

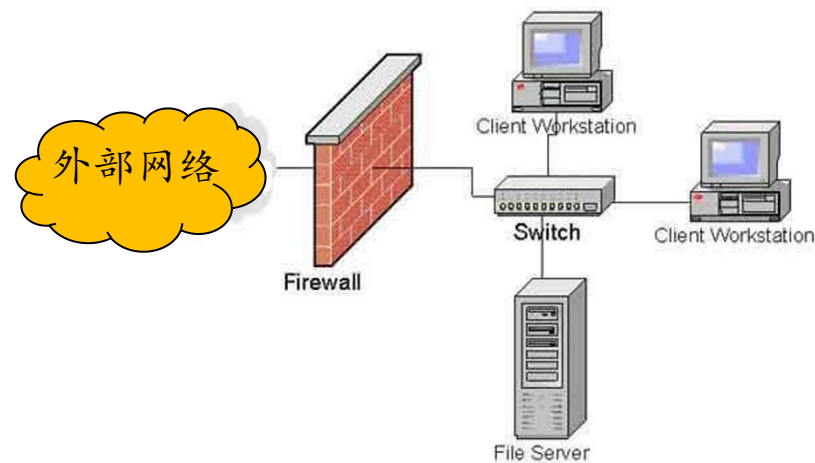
网络应用技术

第10讲 使用防火墙加强网络通信控制

河南中医药大学信息技术学院

网络技术课程教学组

一、认识防火墙



认识防火墙

□ 防火墙是什么？

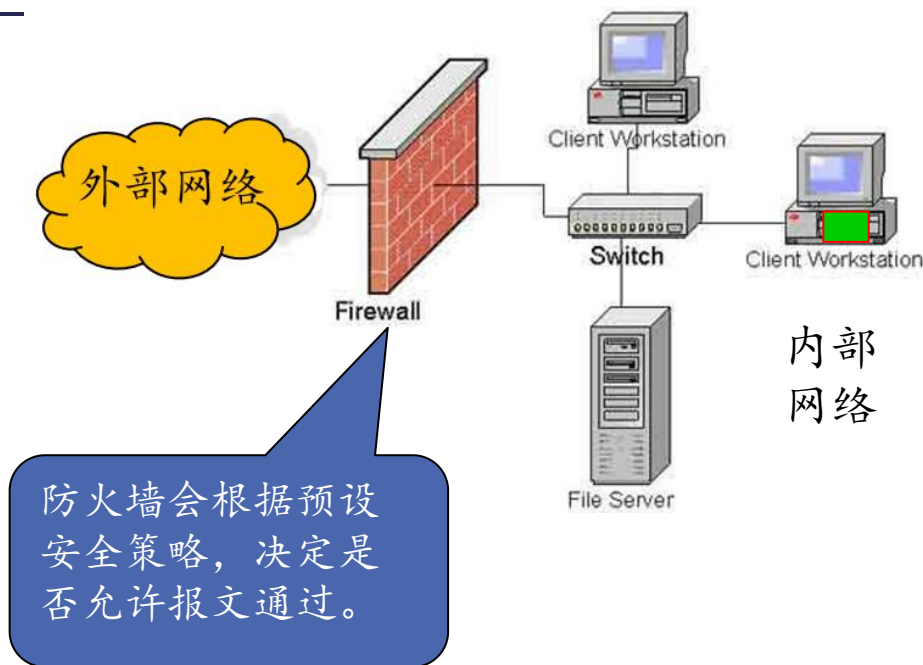
- 防火墙（Firewall）是一种网络安全系统，旨在保护计算机网络免受未经授权的访问和恶意攻击。【基本作用】
- 防火墙可以是软件（防火墙），也可以是融合软、硬件的安全设备，通常部署在不同网络（如可信任的企业内部网络和不可信的公共网络）或网络安全域之间，从而实现对通信的控制。【表现形态、部署位置】
- 在逻辑上，防火墙是一个分离器、一个分析器，也是一个限制器，能够通过预设安全策略，对流经防火墙的数据流进行监控（表现为允许通过或禁止通过），从而保证内部网络和隔离区的安全。【功能特点】

认识防火墙

□ 防火墙是什么？

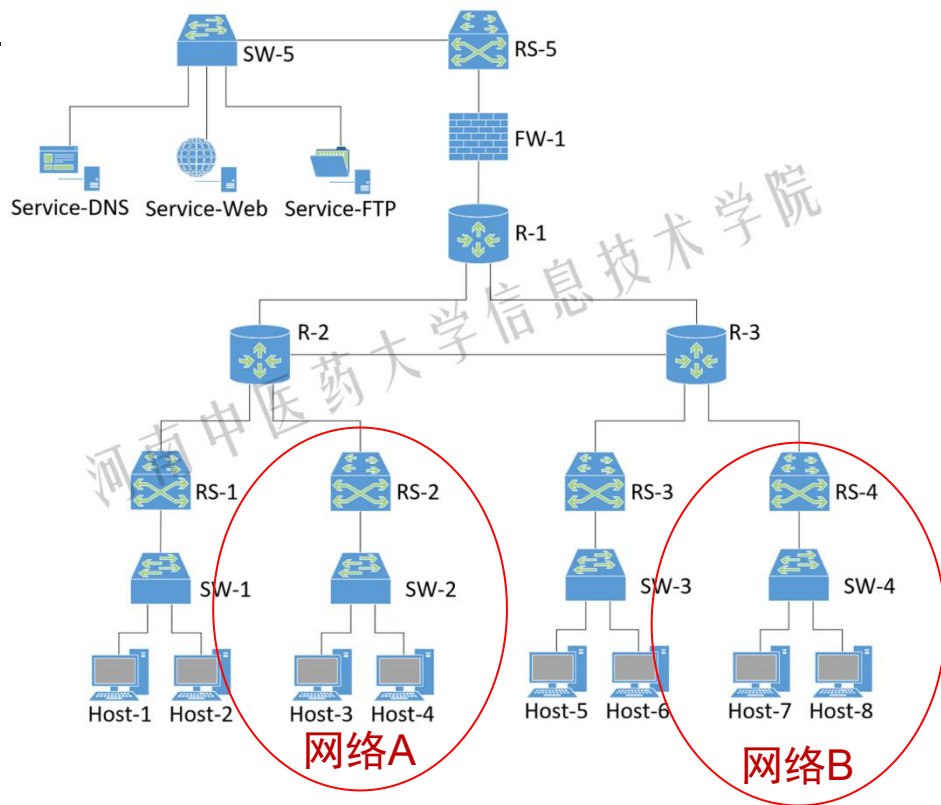
■ 对FW的初步归纳

- **本质：**安全系统
- **体现：**软件+硬件
- **部署特点：**不同网络之间、网络内不同安全域之间
- **功能特点：**分析、限制，根据预设安全策略，决定是否允许报文通过



➤ 防火墙应用举例

- 通过部署防火墙，可实现
 1. 不允许网络A内的主机访问FTP服务，其他网络允许；
 2. 网络B中主机只能在上班时间内访问Web服务
 3.



认识防火墙

□ 防火墙能做什么？

1. **访问控制**：防火墙可以制定和实施安全策略，控制哪些用户可以访问哪些网络资源，以及哪些服务可以被外部用户访问。通过定义规则集，防火墙可以允许或拒绝特定的网络流量，从而保护内部网络免受未经授权访问。
2. **数据包过滤**：防火墙能够检查经过它的所有数据包，并根据预设的规则决定是允许数据包通过还是将其丢弃。这些规则通常基于源IP地址、目标IP地址、源端口、目标端口、协议类型（如TCP、UDP）等信息。
3. **状态检测**：除了简单的包过滤外，现代防火墙还具备状态检测功能。状态检测防火墙能够跟踪网络连接的状态（如新建、已建立、已关闭），并根据连接的状态动态地允许或拒绝数据包。这种方法提高了安全性，因为它可以阻止某些类型的网络攻击，如SYN Flood攻击。

认识防火墙

□ 防火墙能做什么？

4. **网络地址转换（NAT）**：防火墙经常用于实现网络地址转换（NAT），将内部网络的私有IP地址转换为公网可用的IP地址。这不仅可以隐藏内部网络的真实结构，还可以减少可用的攻击面，因为外部攻击者只能看到转换后的公网IP地址。
5. **日志记录和报警**：防火墙能够记录所有通过它的网络活动，包括被允许和被拒绝的数据包。这些日志对于后续的安全审计、故障排查以及检测潜在的安全威胁至关重要。此外，防火墙还可以配置为在检测到特定类型的网络活动时发出警报。

认识防火墙

□ 防火墙能做什么？

6. **应用层过滤：**一些高级防火墙还能够对应用层协议（如HTTP、FTP、SMTP等）进行深度包检测（DPI），从而基于应用层内容来允许或拒绝数据包。这有助于防止基于应用层的攻击，如SQL注入、跨站脚本（XSS）等。
7. **VPN支持：**许多防火墙还支持虚拟专用网络（VPN）技术，允许远程用户通过加密通道安全地访问内部网络资源。
8. **认证接入：**防火墙可以要求指定的接入用户在通过防火墙访问网络时，输入一个用户名和密码，即进行认证。认证成功的用户，以后发出的报文才可以通过防火墙（当然，还要符合安全策略）。如果主机不能和防火墙之间认证成功，这个报文会被丢弃。

