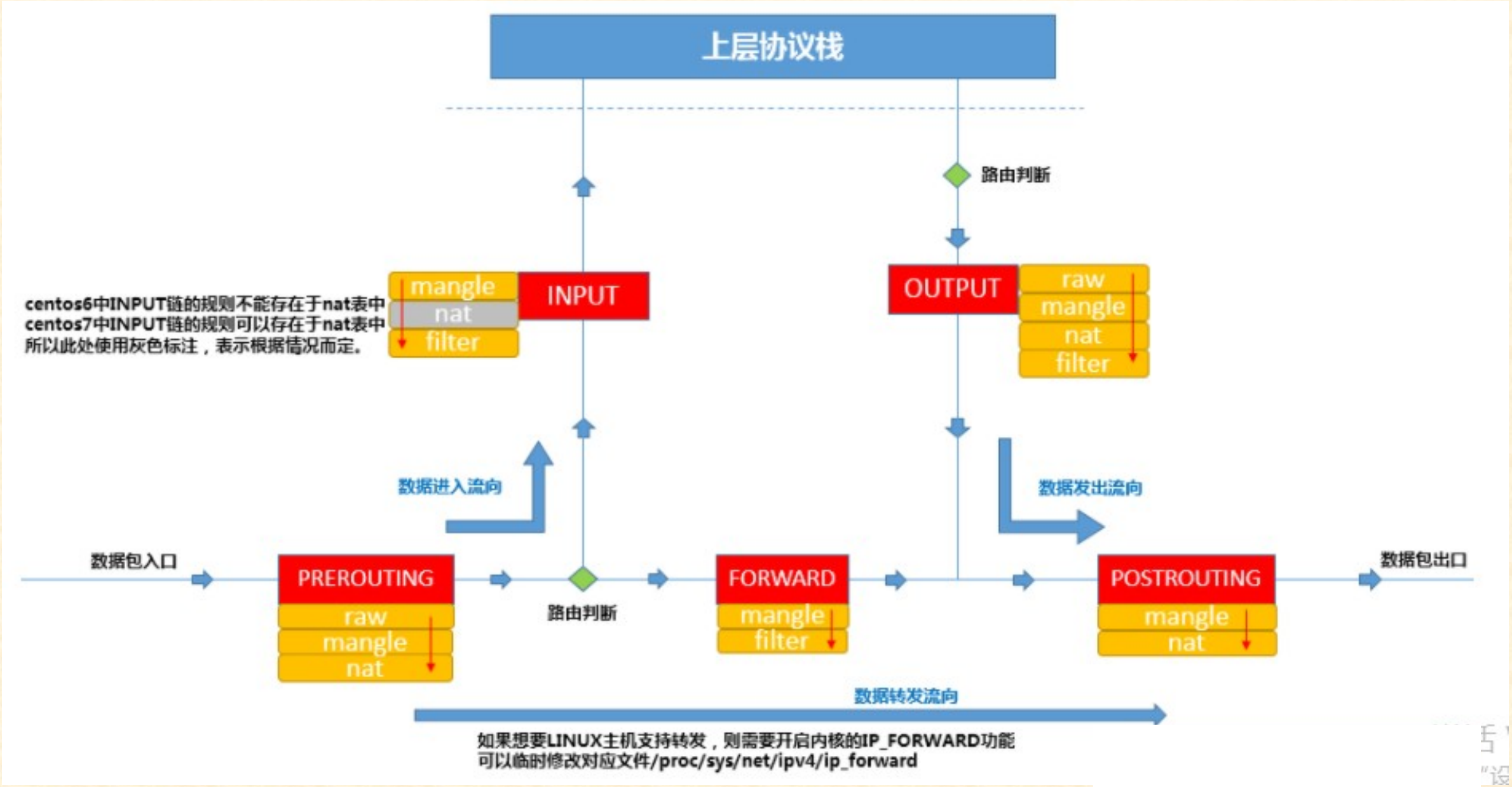
# netfilter/iptables 表链关系

在实际的使用过程中，往往是通过 " 表 " 作为操作入口，对规则进行定义的。

表（功能）<--> 链：

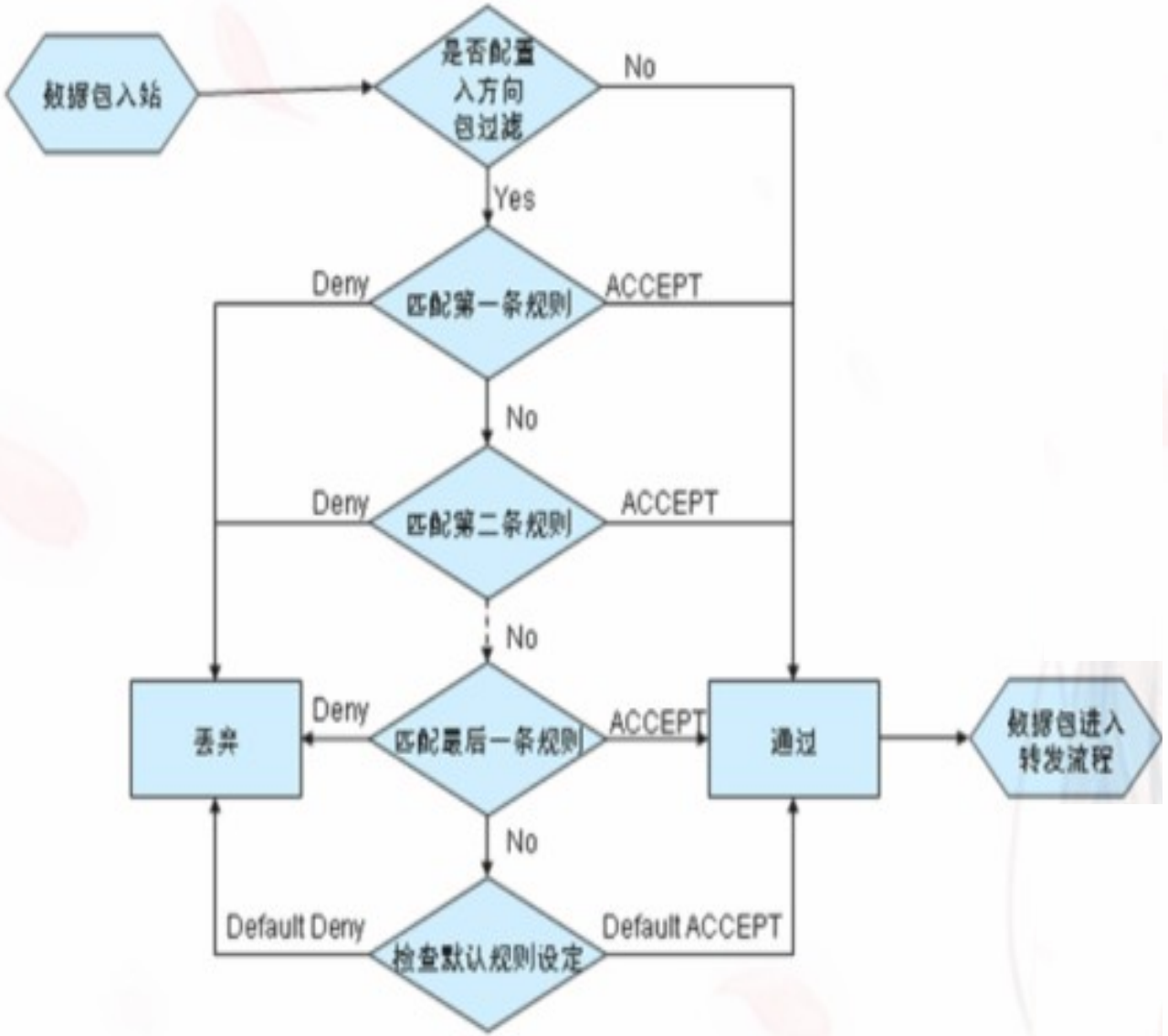
- raw 表中的规则可以被哪些链使用：PREROUTING ， OUTPUT
- mangle 表中的规则可以被哪些链使用：PREROUTING ， INPUT ， FORWARD ， OUTPUT ， POSTROUTING
- nat 表中的规则可以被哪些链使用：PREROUTING ， OUTPUT ， POSTROUTING（ centos7 中还有 INPUT ， centos6 中没有）
- filter 表中的规则可以被哪些链使用：INPUT ， FORWARD ， OUTPUT