认识防火墙

□ 防火墙的分类

■ 按防火墙采用的主要技术划分：

➤ 包过滤防火墙

- ◆ 工作在ISO 7层模型的传输层下，根据数据包头部一些字段进行过滤。
- ◆ 主要包括静态包过滤防火墙、动态包过滤防火墙和状态检测防火墙。

➤ 代理防火墙

- ◆ 工作在ISO 7层模型的应用层。它完全阻断了网络访问的数据流，而是为每一种服务都建立了一个代理，内联网络与外联网络之间没有直接的服务相连，都必须通过相应的代理审核后再转发。

认识防火墙

□ 防火墙的分类

■ 按防火墙的表现形式划分：

➤ 软件防火墙

- ◆ 软件防火墙的产品形式是软件代码，它不依靠具体的硬件设备，而纯粹依靠软件来监控网络信息。

➤ 独立硬件防火墙

- ◆ 独立硬件防火墙基于特定用途集成电路开发，性能优越，但可扩展性、灵活性较差。

➤ 模块化防火墙

- ◆ 防火墙大多基于网络处理器开发，许多路由器都已经集成了防火墙的功能，这种防火墙往往作为路由器的一个可选配的模块存在。

认识防火墙

□ 防火墙的分类

■ 按防火墙的**保护对象**划分：

➤ 单机防火墙

- ◆ 单机防火墙的设计目的是为了保护单台主机网络访问操作的安全，一般是以装载到受保护主机硬盘里的软件程序的形式存在的。

➤ 网络防火墙

- ◆ 网络防火墙的设计目的是为了保护相应网络的安全，一般采用软件与硬件相结合的形式，也有纯软件的网络防火墙存在。

防火墙的分类

□ 防火墙的分类

■ 按防火墙的**使用者**划分：

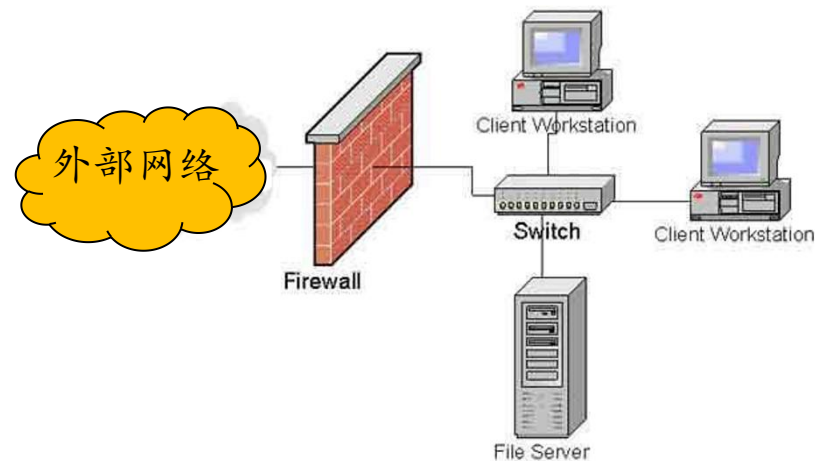
➤ 企业级防火墙

- ◆ 企业级防火墙设计目的是为企业联网提供安全访问控制服务，同时根据企业的安全要求，企业级防火墙还会提供更多的安全功能。

➤ 个人防火墙

- ◆ 个人防火墙主要用于个人使用计算机的安全防护，实际上与单机防火墙是一样的概念，只是看待问题的出发点不同而已。

二、防火墙的主要技术



防火墙的主要技术

- 防火墙技术是一种综合技术，主要包括包过滤技术、状态检测技术、NAT技术、代理技术等等，这些技术互相配合，从而形成一套防御系统。

二、防火墙的主要技术

2.1 包过滤技术

防火墙的主要技术——包过滤

□ 包过滤技术简介

- 包过滤技术是最基本的防火墙技术之一，又称报文过滤技术。它根据一系列预定义（由管理员制定）规则过滤进出网络的数据包。
- 过滤，就是根据防火墙上事先制定的规则集，对通过防火墙的数据包进行匹配检查。若数据包满足某条规则，在依据该规则做出相应的处理，即允许（**permit**）通过或者拒绝（**deny**）通过。若数据包不满足管理员制定的所有规则，则按照防火墙默认规则（通常是禁止）执行。
- 此处的过滤规则也称“安全策略”，通常围绕报文首部中的5个字段（也称“五元组”）信息来制定。
- 五元组：源IP地址、目的IP地址、源端口、目的端口、协议类型。
- 举例

➤ 举例：包过滤防火墙中的安全规则

□ 在防火墙上制定一条名为abc（名称自定）的安全规则

- 该策略允许（permit）来源IP地址是192.168.64.0/24网段的主机，以Web（http协议）方式，访问目的网络是172.16.64.0/24网段的主机，即允许符合该策略的报文通过防火墙。
- 命令配置如下

```
[FW1-policy-security]rule name abc
[FW1-policy-security-rule-abc]source-address 192.168.64.0 24
[FW1-policy-security-rule-abc]destination-address 172.16.64.0 24
[FW1-policy-security-rule-abc]service http
[FW1-policy-security-rule-abc]action permit
```

提示：首先建立abc规则，接下来在abc规则视图配置具体规则。

防火墙的主要技术——包过滤

- 过滤IP数据报首部
字段



防火墙的主要技术——包过滤

- 过滤TCP报文段首部字段



防火墙的主要技术——包过滤

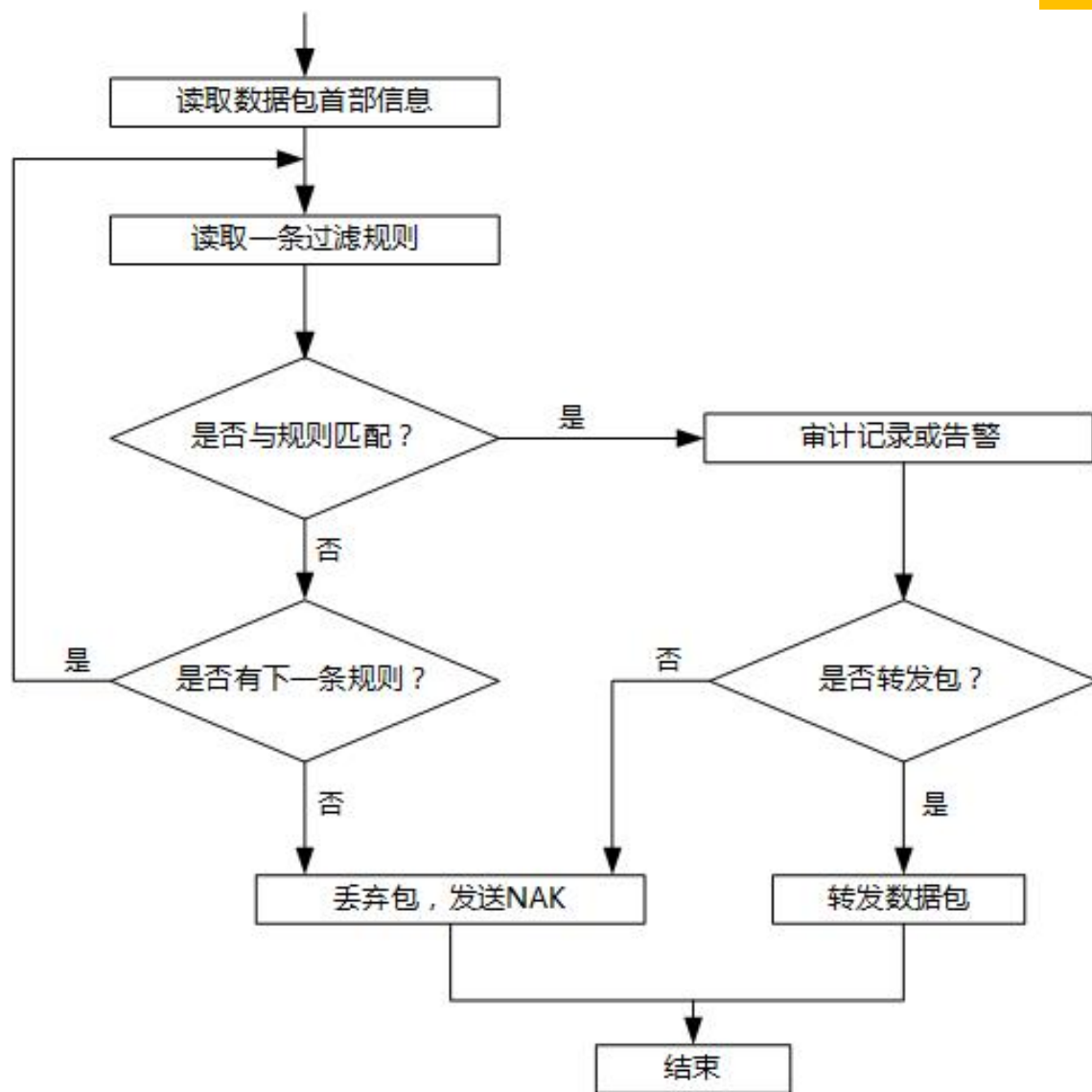
表1 一个过滤规则样表

序号	源 IP	目的 IP	协议	源端口	目的端口	标志位	操作
1	内部网络地址	外部网络地址	TCP	任意	80	任意	允许
2	外部网络地址	内部网络地址	TCP	80	>1023	ACK	允许
3	所有	所有	所有	所有	所有	所有	拒绝

含义：（注意规则的顺序）

1. 允许内部网络访问外部网络中的Web服务（目的端口80）
2. 允许从外部网络中Web服务器的返回报文（源端口80，ACK）
3. 其他任何访问都禁止

➤ 包过滤的实现过程



防火墙的主要技术——包过滤

□ 包过滤技术的优缺点

■ 优点：

- 包过滤技术实现简单、快速。
- 对于用户和应用来说，包过滤通常是透明的，不需要修改应用或用户行为。
- 包过滤仅查看数据包的头部信息，不需要深入到数据包内容，从而减少了处理时间，在高速网络环境中尤为重要。

■ 缺点：

- 包过滤技术过滤思想简单，对信息的处理能力有限。
- 包过滤技术控制层次较低，不能实现用户级控制。

二、防火墙的主要技术

2.2 状态检测

防火墙的主要技术——状态检测

□ 状态检测技术的概念

- 为了解决静态包过滤技术安全检查措施简单、管理较困难等问题，提出了状态检测技术（Stateful Inspection）的概念。
- 早期的状态检测技术被称为动态包过滤（Dynamic Packet Filter）技术，是静态包过滤技术在传输层的扩展应用。
- 状态检测不仅仅只是对状态进行检测，还进行包过滤检测，从而提高了防火墙的功能。

防火墙的主要技术——状态检测

□ 状态检测的核心

- 是对象的各种状态，并且根据状态来判断数据包是否合法。
 - TCP及状态
 - UDP及状态
 - ICMP及状态

防火墙的主要技术—— 状态检测

□ TCP及状态

- TCP是一个面向连接的协议，对于通信过程各个阶段的状态都有很明确的定义，并可以通过TCP的标志位进行跟踪。
- TCP共有11种状态，这些状态标识由RFC793定义。

TCP 状态详情表

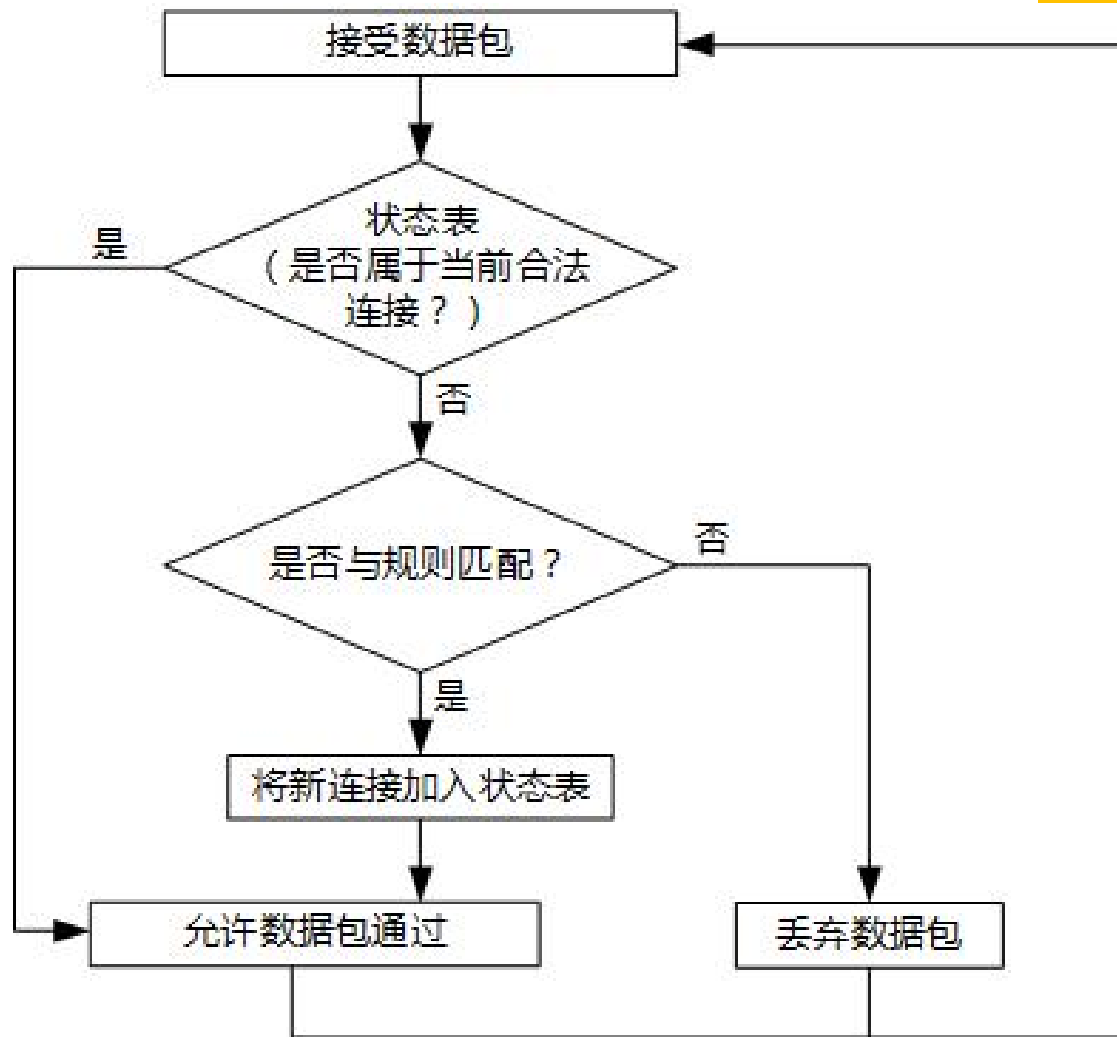
状态	状态解释
CLOSED	在连接之前的状态
LISTEN	等待连接请求的状态
SYN-SENT	发出 SYN 报文后等待返回响应时间的状态
SYN-RECEIVED	收到 SYN 报文并返回 SYN-ACK 相应后的状态
ESTABLISHED	建立连接后的状态，即发送方收到 SYN-ACK 后的状态，接收方在收到 3 次握手最后的 ACK 报文后的状态
FIN-WAIT-1	关闭连接，发起者发送初始 FIN 报文后的状态
CLOSE-WAIT	关闭连接，接受者收到初始 FIN 并返回 ACK 响应后的状态
FIN-WAIT-2	关闭连接，发起者收到初始 FIN 报文的 ACK 响应后的状态
LAST-ACK	关闭连接，接受者将最后的 FIN 报文发送给关闭连接发起者后的状态
TIME-WAIT	关闭连接，发起者收到最后的 FIN 报文并返回 ACK 响应后的状态
CLOSING	采用非标准同步关闭连接时，在收到初始 FIN 报文并返回 ACK 响应之后，通信双方进入 CLOSING 状态。在收到对方返回的 FIN 报文的 ACK 响应后，通信双方进入 TIME-WAIT 状态

防火墙的主要技术——状态检测

□ 状态检测工作原理

- 状态检测技术根据连接的“状态”进行检查，当一个连接的初始数据报文到达执行状态检测的防火墙时，需要经过3个步骤：
 - 步骤1：当一个连接被建立时，防火墙会创建一个状态表来跟踪该连接的所有请求和响应信息。
 - 步骤2：当接收到数据包后，首先查看状态表，判断该包是否属于当前合法连接，若是，则接收该包让其通过，否则进入步骤3。
 - 步骤3：在过滤规则表中遍历，如不允许该数据包通过，则直接丢弃该包，跳回步骤2处理后续数据包；若允许该数据包通过，则进入步骤4。
 - 步骤4：在状态表中加入该新连接条目，并允许数据包通过。跳回步骤2处理后续数据包。