# netfilter 工作流程

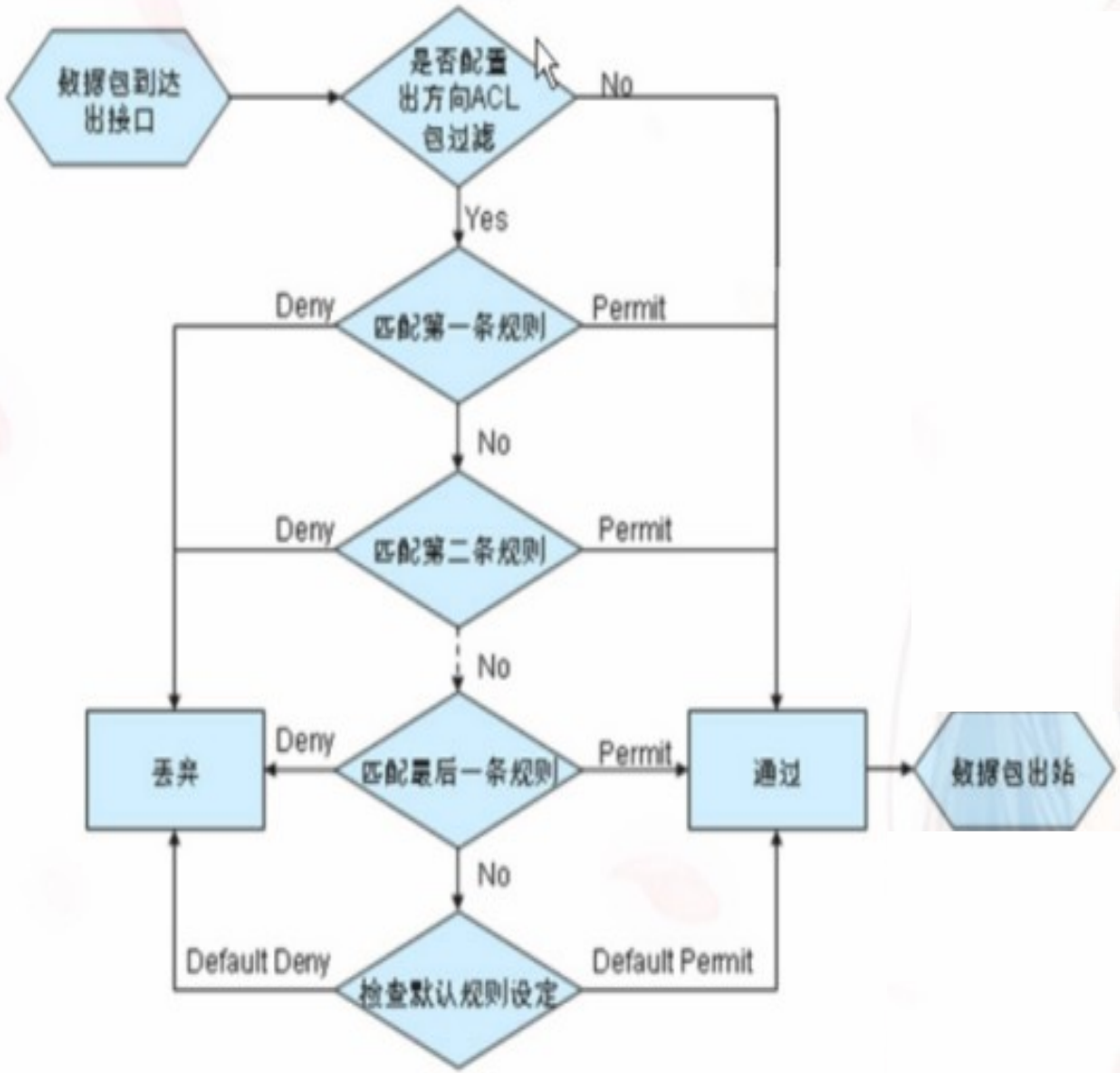


# netfilter 规则判断流程

## 入站数据包




## 出站数据包



# 本讲内容概要

1 防火墙概述

2 防火墙的类型和结构

3 静态包过滤器

4 动态包过滤防火墙

5 电路级网关

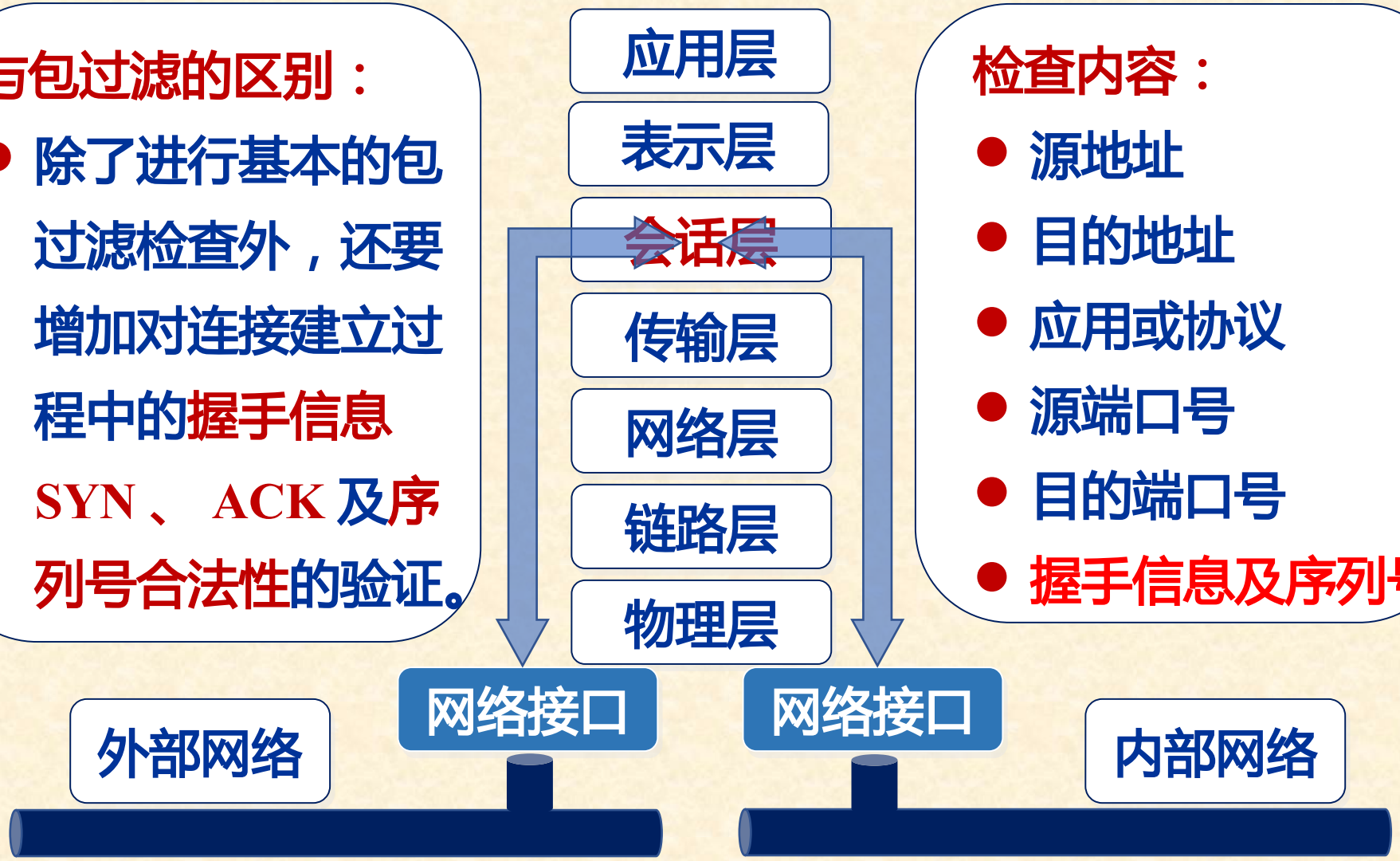
6 应用级网关

# 工作于会话层的电路级网关

主要功能是确保已建立的连接是安全的。

**与包过滤的区别：**

- 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。




**检查内容：**

- 源地址
- 目的地址
- 应用或协议
- 源端口号
- 目的端口号
- 握手信息及序列号

# 电路级网关

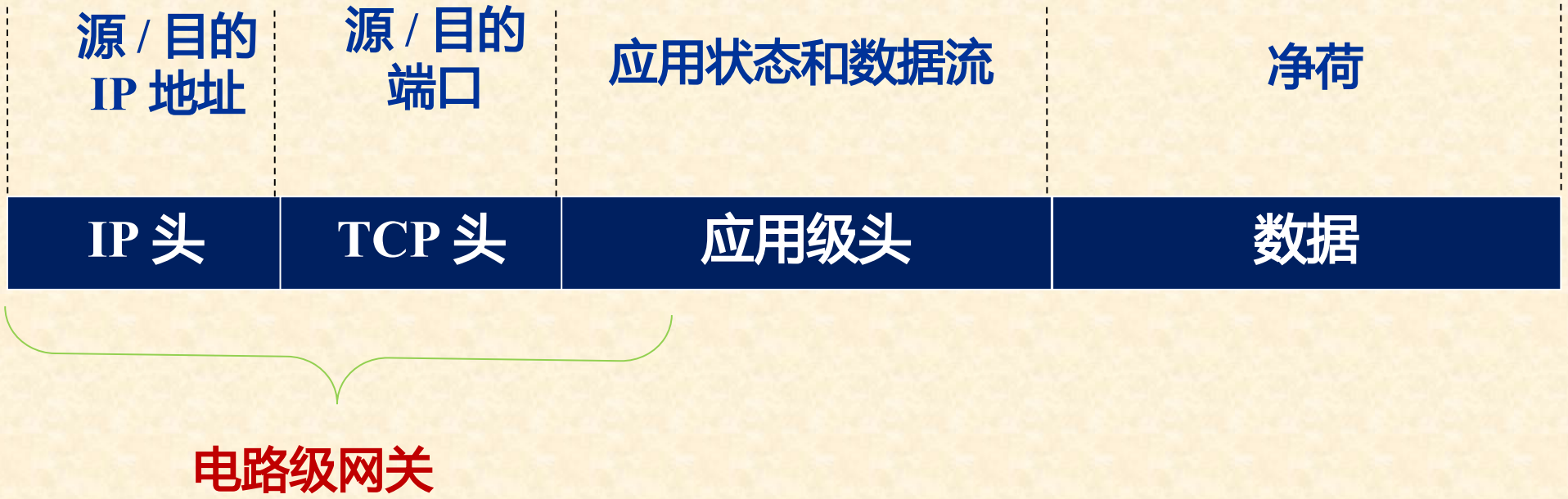
**电路级网关通常作为应用代理服务器的一部分，在应用代理类型的防火墙中实现。**

- 它的作用就像一台中继计算机，用于在两个连接之间来回地复制数据；
- 它也可以记录和缓存数据。

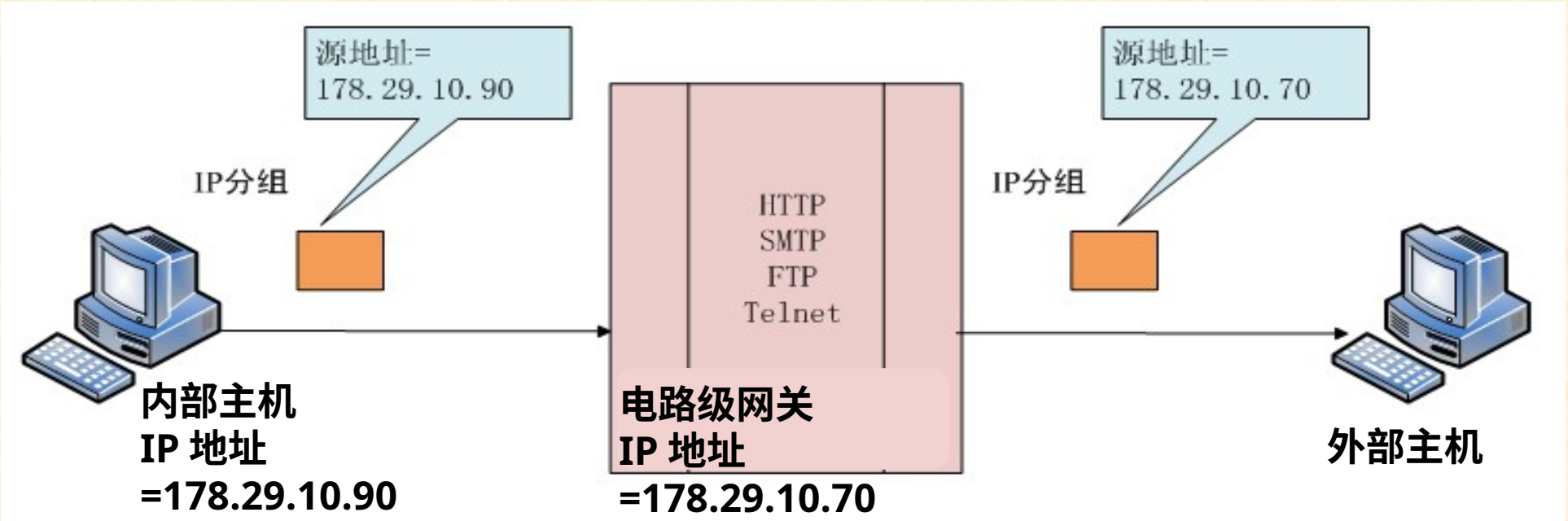
- 采用 C/S 结构，网关充当了服务器的角色；
- 作为代理服务器，在 Internet 和内部主机之间过滤和转发数据包。

- 它工作于会话层， IP 数据包不会实现端到端流动；
- 在有些实现方案中，电路连接可自动完成。

# 电路级网关所过滤的内容



# 电路级网关的工作原理




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。

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。

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。

# SOCKS 连接

- SOCKS 由 David 和 Michelle Koblas 设计并开发
- 是现在已得到广泛应用的电路级网关（ SSL ）
- 事实上， SOCKS 是一种网络代理协议

内网主机请求访问互联网

与 SOCKS 服务器建立通道

将请求发送给服务器

收到请求后向目标主机发出请求

响应后将数据返回内网主机

# 电路级网关优缺点

## 优点

- 性能比包过滤防火墙稍差，但是比应用代理防火墙好。
- 切断了外部网络到防火墙后的服务器直接连接。
- 比静态或动态包过滤防火墙具有更高的安全性。

## 缺点

- 具有一些固有缺陷。例如，电路级网关不能对数据净荷进行检测，无法抵御应用层攻击等。
- 仅提供一定程度的安全性。
- 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。

# 本讲内容概要

1 防火墙概述

2 防火墙的类型和结构

3 静态包过滤器

4 动态包过滤防火墙

5 电路级网关

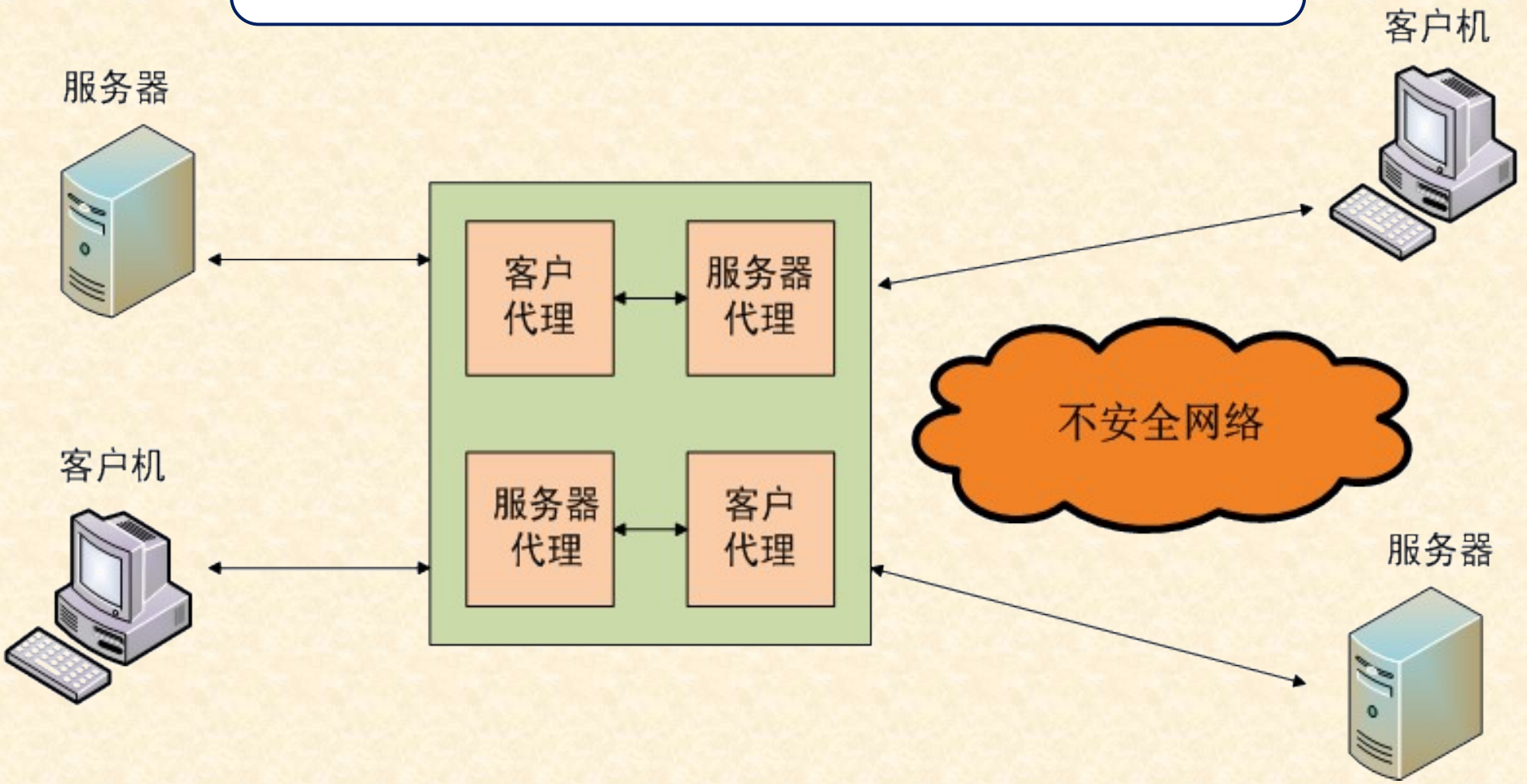
6 应用级网关

# 包过滤防火墙与应用级网关的区别

| 包过滤防火墙 | 应用级网关 |
| --- | --- |
| 过滤所有不同服务的数据流 | 只能过滤特定服务的数据流 |
| 不需要了解数据流的细节，它只查看数据包的源地址和目的地址或检查 UDP/TCP 的端口号和某些标志位。 | 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。 |

# 包过滤防火墙与应用级网关的区别

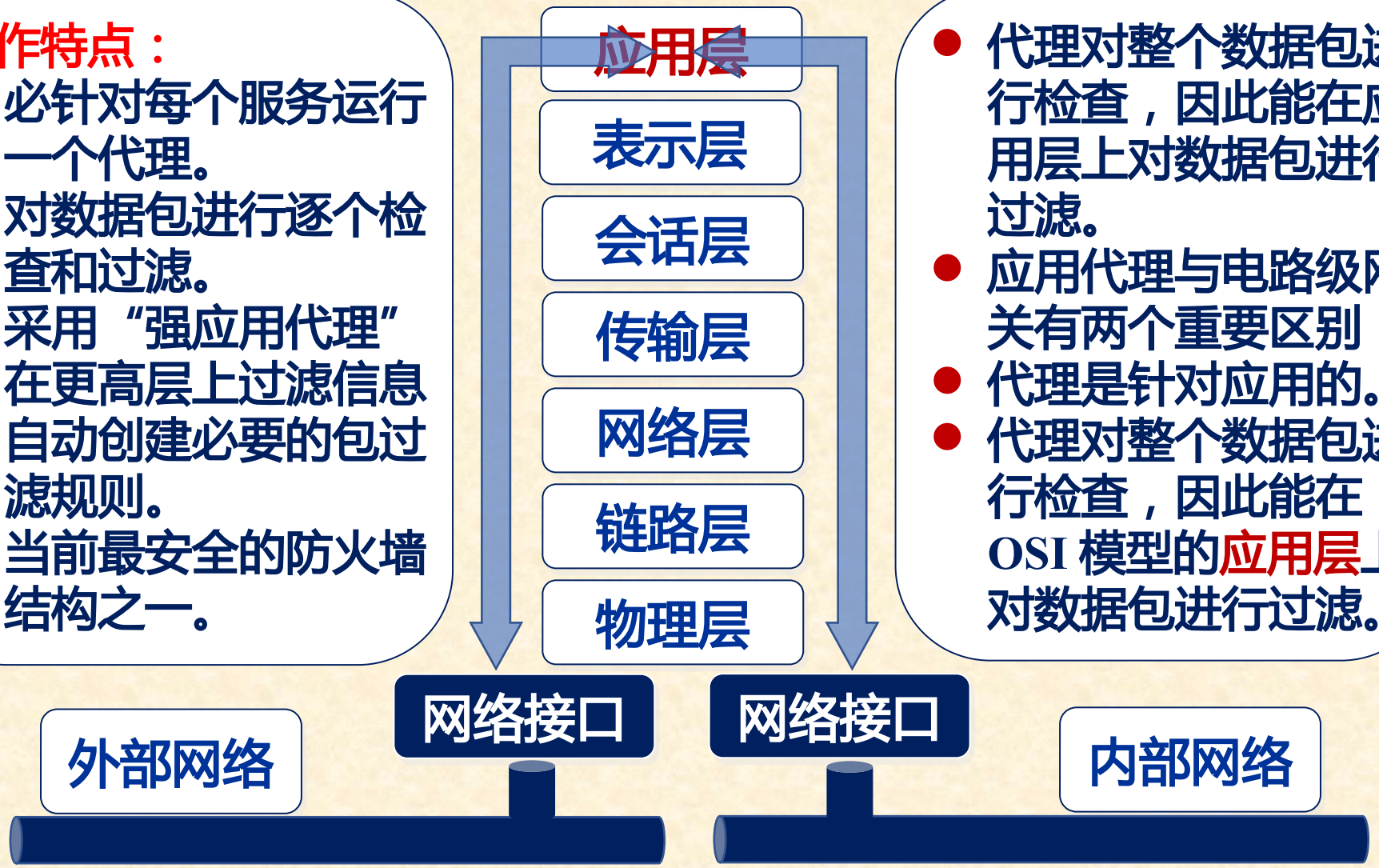
**当各种类型的应用服务通过网关时，必须经过客户机代理和服务器代理的过滤。**



# 应用级网关的工作层次

**工作特点：**

- 必针对每个服务运行一个代理。
- 对数据包进行逐个检查和过滤。
- 采用“强应用代理”
- 在更高层上过滤信息自动创建必要的包过滤规则。
- 当前最安全的防火墙结构之一。




- 代理对整个数据包进行检查，因此能在应用层上对数据包进行过滤。
- 应用代理与电路级网关有两个重要区别：
- 代理是针对应用的。
- 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。

# 应用层网关

## 1．WAF 的功能

WAF 是对 Web 服务器提供保护的应用层网关，用于防御黑客对 Web 服务器实施的攻击。由于与访问 Web 服务器相关的应用层协议是 HTTP 和 HTTPS，因此，WAF 主要检测 **HTTP 消息和 HTTPS 消息**。

# Web 应用防火墙（ WAF ）工作原理

**WAF 三种检测机制**

**（ 1 ）协议验证**

**WAF 通过检测经过的 HTTP 请求和响应消息中各个字段的值可以发现不规范的 HTTP 请求和响应消息，这些不规范的 HTTP 请求和响应消息中往往包含攻击信息。**

# Web 应用防火墙（ WAF ）工作原理

## WAF 三种检测机制

### （ 2 ）攻击特征

WAF 对每一个 HTTP 请求消息，根据攻击特征库中的每一个攻击行为，逐个检测相关字段，如果该 HTTP 请求消息的相关字段值中包含了某个攻击行为的特征信息，表明该 HTTP 请求消息是实施该攻击行为的 HTTP 请求消息。

# Web 应用防火墙（ WAF ）工作原理

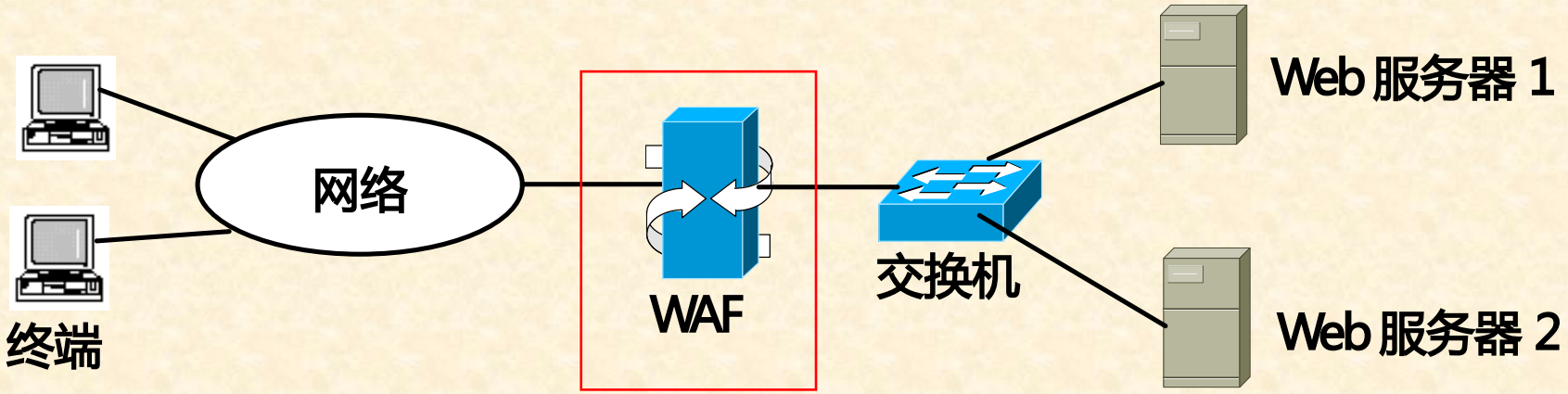
**WAF 三种检测机制**

**（ 3 ）应用规范**

**可以根据长期统计分析得出的规律来制定应用规范，当 Web 服务器访问方式与应用规范之间出现较大偏差时，表明 Web 服务器正在遭受攻击。**

**如：某个注册用户一般在什么时间段、用什么 IP 地址的终端登录 Web 服务器，每一个用户访问 Web 服务器过程， Web 服务器在不同时间段的登录用户数， Web 服务器主页中每一个链接的打开密度等。**

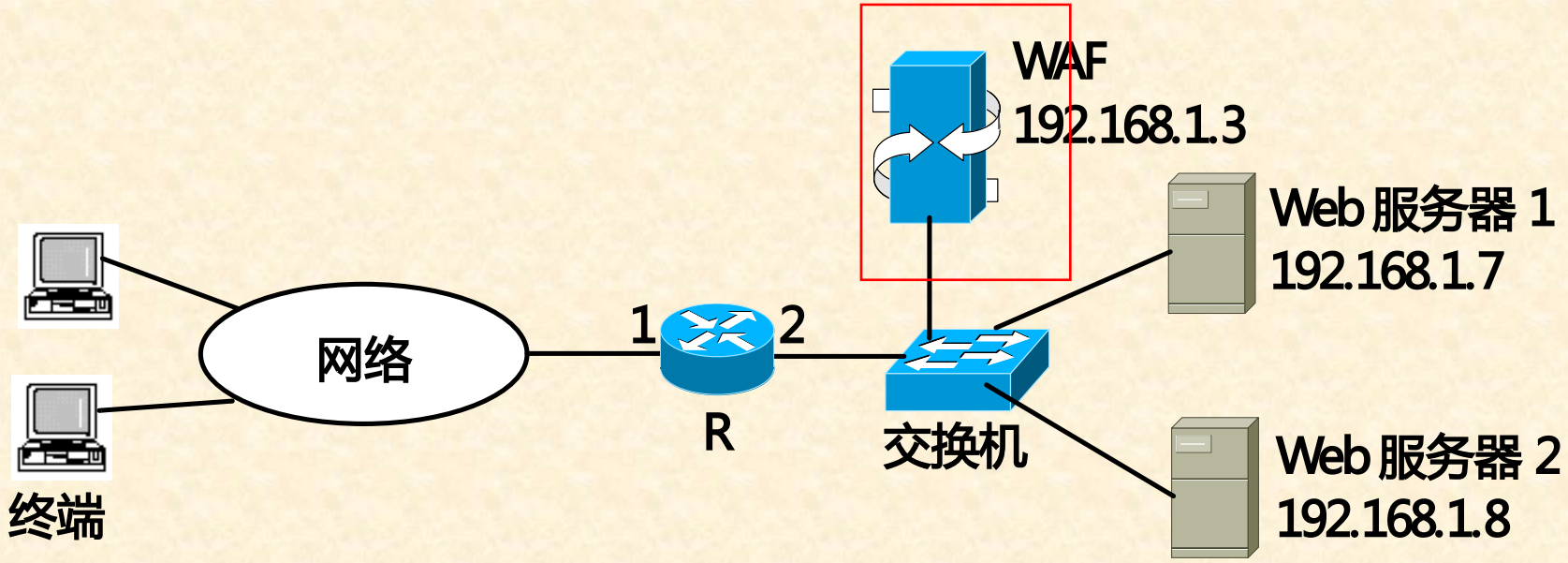
# Web 应用防火墙工作模式




1 ．透明模式

WAF 位于终端与 Web 服务器之间的传输路径上，终端与 Web 服务器之间交换的 HTTP 请求和响应消息全部经过 WAF ，由 WAF 对经过的 HTTP 请求和响应消息进行检测。

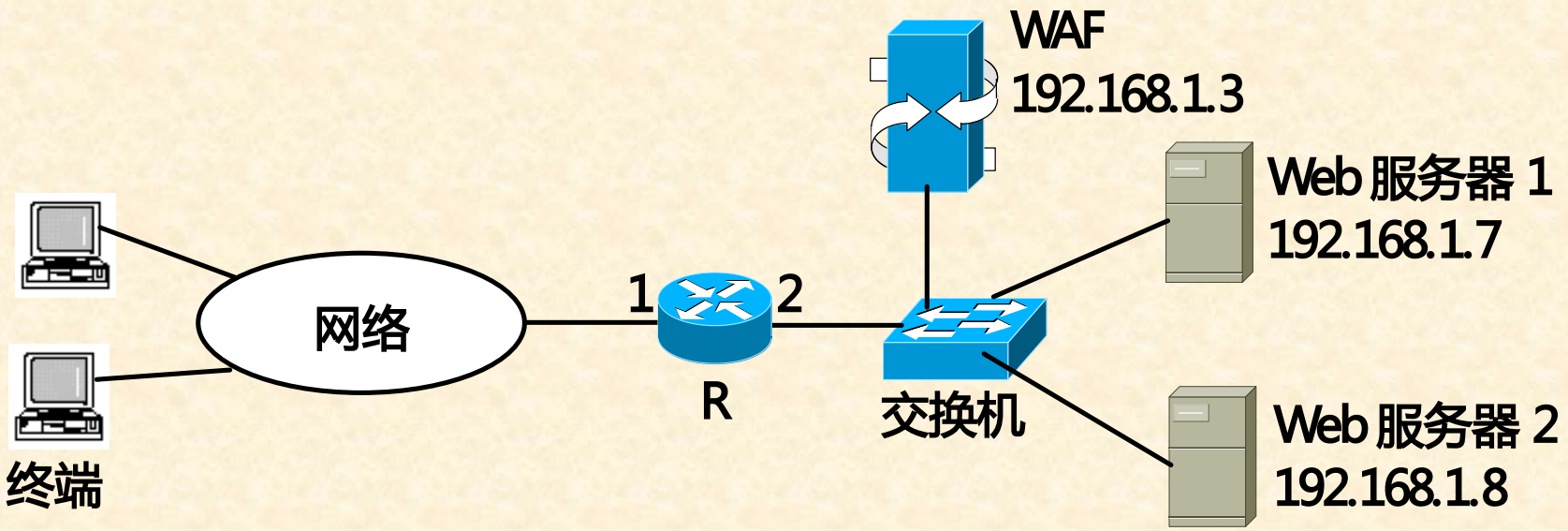
# Web 应用防火墙（WAF）工作模式




2．反向代理模式

WAF 并没有位于终端与 Web 服务器之间的传输路径上。为了强迫终端发送给 Web 服务器的 HTTP 请求消息经过 WAF ，在路由器 R 中添加两项静态路由项，这两项静态路由项使得路由器 R 将以 Web 服务器的 IP 地址为目的 IP 地址的 IP 分组转发给 WAF ，并因此使得所有终端发送的、以 Web 服务器的 IP 地址为目的 IP 地址的 IP 分组经过 WAF 。由 WAF 对经过的 HTTP 请求消息进行检测。 Web 服务器回送的 HTTP 响应消息可以不经过 WAF 。