➤ 状态检测
处理流程



二、防火墙的主要技术

2.3 代理服务技术

防火墙的主要技术——代理技术

□ 代理技术简介

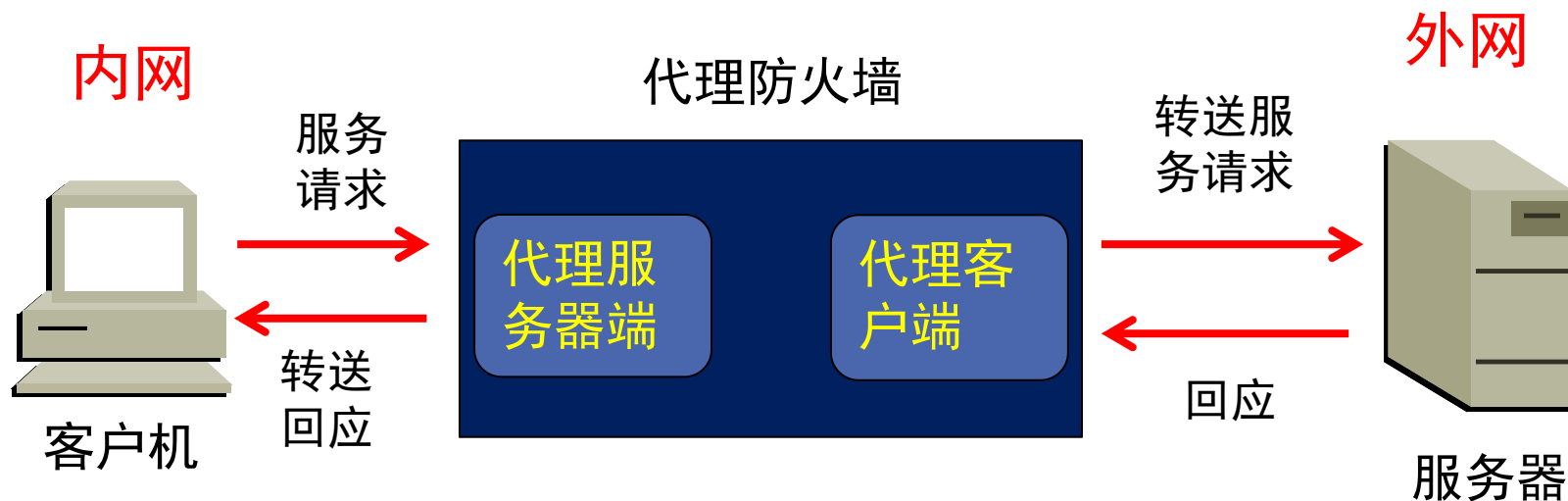
- 代理（Proxy）服务技术，也称为应用层代理或应用网关技术，与包过滤技术完全不同，是基于另一种思想的安全控制技术。
- 代理服务，就是将所有进入的请求都转发到代理服务器，代理服务器将检查单个请求，确保其符合安全策略，然后将其传递给目标服务器。
- 采用代理技术的代理服务器运行在内部网络和外部网络之间，在应用层实现安全控制功能，起到内部网络与外部网络之间应用服务的转接作用。

防火墙的主要技术——代理技术

□ 代理技术的工作原理

- 代理防火墙具有传统的代理服务器和防火墙的双重功能。它位于客户机与服务器之间，完全阻挡了二者间的直接数据交流。
- 当外部主机尝试与内部主机通信时，代理防火墙会先接受来自外部主机的请求，然后以自己的身份（即代理服务器的身份）与内部主机建立连接，获取所需资源后再返回给外部主机。
- 通过这种方式，代理防火墙实现了对通信内容的全面监控和过滤。

防火墙的主要技术——代理技术



基于代理技术实现防火墙的应用层控制

防火墙的主要技术——代理技术

□ 代理技术的主要功能

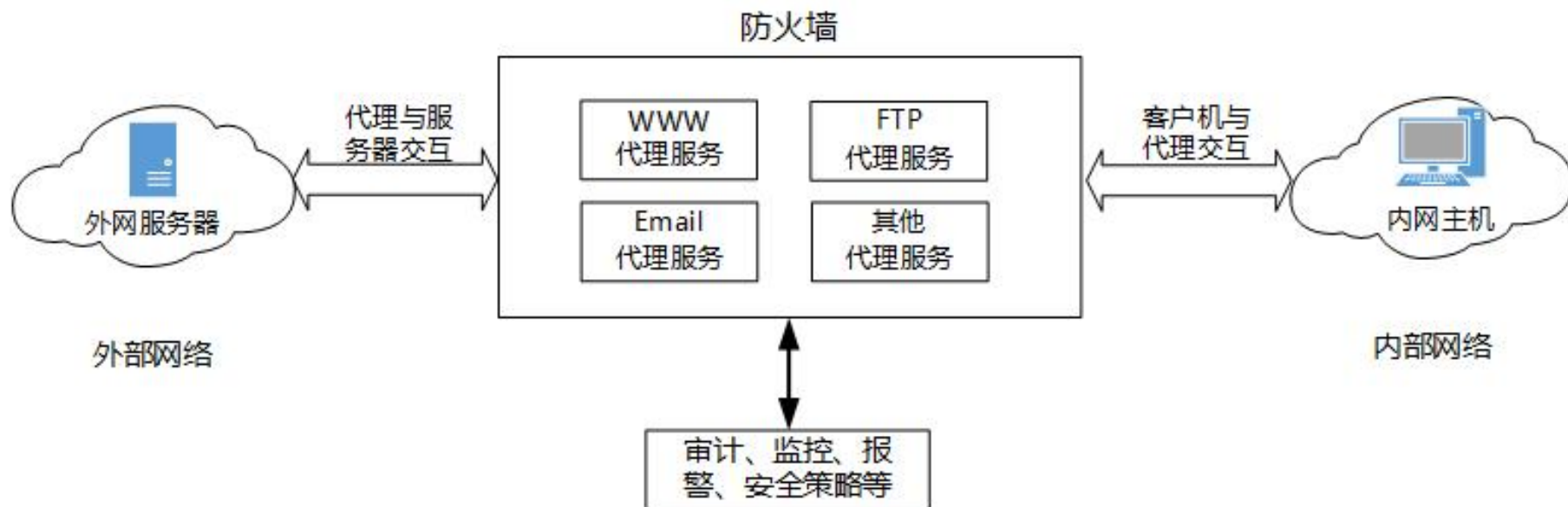
- **隐藏内部主机**：外部主机无法直接连接到内部主机，只能访问到代理服务器，从而保证内部网络中主机免受攻击。
- **深度解析与检查**：应用层代理能够深入解析和检查应用层协议数据，如HTTP、FTP、SMTP等，提供更精细化的安全防护。它不仅可以阻止不合规的数据包通过，还可以对通过它的**应用层内容**进行深度检查和处理。
- **数据内容进行过滤和审查**：通过检测和阻止恶意应用层协议的传输，防范网络攻击和数据泄露。同时，应用层代理还可以对数据内容进行过滤和审查，防止传输敏感信息或携带恶意代码的数据包进入内部网络。

防火墙的主要技术——代理技术

□ 代理技术的主要功能

- **合规性监控：**监控应用层通信内容，确保网络通信符合法律法规和企业政策。管理员可以根据需要定义允许或拒绝特定应用层协议的通信。
- **资源管理：**控制网络带宽的使用，优化网络资源的分配和利用。部分应用层代理还具有缓存功能，可以暂存经常访问的网络资源，提高网络访问速度和性能。

防火墙的主要技术——代理技术



基于代理技术实现防火墙的应用层控制

二、防火墙的主要技术

2.4 网络地址转换 (NAT)

防火墙的关键技术—— NAT技术

□ NAT技术简介

- 网络地址转换（Network Address Translation, NAT），是一种将私有IP地址转换为公有IP地址的技术。
- NAT的基本思想是在内部网络（使用私有IP地址）和外部网络（使用全球唯一的公有IP地址）之间建立一个IP地址映射关系，从而使得内部网络中的设备能够共享一个或少数几个公有IP地址来访问外部网络，以缓解IP地址短缺的问题。
- 防火墙应用：通过隐藏内部网络的真实IP地址，使内部网络免受黑客的直接攻击。
- 优点：增强了内部网络的安全性，并允许多个内部设备共享一个公共IP地址访问互联网。