# Web 应用防火墙（WAF）工作模式




| 目的网络 | 输出接口 | 下一跳 |
| --- | --- | --- |
| 192.168.1.7/32 | 2 | 192.168.1.3 |
| 192.168.1.8/32 | 2 | 192.168.1.3 |

# 应用级网关优缺点

**优 点**

- 在已有的安全模型中安全性较高。
- 具有强大的认证功能。
- 具有超强的日志功能。
- 规则配置比较简单。

**缺 点**

- 灵活性很差，对每一种应用都需要设置一个代理。
- 配置烦琐，增加了管理员的工作量。
- 性能不高，有可能成为网络的瓶颈。

# 本讲内容概要

7 状态检测防火墙

8 切换代理

9 空气隙防火墙

10 分布式防火墙

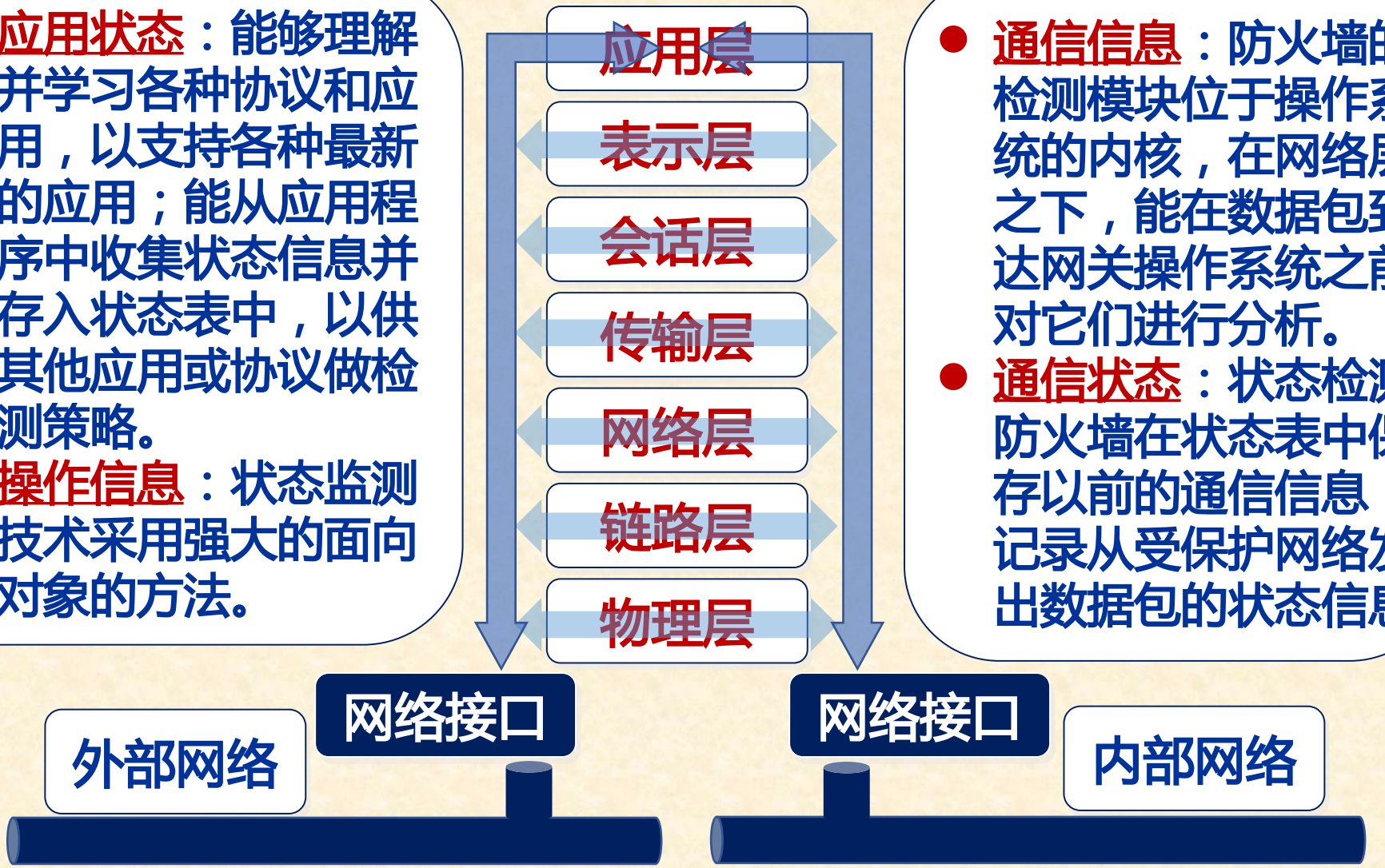
11 下一代防火墙

12 防火墙的典型产品

13 防火墙的发展趋势

# 状态检测防火墙在所有 7 层上进行过滤

- **应用状态**：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。
- **操作信息**：状态监测技术采用强大的面向对象的方法。




- **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。
- **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数据包的状态信息。

# 状态检测防火墙优缺点

**优点**

- 具备动态包过滤所有优点，同时具有更高的安全性。
- 它没有打破 C/S 结构，因此不需要修改很多应用程序。
- 提供集成的动态（状态）包过滤功能。
- 当以动态包过滤模式运行时，其速度很快。
- 当采用对称多处理器 SMP 模式时，其速度更快。

**缺点**

- 采用单线程进程，对防火墙性能产生很大影响。
- 因未打破 C/S 结构，可能会产生很大的安全风险。
- 不能满足对高并发连接数量的要求。

# 本讲内容概要

7 状态检测防火墙

8 切换代理

9 空气隙防火墙

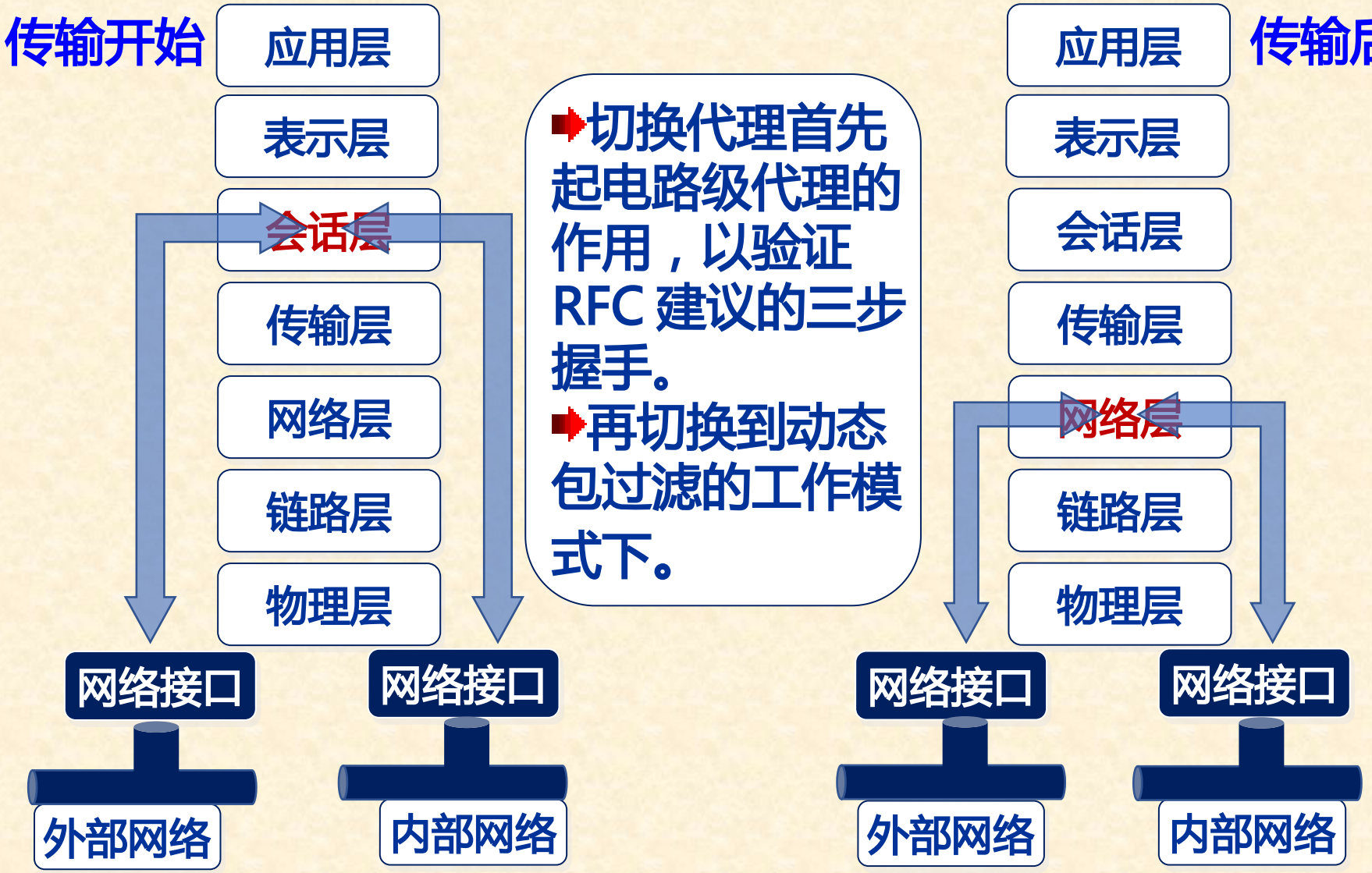
10 分布式防火墙

11 下一代防火墙

12 防火墙的典型产品

13 防火墙的发展趋势

# 切换代理的工作过程


传输开始
应用层
表示层
会话层
传输层
网络层
链路层
物理层
网络接口
网络接口
外部网络
内部网络
切换代理首先起电路级代理的作用，以验证RFC 建议的三步握手。
再切换到动态包过滤的工作模式下。
应用层
表示层
会话层
传输层
网络层
链路层
物理层
传输后续
网络接口
网络接口
外部网络
内部网络

# 切换代理优缺点

**优 点**

- 与传统电路级网关相比，对网络性能造成影响要小。
- 由于对三步握手进行了验证，降低了 IP 欺骗的风险。

**缺 点**

- 它不是一个电路级网关。
- 它仍然具有动态包过滤器遗留的许多缺陷。
- 由于没检查数据包的净荷部分，因此具有较低的安全性。
- 难于创建规则（受先后次序的影响）。
- 其安全性不及传统的电路级网关。

# 本讲内容概要

7 状态检测防火墙

8 切换代理

9 空气隙防火墙

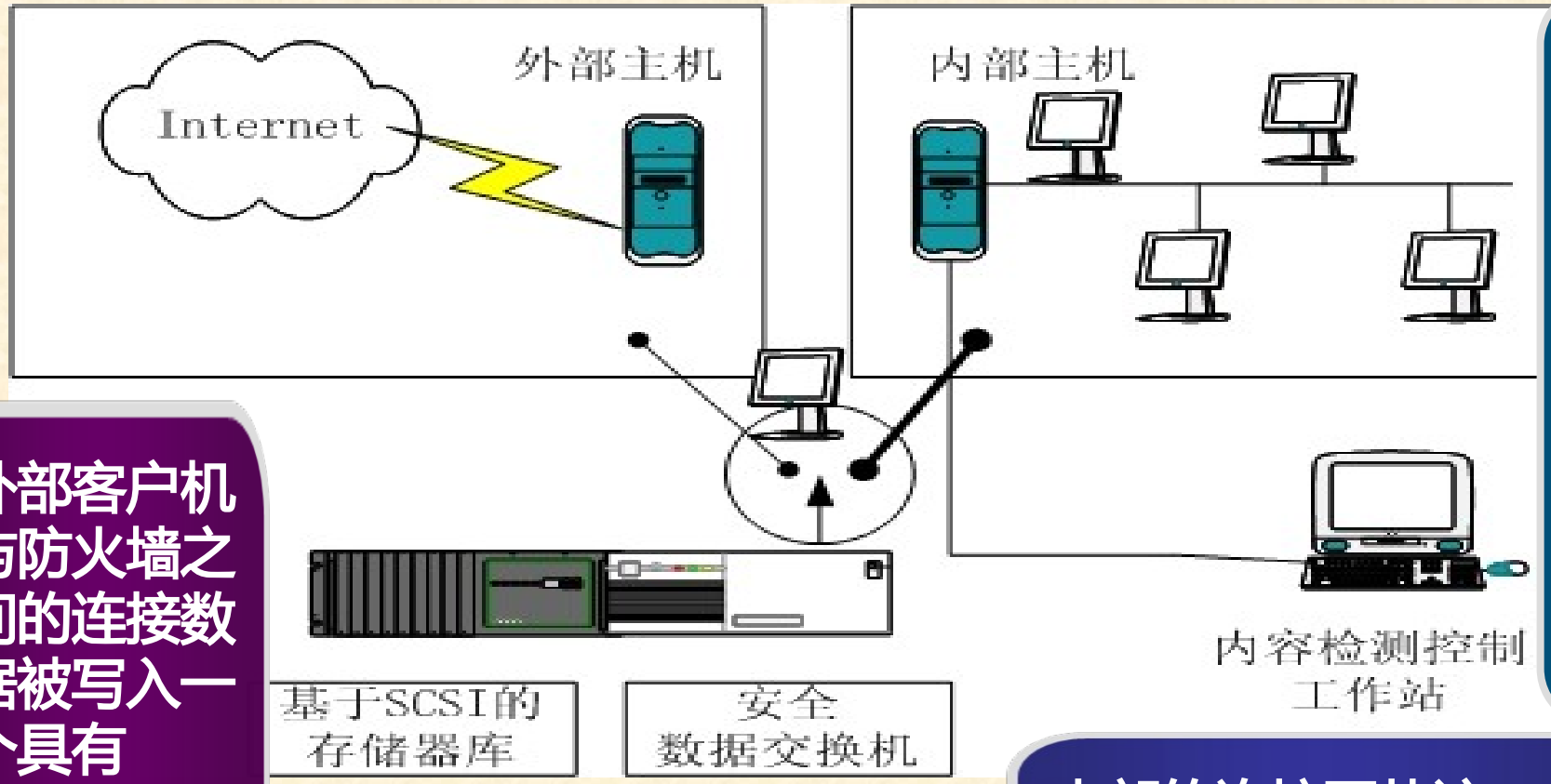
10 分布式防火墙

11 下一代防火墙

12 防火墙的典型产品

13 防火墙的发展趋势

# 空气隙防火墙的工作原理




外部客户机与防火墙之间的连接数据被写入一个具有 SCSI 接口的高速硬盘。

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。

内部的连接再从该 SCSI 硬盘中读取数据。

# 空气隙防火墙优缺点

## 优　点

- 切断与防火墙后面服务器的直接连接，消除隐信道攻击的风险。
- 采用应用代理对协议头长度进行检测，消除缓冲器溢出攻击。
- 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

- 降低网络的性能。
- 不支持交互式访问。
- 适用范围窄。
- 系统配置复杂。
- 结构复杂，实施费用高。
- 带来瓶颈问题。

# 本讲内容概要

7 状态检测防火墙

8 切换代理

9 空气隙防火墙

10 分布式防火墙

11 下一代防火墙

12 防火墙的典型产品

13 防火墙的发展趋势

# 分布式防火墙的工作原理

| | |
|---|---|
| 网络防火墙 | ● 内部网与外部网之间、内部网各子网之间<br>● 对内部子网之间的安全防护层 |
| 主机防火墙 | ● 对服务器和桌面机进行防护<br>● 内核模式应用，过滤和限制信息流 |
| 管理中心 | ● 服务器软件<br>● 管理、分发总体安全策略；汇总日志 |

# 分布式防火墙的优缺点

**优 点**

- 增强了系统安全性。
- 提高了系统性能。
- 提供了系统的扩展性。
- 可实施主机策略。

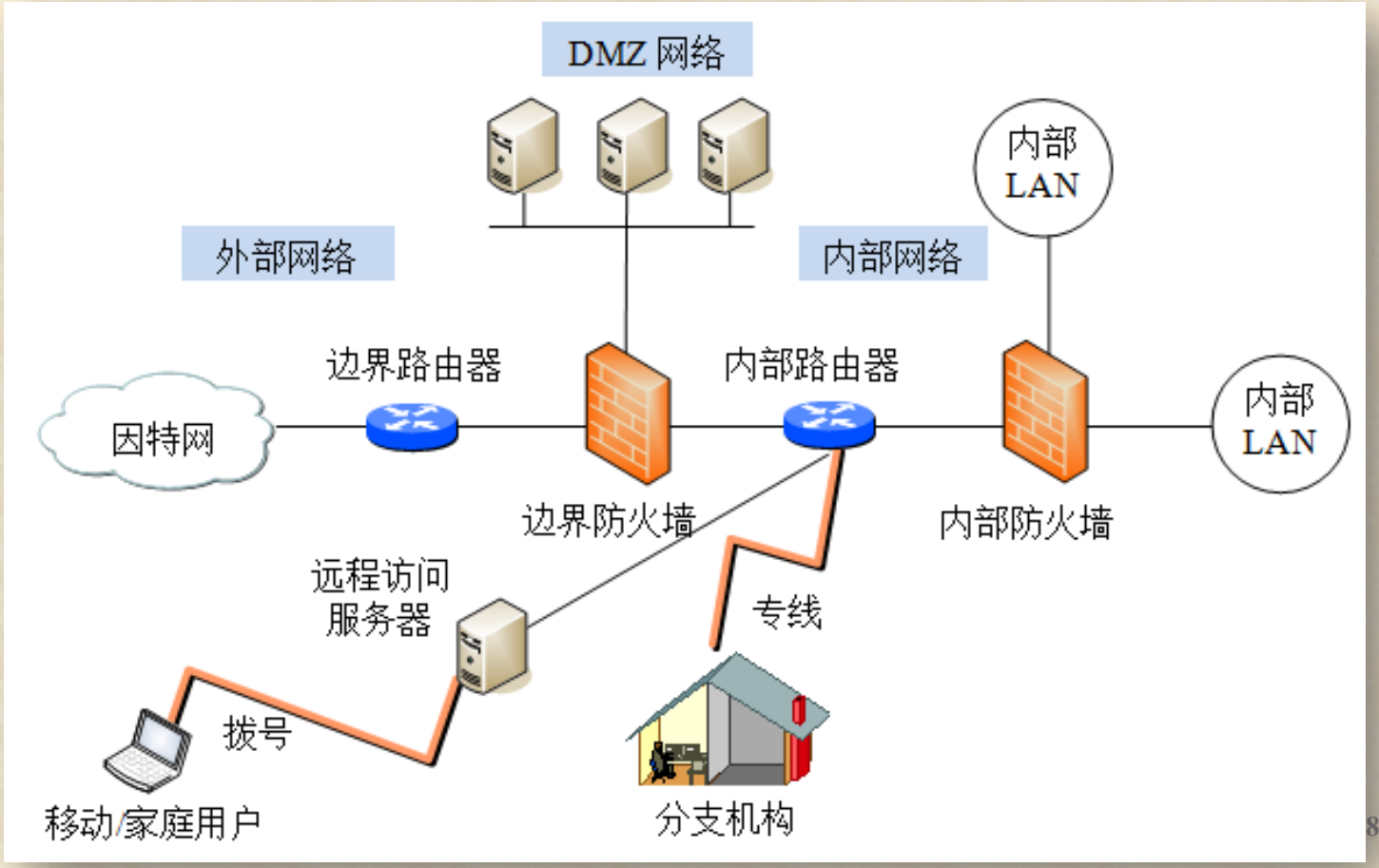
**缺 点**

- 系统部署时间长、复杂度高，后期维护工作量大。
- 可能受到来自系统内部的攻击或系统自身安全性的影响。

# 防火墙部署

# 防火墙的部署

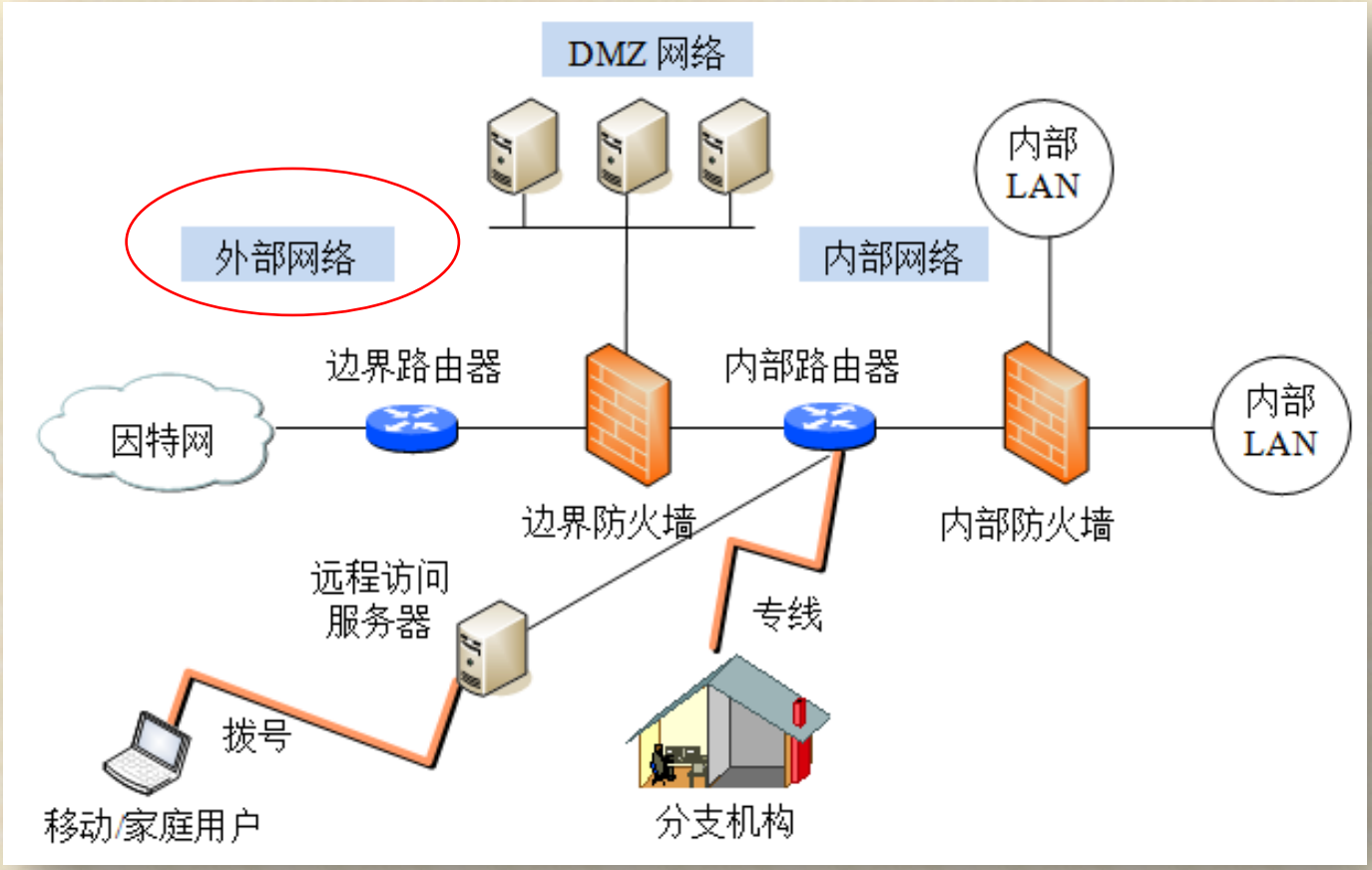
- 只需要把防火墙的 LAN 端口与组织内部的局域网线路连接，把防火墙的 WAN 端口连接到外部网络线路连接即可。其实这是非常错误的观点，防火墙的具体部署方法要根据实际的应用需求而定，不是一成不变的。
- 考虑一个典型的网络应用结构