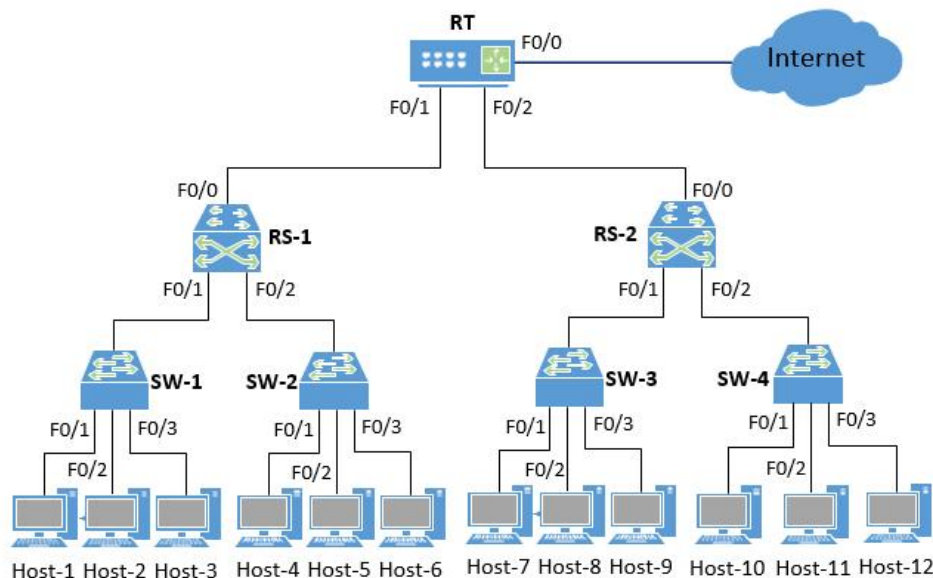
防火墙的关键技术—— NAT技术

□ NAT举例：

- 当一个企业分配到的IP地址少于内部主机数量时，如何实现内部局域网（多台计算机）接入互联网？

□ 做法：

- 内部网使用私有IP地址，通过网络地址转换（NAT），接入互联网。（具有私有IP地址的主机无法直接访问互联网）



防火墙的关键技术—— NAT技术

□ 回忆：私有IP地址

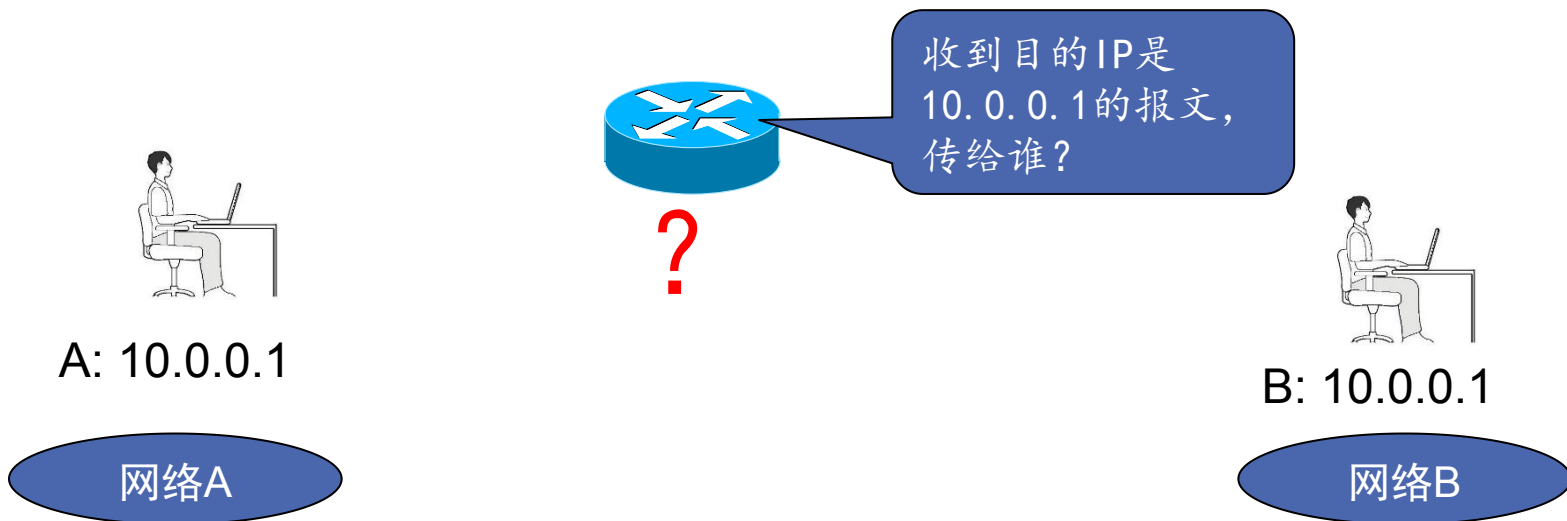
- 根据TCP/IP的规定，有一部分IP地址专门保留给使用TCP/IP协议的内部网络使用的，又称为“私有IP地址”。
 - 内部网络由于不接入互联网，因而网络管理者可以使用任意的IP地址，只要内部主机相互之间IP不重复即可。之所以保留专门的私有IP地址供其使用，其目的是为了避免内部网络以后接入互联网时引起地址混乱。

地址类型	私有地址范围	网络个数
A类	10.0.0.0 ~ 10.255.255.255	1个A
B类	172.16.0.0 ~ 172.31.255.255	16个B
C类	192.168.0.0 ~ 192.168.255.255	256个C

防火墙的关键技术—— NAT技术

□ 内部网络接入互联网时面临的问题

- 根据规定，所有以私有地址为目标地址的数据包，都不能被互联网上的路由器所转发，以防止在Internet上出现IP地址冲突。



防火墙的关键技术—— NAT技术

□ NAT的基本工作原理

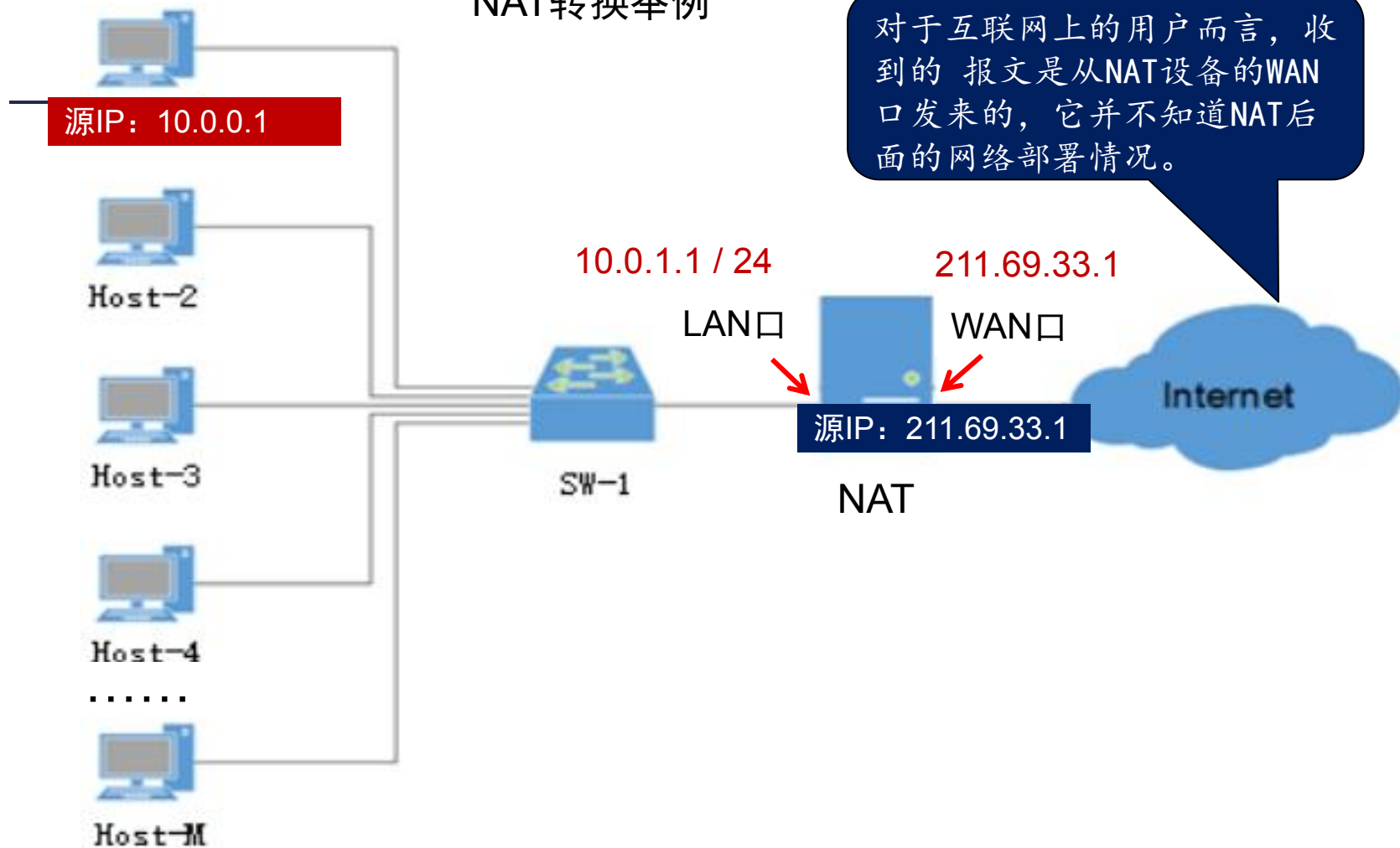
1. **检查源IP地址：**当内部网络中的主机（配置私有IP地址）访问外部网络（如互联网）时，NAT设备（通常是部署在内部网边界处的路由器或防火墙，）收到内部主机发送的数据包后，会检查数据包的**源IP地址**（即私有IP地址）。
2. **地址转换：**根据NAT设备配置的地址转换规则，NAT设备将数据包的源IP地址转换为公有IP地址。这个转换过程可能是一对一的映射（静态NAT），也可能是动态分配（动态NAT）或端口多路复用（NAPT/PAT）。
3. **会话建立：**转换后的数据包通过NAT设备发送到外部网络。此时，NAT设备会记录这个转换的映射关系，以便在外部网络**响应**时，能够正确地将数据包返回给内部网络的设备。

防火墙的关键技术—— NAT技术

□ NAT的基本工作原理

4. **外部网络响应：**外部网络的主机或服务器接收到数据包后，会向数据包的源IP地址（即NAT设备转换后的公有IP地址）发送响应。
5. **NAT设备转换响应报文：**响应数据包到达NAT设备后，NAT设备根据之前记录的映射关系，将目的IP地址（和端口号）从公有IP地址（和端口号）转换回内部网络的私有IP地址（和端口号）。
6. **NAT设备转发响应报文：**NAT设备将转换后的响应数据包发送到内部网络的设备。。