# 防火墙的部署

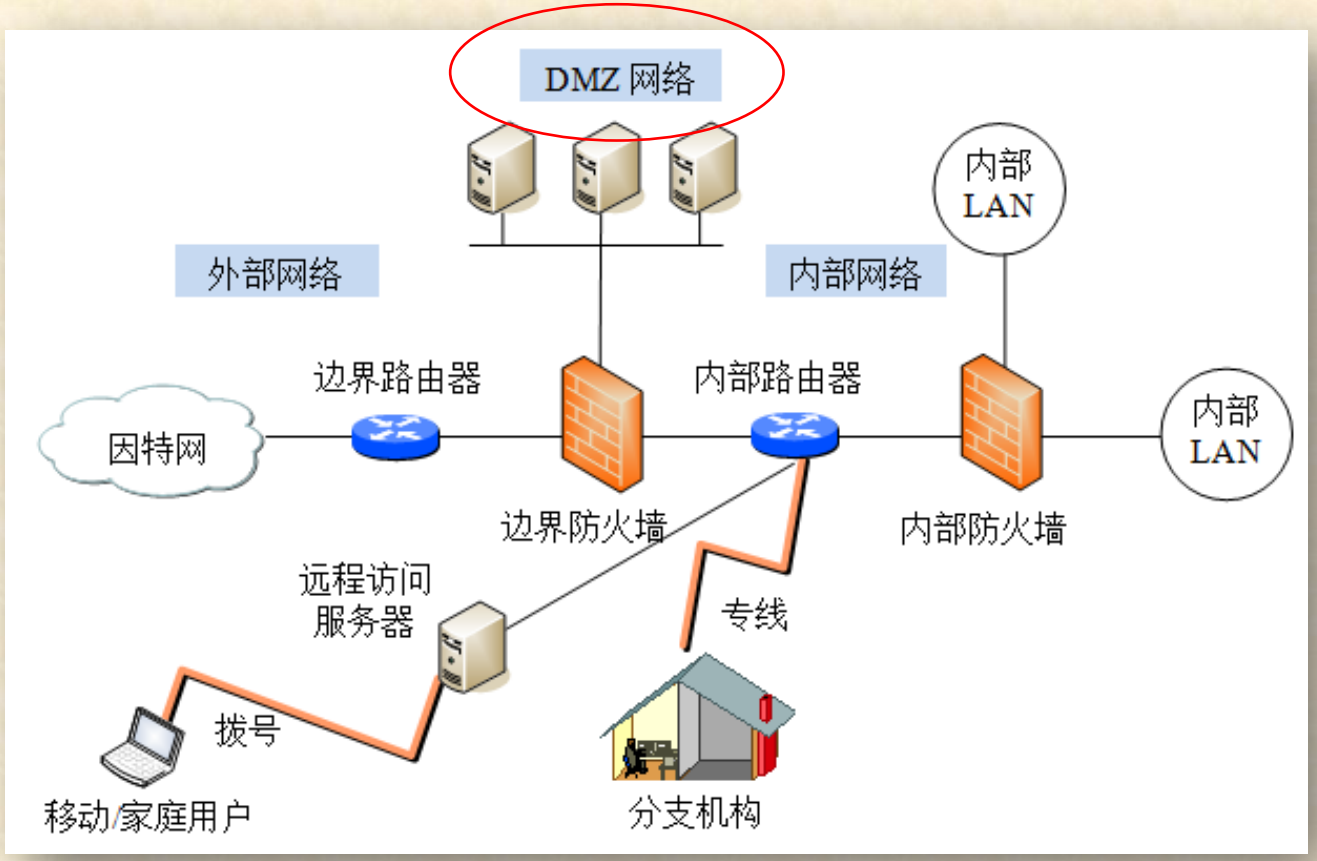
在这种应用中，整个网络结构分为 3 个不同的安全区域

1 ）外部网络。包括外部因特网用户主机和设备，这个区域为防火墙的非可信网络区域，此边界上设置的防火墙将对外部网络用户发起的通信连接按照防火墙的安全过滤规则进行过滤和审计，不符合条件的则不允许连接，起到保护内网的目的。



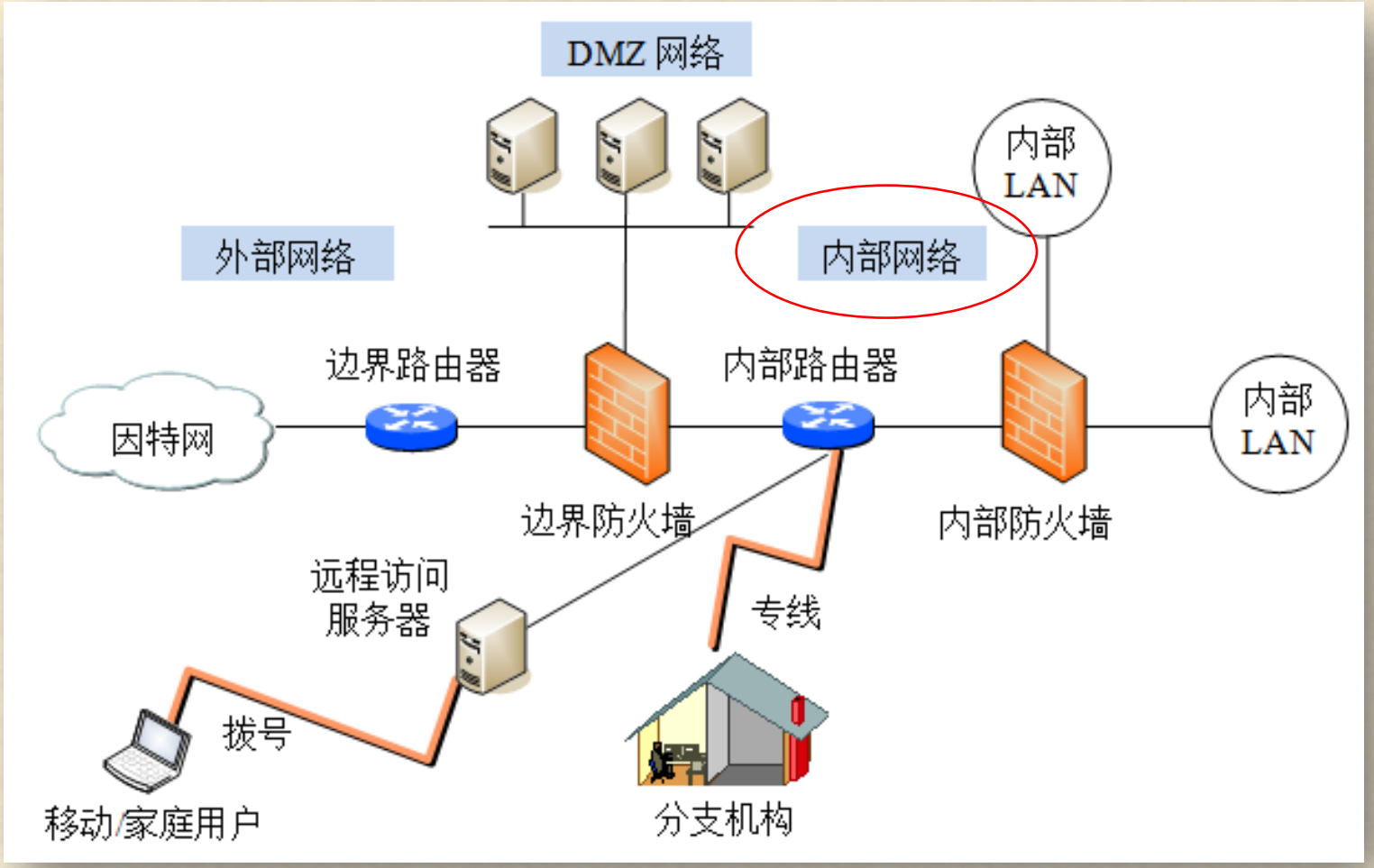
# 防火墙的部署

2 ）DMZ 网络。它是从内部网络中划分的一个小区域，其中包括内部网络中用于公众服务的服务器，如 Web 服务器、 Email 服务器、 FTP 服务器、外部 DNS 服务器等，都是为因特网公众用户提供某种信息服务的。在这个区域中，由于需要对外开放某些特定的服务和应用，因而网络受保护的级别较低，如果级别太高，则这些提供公共服务的网络应用就无法进行。也正因此，在这个区域中的网络设备所运行的应用也非常单一。



# 防火墙的部署

3 ）内部网络。这是防火墙要保护的对象，包括全部的内部网络设备、内网核心服务器及用户主机。



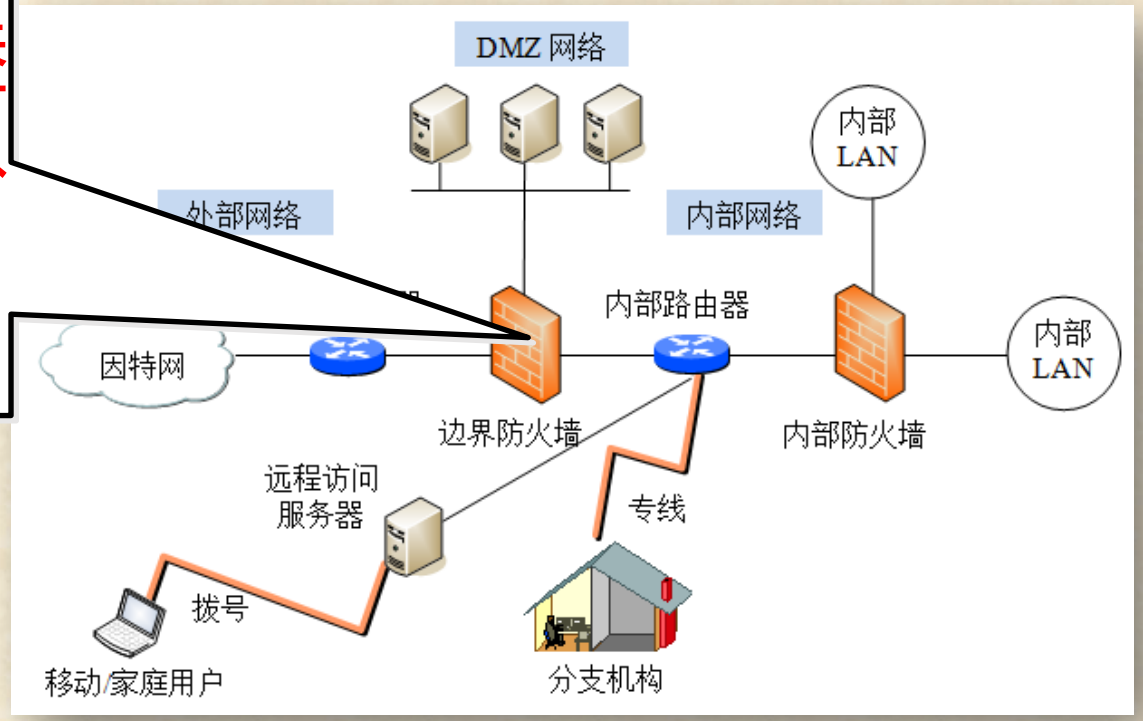
# 防火墙的部署

对于要保护的大部分内部网络来说，在一般情况下，禁止所有来自因特网用户的访问；而由企业内部网络划分出去的 DMZ 区，因需为因特网应用提供相关的服务，所以在一定程度上没有内部网络限制得那么严格，如 Web 服务器通常是允许任何人进行正常访问的。虽然这些服务器很容易遭受攻击，但是由于在这些服务器上所安装的服务非常少，所允许的权限非常低，真正的服务器数据是在受保护的内部网络主机上，所以黑客攻击这些服务器最可能的后果就是使服务器瘫痪。

# 防火墙的部署

- 对于以上典型的网络体系结构，可以部署 3 种类型的防火墙：

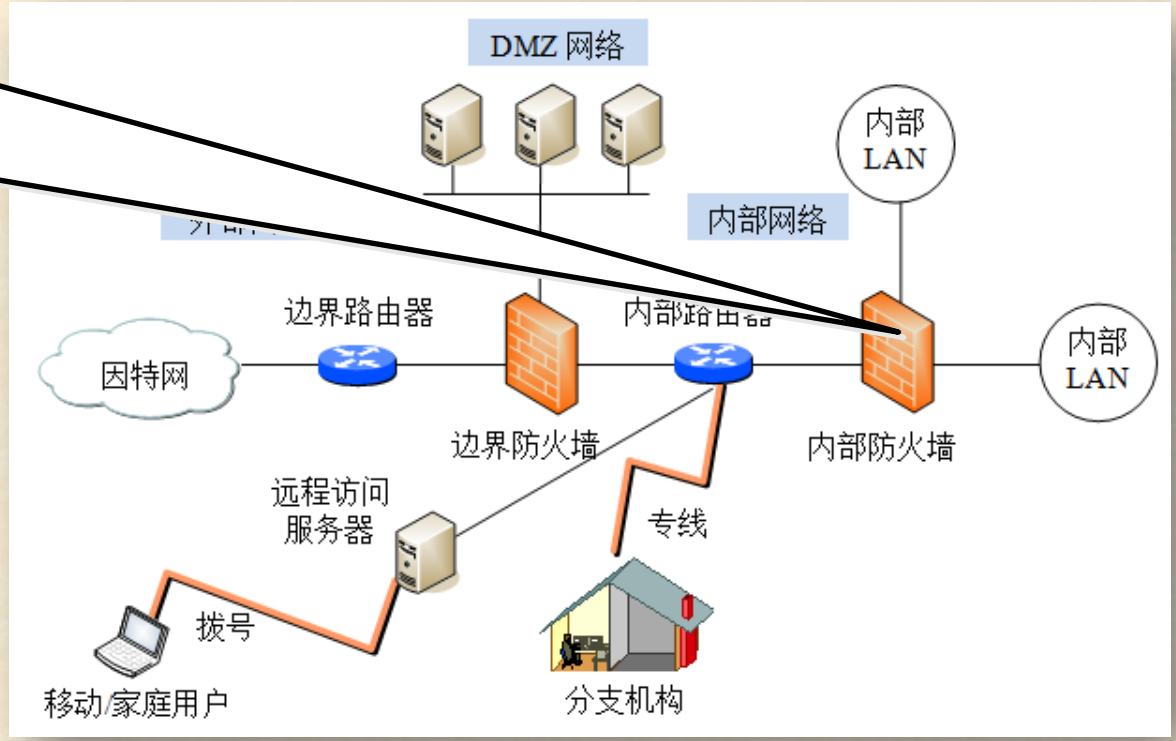
**外部防火墙。处于外部不可信网络（包括因特网、广域网和其他公司的专用网）与内部可信网络之间，控制来自外部不可信网络对内部可信网络的访问，防范来自外部网络的非法攻击。同时，保证 DMZ 区服务器的相对安全性和使用便利性。**