NAT转换举例



防火墙的关键技术—— NAT技术

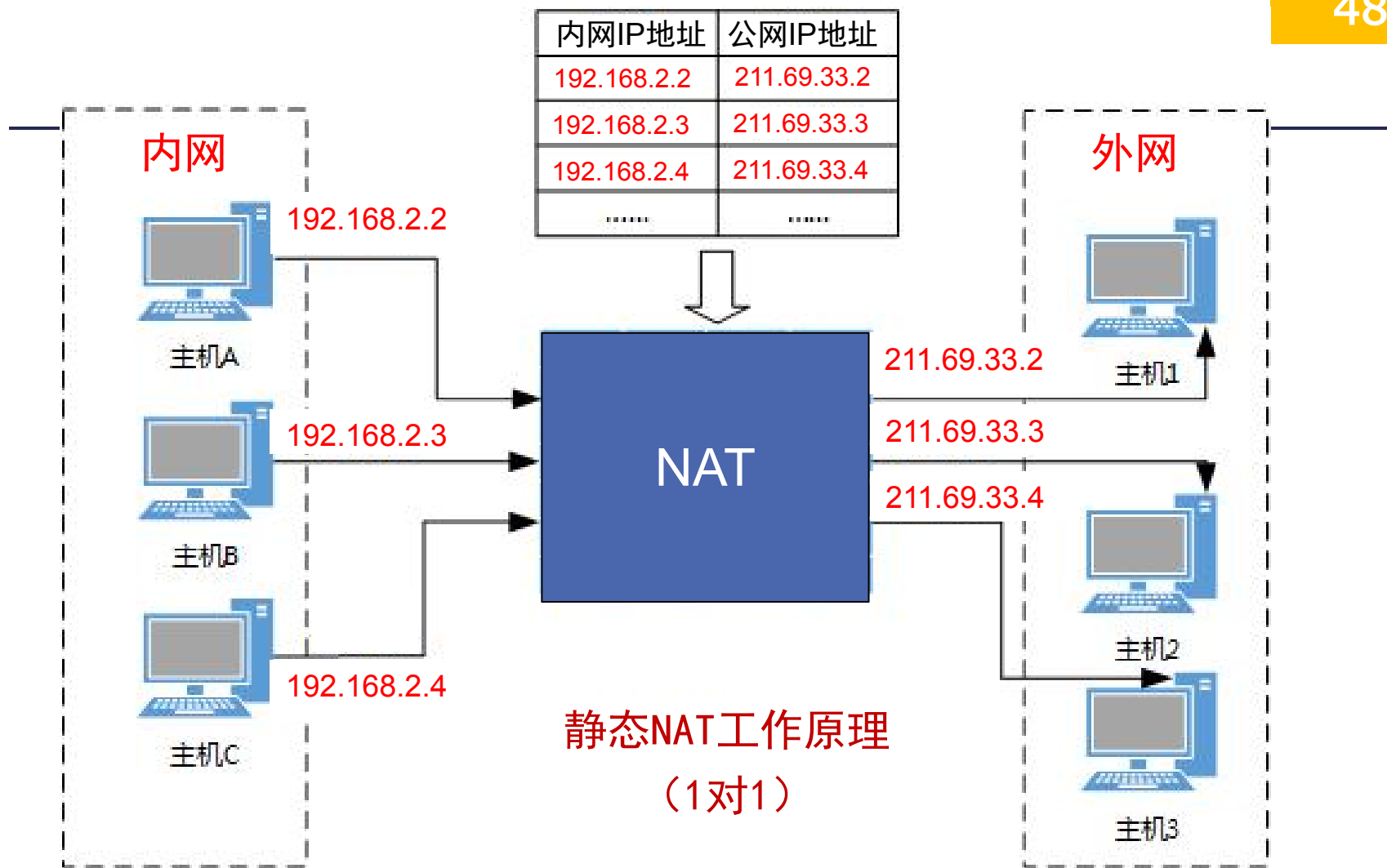
□ NAT主要有三种类型

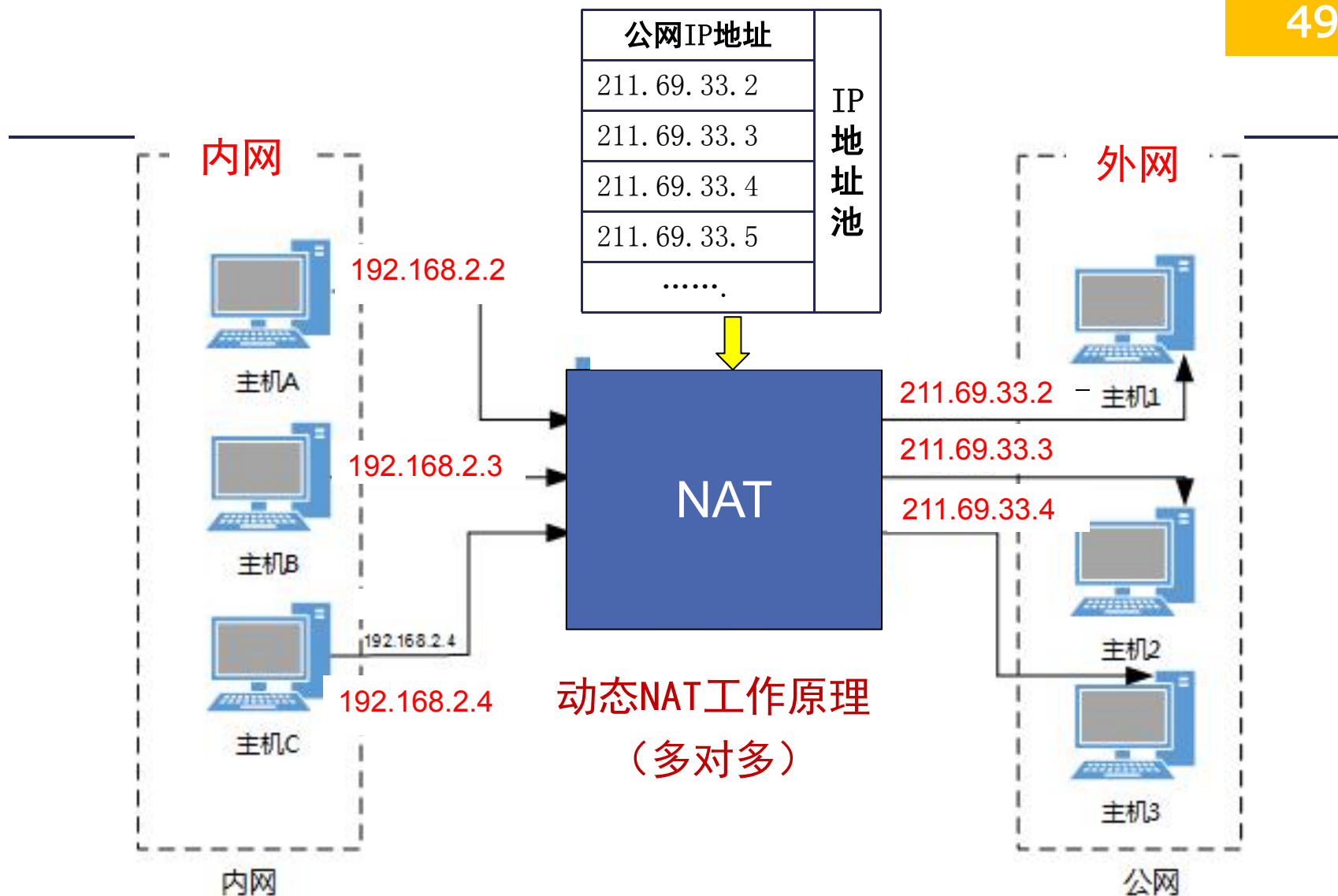
1. **静态NAT (Static NAT)**：一对一映射，将内部网络中的一个私有IP地址永久性地映射到外部网络上的一个公共IP地址。这种映射关系在配置后不会改变，除非管理员手动更改。
2. **动态NAT (Dynamic NAT)**：多对多映射，将内部网络中的多个私有IP地址映射到外部网络上的一个地址池中的公共IP地址。当一个内部设备需要访问外部网络时，NAT设备会从地址池中分配一个公共IP地址给它，当会话结束时，这个公共IP地址会被释放回地址池，供其他内部设备使用。

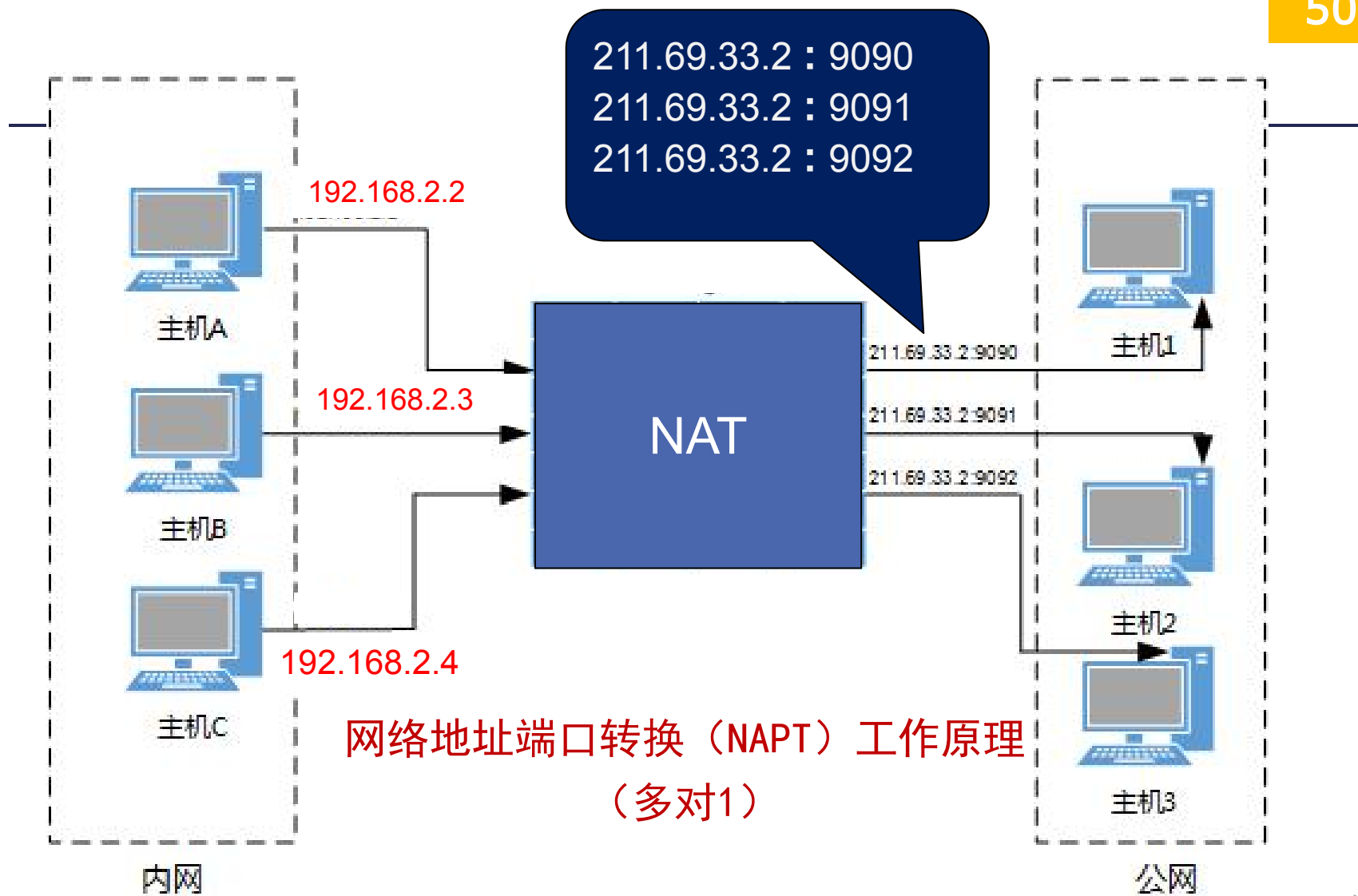
防火墙的关键技术—— NAT技术

□ NAT主要有三种类型

3. PAT (Port Address Translation, 端口地址转换) : 也称为NAPT (Network Address Port Translation, 网络地址端口转换), 是动态NAT的一种扩展, 允许多个内部设备共享同一个公共IP地址 (多对一)。它通过修改TCP/UDP端口号来实现这一点, 每个内部会话都会分配一个唯一的端口号, 这样即使它们共享同一个公共IP地址, 也可以同时与外部设备进行通信。







防火墙的关键技术—— NAT技术

□ 防火墙中的NAT技术

- 通过NAT，既可以实现内部网络接入互联网，同时，外部用户只能知道NAT设备的地址（WAN接口地址），无法知道内部网络的具体情况，更不能直接访问内部网络，因此提高了内部网络的安全性。
- 正是NAT技术的这种特性，使NAT技术成为了防火墙实现中经常采用的技术之一。

二、防火墙的主要技术

2.5 其他防火墙技术

防火墙的主要技术——其他技术

□ 复合式防火墙(Hybrid Firewall)

- 复合式防火墙结合了包过滤技术和代理服务技术，它能够根据数据包的内容和会话信息进行过滤和转发。
- 复合式防火墙通常包括两个主要组件：一个是包过滤引擎，另一个是代理服务引擎。这种防火墙可以提供更高级别的安全性和灵活性，但配置和管理相对复杂。

防火墙的主要技术——其他技术

□ 分布式防火墙

- 分布式防火墙将防火墙功能分布到网络中的多个位置，如网络边界、服务器和桌面系统等这样可以提供更全面的保护，并减轻单一设备的负载。分布式防火墙的优点是可以更好地应对复杂的网络攻击和威胁。但它的配置和管理可能比集中式防火墙更为复杂。

防火墙的主要技术——其他技术

□ 智能型防火墙

- 智能型防火墙是一种先进的防火墙技术，它结合了传统的包过滤、应用级网关、代理服务等技术，并加入了人工智能和机器学习算法。智能型防火墙可以自动识别和分类数据流量，并根据历史数据预测潜在的威胁和攻击。这样可以更好地保护网络安全和数据隐私。

防火墙的主要技术——其他技术

□ 入侵检测和防御（IDS/IPS）

- 定义：现代防火墙往往集成了入侵检测和防御功能。
- 原理：通过分析网络流量，识别潜在的恶意行为，并自动采取措施（如阻断连接）来防止攻击。
- 优点：提供了实时的安全监测和响应能力，能够及时发现并阻止网络攻击。

三、防火墙应用——安全区域

防火墙的安全区域

□ 设置防火墙安全区域的目的

- 在网络安全的应用中，如果网络安全设备对所有报文都进行逐包检测，会导致设备资源的大量消耗和性能的急剧下降。而这种对所有报文都进行检查的机制也是没有必要的。所以在网络安全领域出现了基于安全区域的报文检测机制。

防火墙的安全区域

□ 什么是安全区域？

- 安全区域（Security Zone），或者简称为区域（Zone），是防火墙所引入的一个安全概念，大部分的安全策略都基于安全区域实施。
- 引入安全区域的概念之后，网络管理员可以将具有相同优先级的网络设备划入同一个安全区域。由于同一安全区域内的网络设备是“同样安全”的，FW认为在同一安全区域内部发生的数据流动是不存在安全风险的，不需要实施任何安全策略。
- 只有当不同安全区域之间发生数据流动时，才会触发设备的安全检查，并实施相应的安全策略。

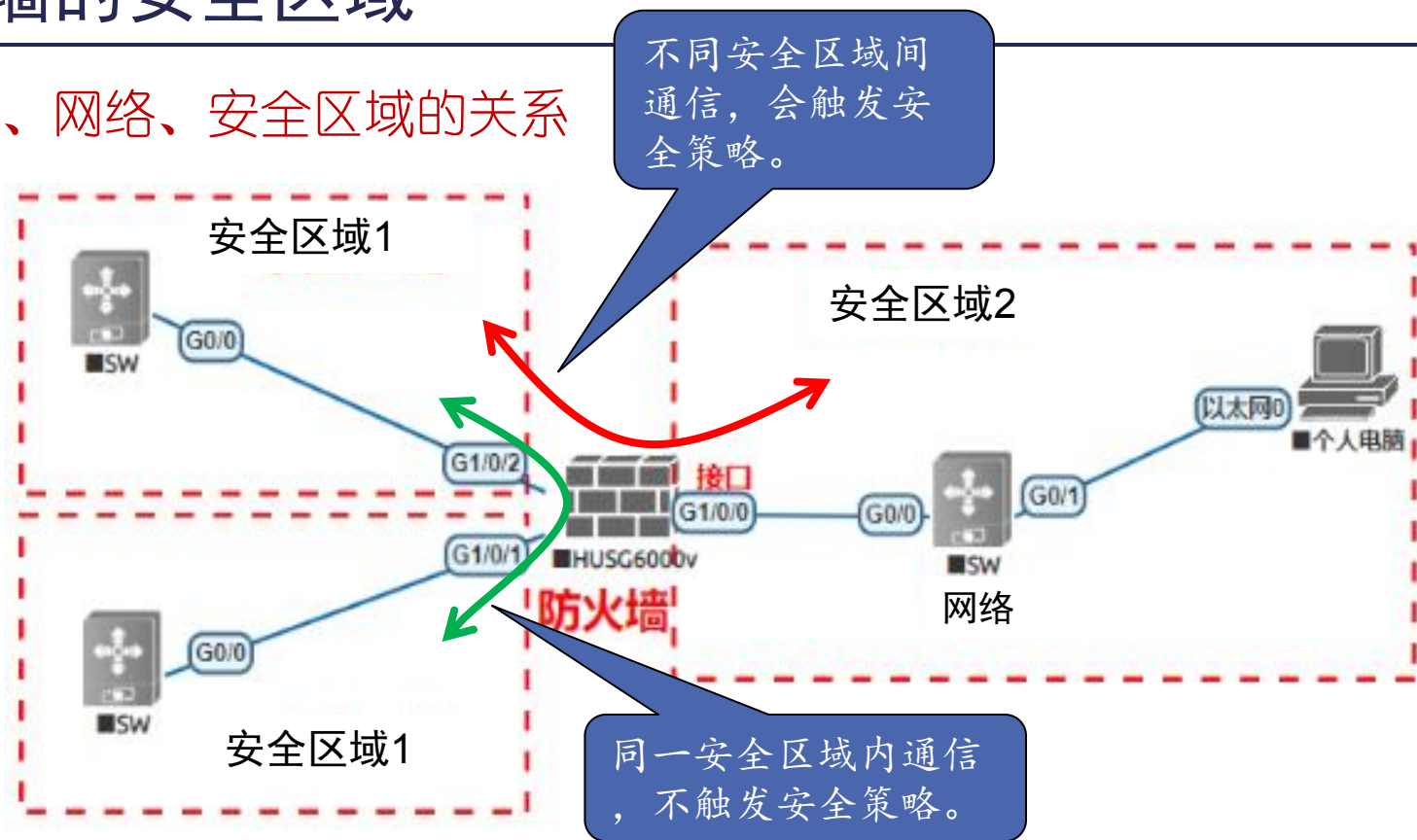
防火墙的安全区域

□ 防火墙接口、网络、安全区域的关系

- 防火墙通过安全区域来划分网络、标识报文流动的路线。例如，报文从安全区域A发往安全区域B。
- 默认情况下，华为防火墙报文在不同的安全区域之间流动时受到控制，在同一安全区域内流动不受控制。同时也支持同一安全区域内流动的报文控制。
- 防火墙通过接口来连接网络，在华为防火墙上，一个接口只能加入到一个安全区域中。将接口划分到安全区域后，通过接口就能把安全区域和网络关联起来。可以理解为：一个安全区域是若干接口所连网络的集合，这些网络中的用户具有相同的安全属性。