# 防火墙的部署

- 对于以上典型的网络体系结构，可以部署 3 种类型的防火墙：

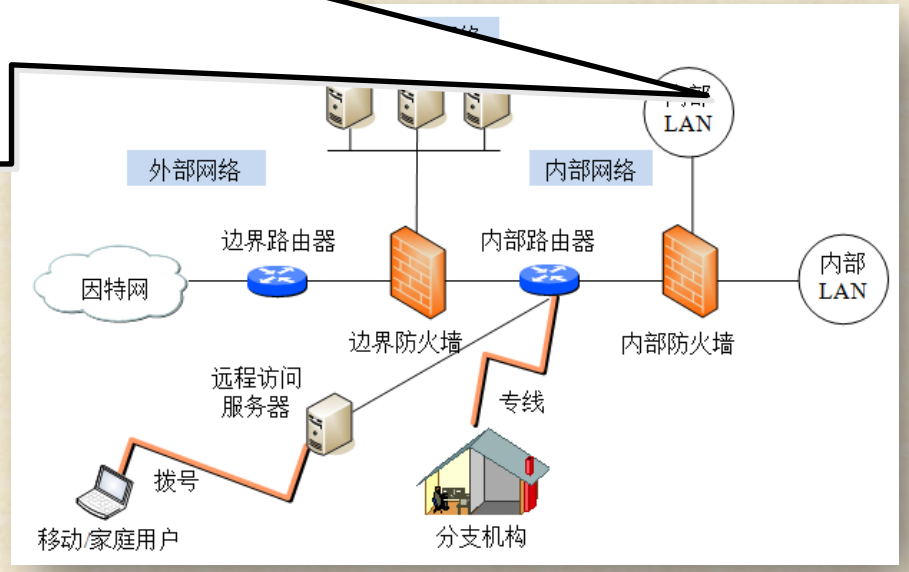
**内部防火墙。处于内部不同可信等级安全域之间，起到隔离内网关键部门、子网或用户的目的。**



# 防火墙的部署

- 对于以上典型的网络体系结构，可以部署 3 种类型的防火墙：

**主机型防火墙，又称个人防火墙。服务于广大的个人主机用户，通常为软件防火墙，安装于单台主机中，防护的也只是单台主机。它可以监测主机上进行的入站和出站网络连接，并能够根据预先定义的规则，执行基于网络地址和基于应用的访问控制，通常还具有反恶意软件、入侵检测和网络告警等其他安全功能。**



# 本讲内容概要

7 状态检测防火墙

8 切换代理

9 空气隙防火墙

10 分布式防火墙

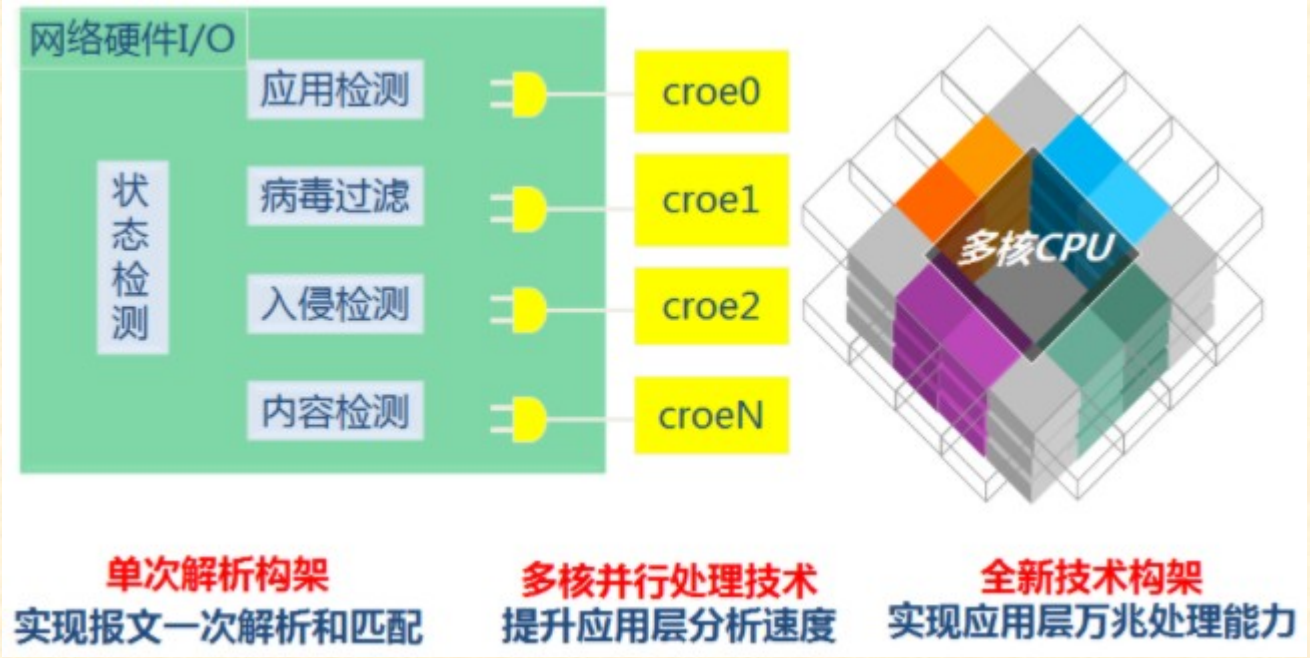
11 下一代防火墙

12 防火墙的典型产品

13 防火墙的发展趋势

# 下一代防火墙（ NGFW ）

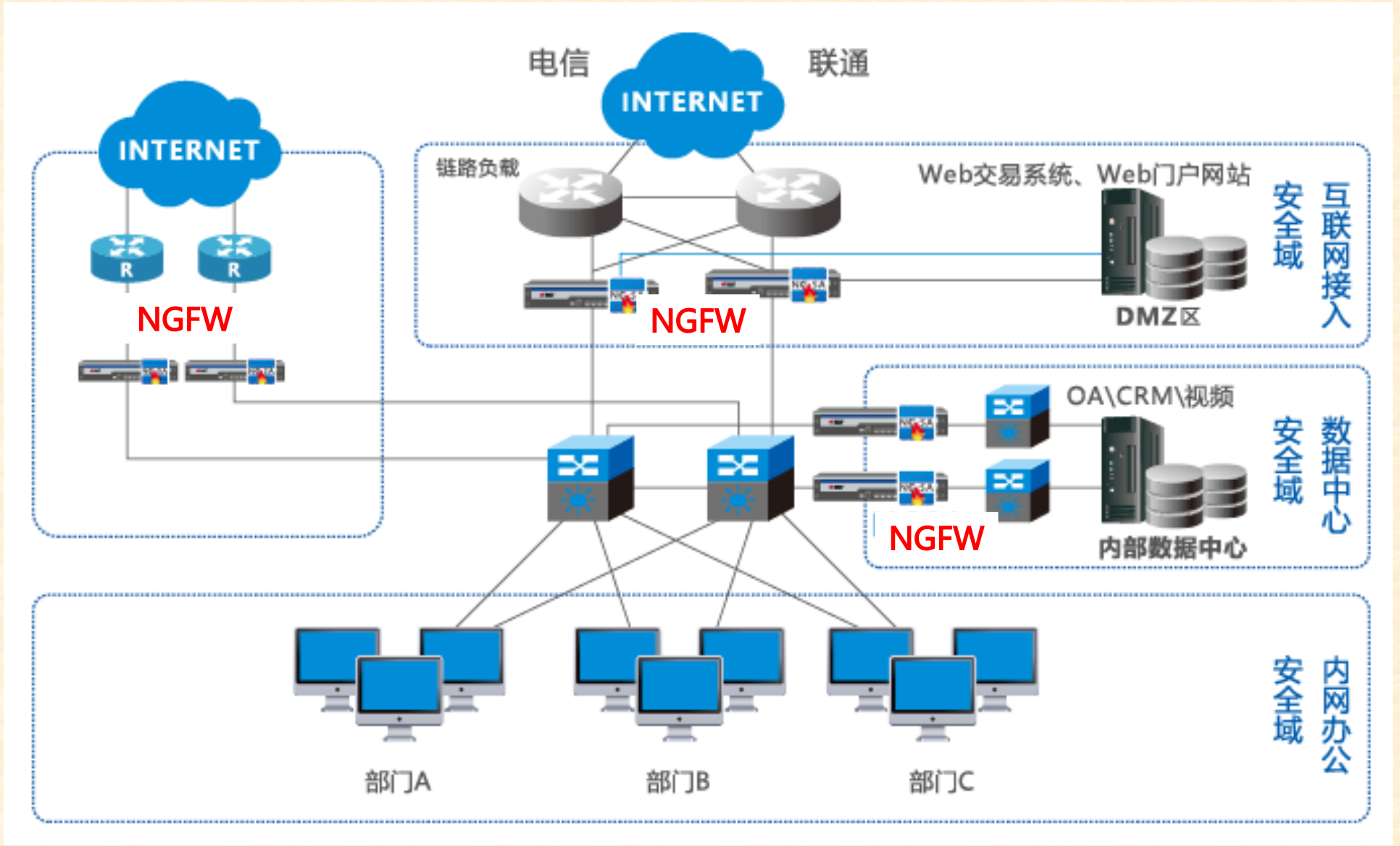
- 下一代防火墙（ NGFW ），从用户、应用和行为的角度出发，重新实现了流量分类、访问控制、攻击防护和 QoS 等所有传统防火墙功能；
- 并基于这些功能进行了高级抽象，提供用户策略、应用策略和行为策略等智能控制手段，有效解决了传统防火墙无法解决的问题。
- 并集合了智能接入、灵活组网、全面安全、入侵防御、防病毒、云化管理可视化运维为一体等下一代防火墙部署场景；
- 提供从网络层到应用层的攻击防护，为用户构建高效一体化的安全防护体验。



# 下一代防火墙功能

1. 立体化的安全防御体系：实现 IPS 、 AV 、 URL 识别、跨站、木马、 DOS/DDoS 防护及应用识别等多种安全特性；
2. 应用识别、内容识别与管控：内置 20 大类超过 2700 种应用类别数据库，包括 P2P 、 IM 、视频、游戏软件、炒股软件实施全面控制。
3. 未知威胁防御防护：支持 APT 防护功能，支持可疑文件、 0day 攻击、泄密行为、加密 C&C 流量、病毒等威胁定位、阻断和溯源。
4. 网络行为优化：基于用户身份、应用程序、优先级灵活的智能流量管理；基于应用和用户的链路负载，支持应用、行为、内容精细化管控；
5. 安全可视化和行为审计：提供从网络层到应用层、从用户到全网的多层次多角度地展现模式；
6. 强大的网络适应性：支持多种形式灵活部署，具备 GER 、 NAT 、 IPv6 支持、 VPN 、 OSPF 、 VRRP 、 HA 、 ALG 等功能，满足用户多样化的网络功能需求。
7. 可靠性保障：支持双机状态热备功能，支持 Active/Active 和 Active/Passive 两种工作模式，实现负载分担和业务备份。

# 下一代防火墙部署应用


电信
INTERNET
联通
INTERNET
R
R
NGFW
链路负载
NGFW
Web交易系统、Web门户网站
DMZ区
互联网接入安全域
OA\CRM\视频
NGFW
内部数据中心
数据中心安全域
部门A
部门B
部门C
内网办公安全域

# 本讲内容概要

7 状态检测防火墙

8 切换代理

9 空气隙防火墙

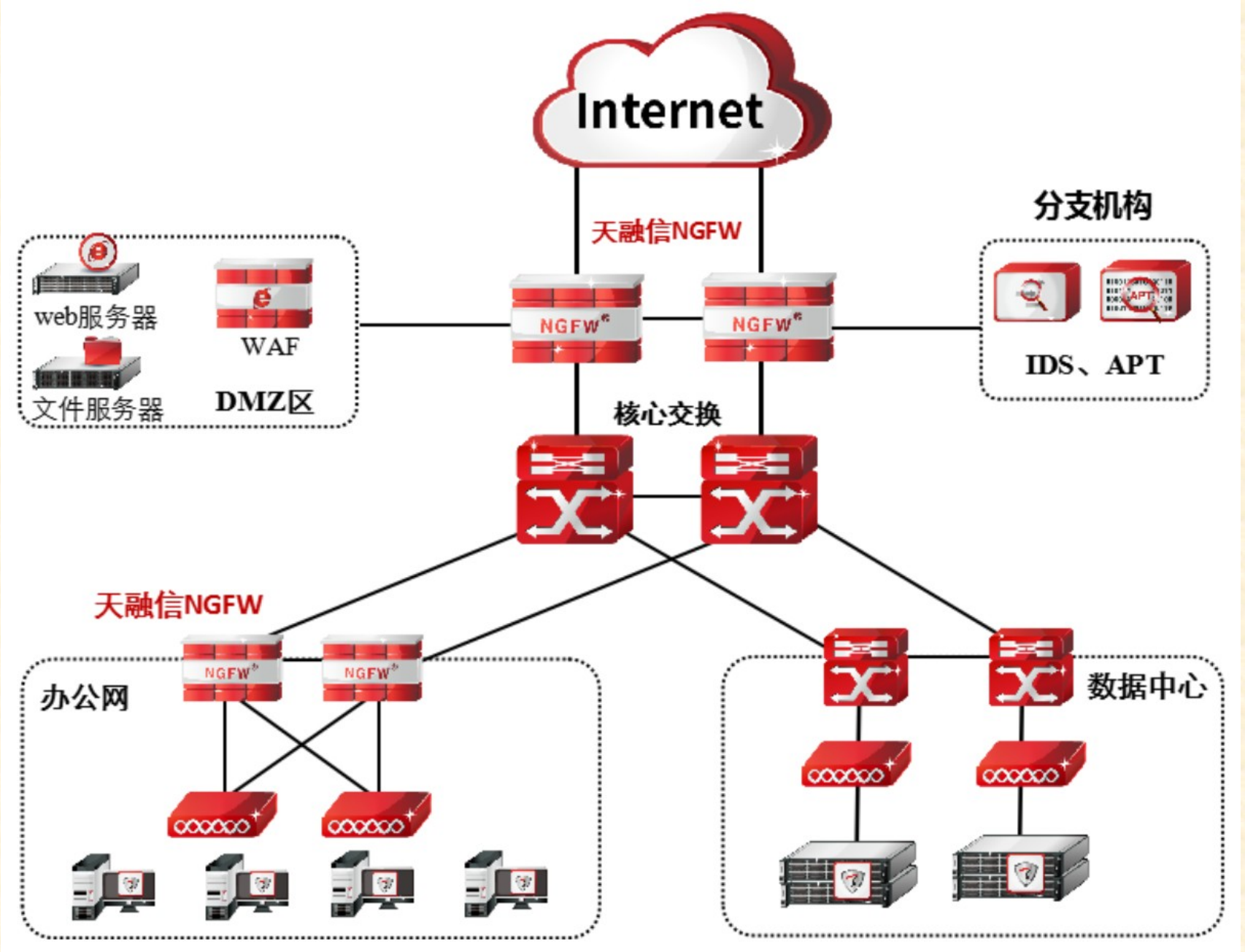
10 分布式防火墙

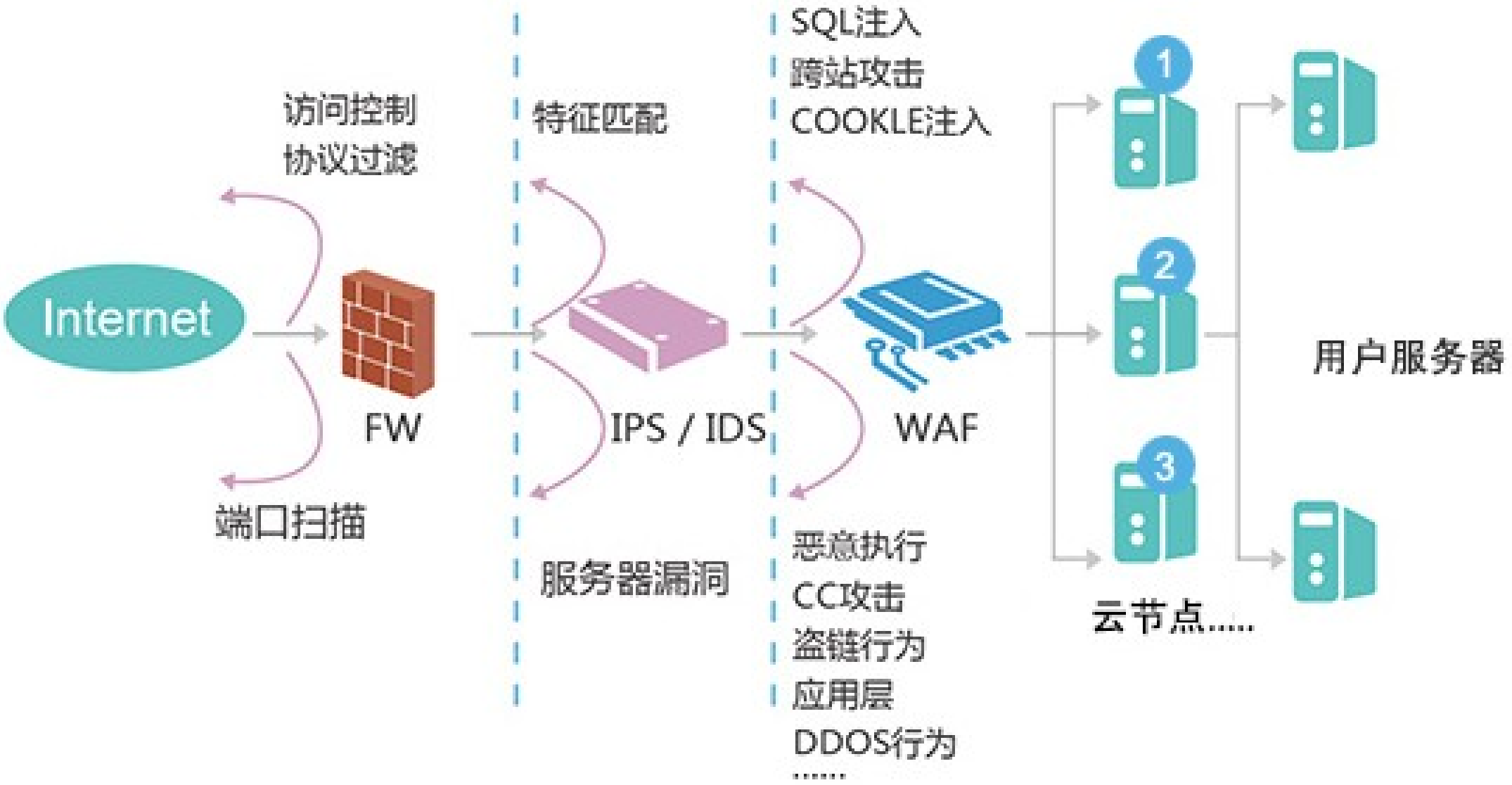
11 下一代防火墙

12 防火墙的典型产品

13 防火墙的发展趋势

# 天融信 NGFW® 下一代防火墙



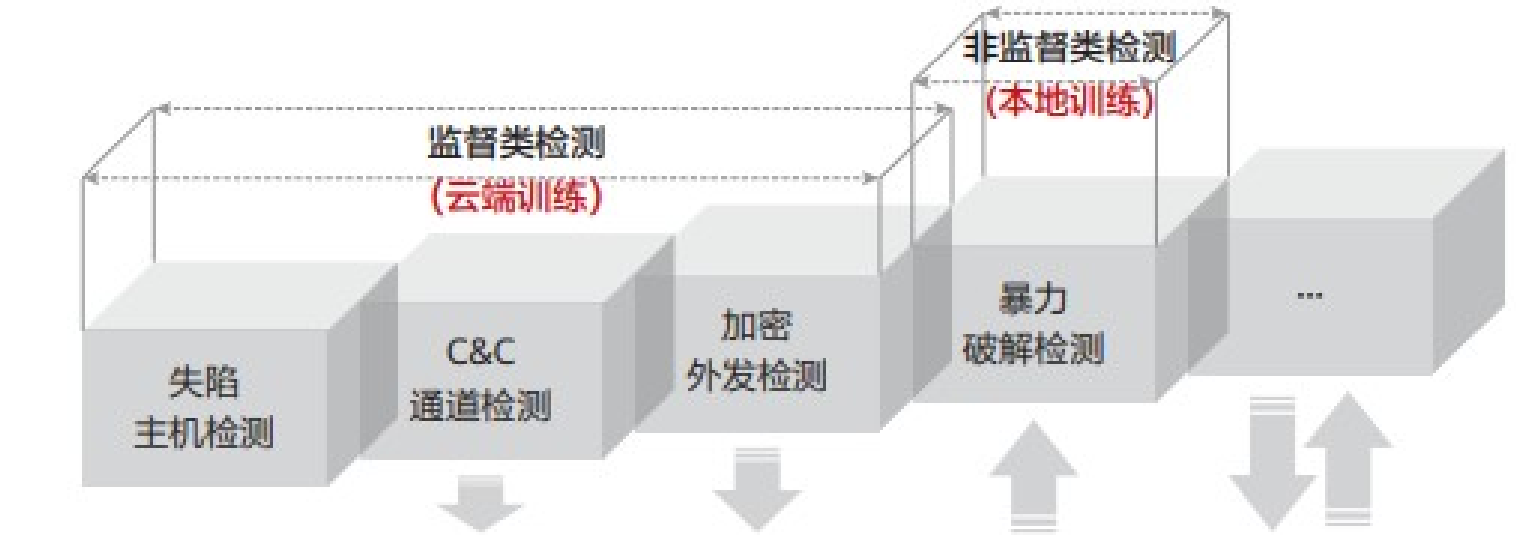



华数网络 多节点集群WAF防火墙设备

# 华为 HiSecEngine USG6600E 系列 AI 防火墙（盒式）

集传统防火墙、 VPN 、入侵防御、防病毒、数据防泄漏、带宽管理、 Anti-DDoS 、 URL 过滤、反垃圾邮件等多种功能于一身。

- NGE ：提供 IPS 、反病毒和 URL 过滤等；
- CDE ：数据深度分析，暴露威胁的细节，快速检测恶意文件；
- AIE ： APT 威胁检测引擎，针对暴力破解、 C&C 异常流量、 DGA 恶意域名和加密威胁流量进行检测。




- 云端实时加载新威胁检测模型，无需客户升级版本
- 华为不断耕耘AI APT检测，应对更多更新更多样的威胁


# 本讲内容概要

7 状态检测防火墙

8 切换代理

9 空气隙防火墙

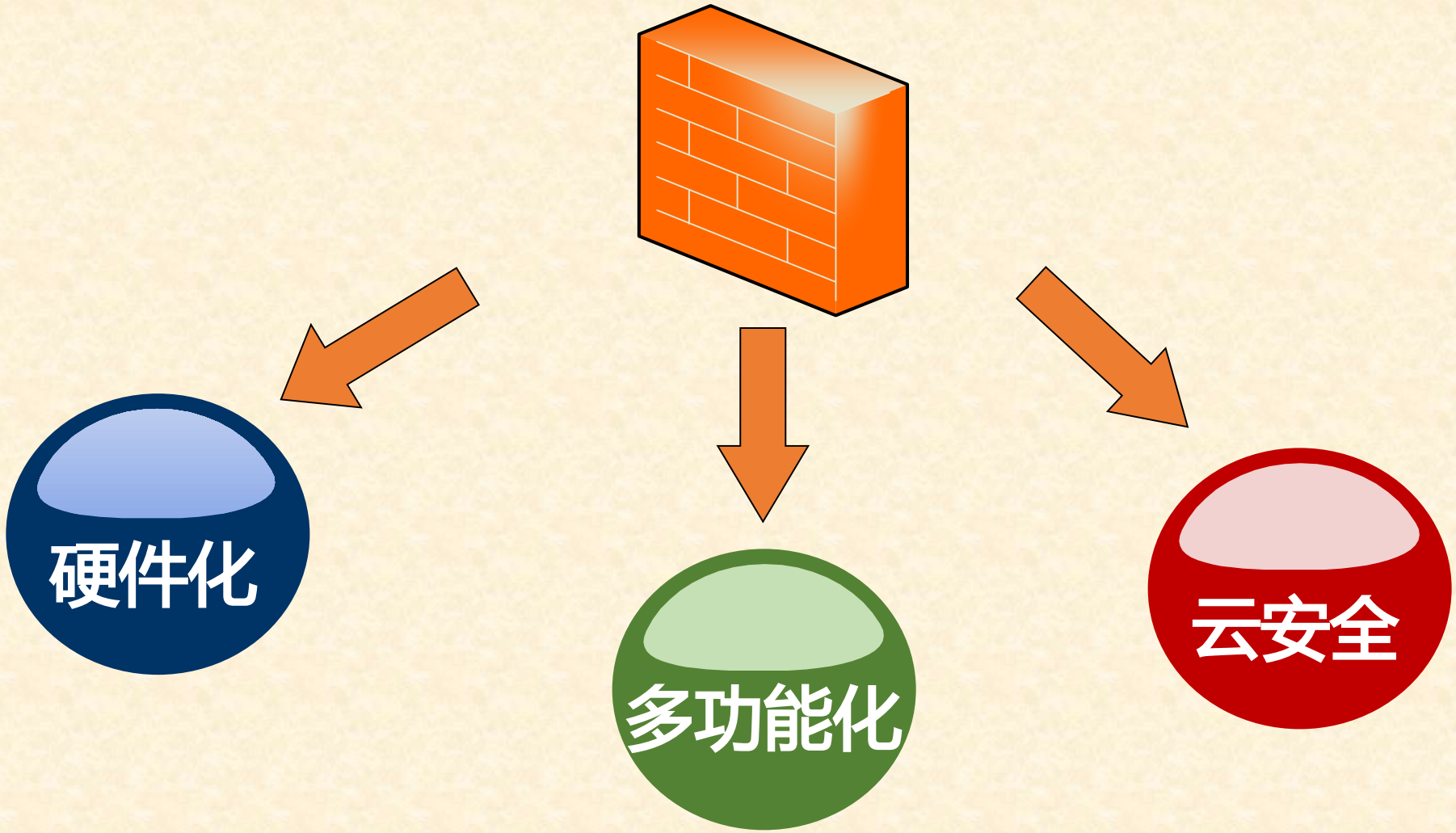
10 分布式防火墙

11 下一代防火墙

12 防火墙的典型产品

13 防火墙的发展趋势

# 防火墙的发展趋势




# 谢 谢！