防火墙的安全区域

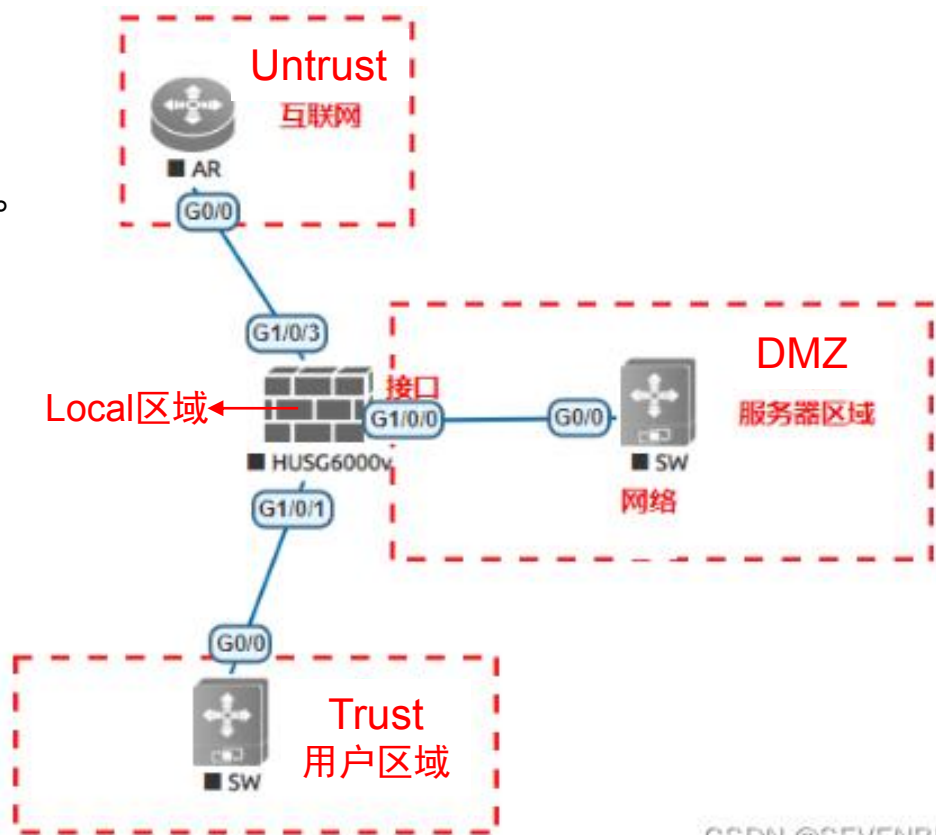
□ 接口、网络、安全区域的关系



防火墙的安全区域

□ 防火墙默认的安全区域

- Trust区域：受信任程度高，通常用来定义内部用户所在的网络。
- Untrust区域：不受信任的网络。通常用来定义Internet等不安全的网络。
- DMZ区域：网络的受信任程度中等，通常用来定义内部服务器所在的网络（既能被内部访问，也能被外部访问）。



防火墙的安全区域

□ 默认的安全区域—— 防火墙的Local区域

- 除了在不同网络之间流动的报文之外，还存在从某个网络到达防火墙本身的报文，例如登录防火墙进行配置，以及防火墙本身发出的报文。如何标识这类报文的路线？
- 华为防火墙提供Local区域，代表防火墙本身。凡是由防火墙主动发出的报文均可认为是从Local区域发出。凡是需要防火墙进行响应并处理（而不是转发）的报文均可认为是Local区域接收。
- 关于Local区域，该区域不能添加任何接口，但防火墙所有接口本身都隐含属于Local区域，也就是说，报文通过防火墙某接口去往某个网络时，目的安全区域是该接口所在的安全区域；报文通过接口到达防火墙本身时，目的区域是Local区域。

防火墙的安全区域

□ 报文在安全区域之间流动方向

■ 问题：用安全区域来表示网络后，怎么判断一个安全区域的受信程度？

- 在华为防火墙上，每个安全区域都有1个表示安全级别的ID，用1-100数字表示，数字越大，越可信。
- 默认安全区域的安全级别ID是：Local (100)，Trust (85)，DMZ (50)，Untrust (5)

■ 华为防火墙规定：

- 报文从低级别的安全区域向高级别的安全区域流动时为入方向（Inbound）
- 报文从高级别区域向低级别区域流动时为出方向（Outbound）

防火墙的安全区域

□ 防火墙如何判断报文在哪两个安全区域之间流动？

- 确定源安全区域很容易，防火墙从哪个接口接收报文，该接口所属的安全区域就是源安全区域。
- 路由模式下，防火墙通过查找路由表确定报文从哪个接口转发出去，该接口所属区域就是目的安全区域。
- 交换模式下，防火墙通过查找MAC地址表转发确定报文从哪个接口发出，该接口所属区域就是目的安全区域。
- VPN场景中，防火墙收到封装报文，解封装后得到原始报文，通过查找路由表确定报文从哪个接口转发，该接口所属区域就是目的安全区域

防火墙的安全区域

□ 安全区域配置

■ 案例1：创建自定义安全区域（包括3步操作）：

- 创建自定义安全区域
- 设置新创建安全区域的安全级别
- 将指定接口G1/0/0加入该安全区域

■ 举例1，创建安全区域SecA，包含GE1/0/0接口，安全级别是10

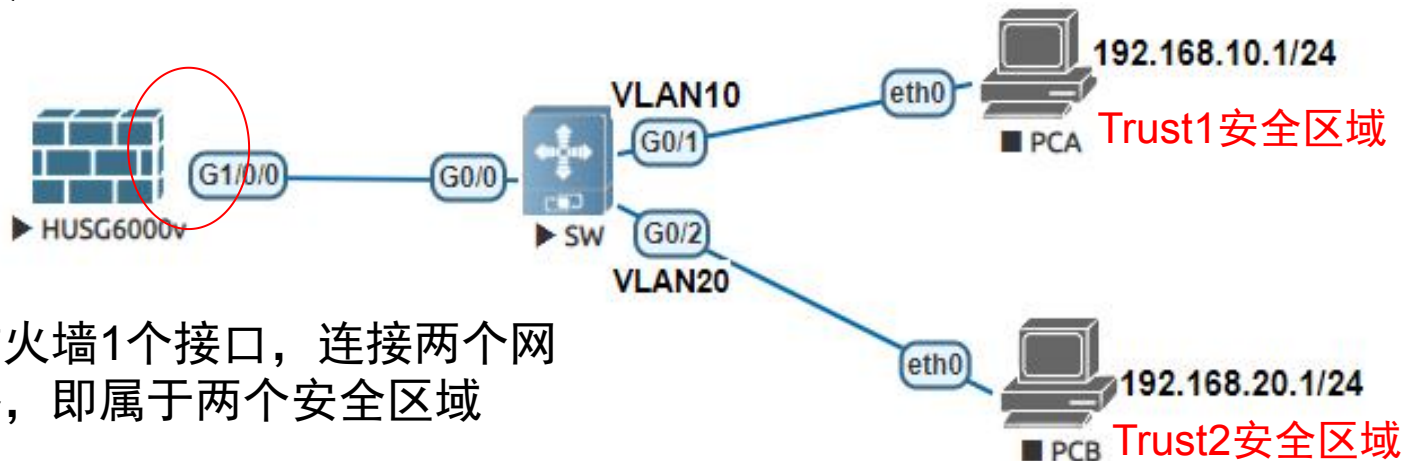
```
[FW1]firewall zone name SecA // 创建安全区域SecA
[FW1-zone-SecA]set priority 10 // 将安全级别设置为10
[FW1-zone-SecA]add interface GigabitEthernet 1/0/0 // 将接口G1/0/0加入安全区域
```

防火墙的安全区域

安全区域配置

案例2：将逻辑接口接入安全区域

- 华为防火墙支持物理接口接入安全区域，还支持逻辑接口，例如子接口、VLANIF接口



防火墙1个接口，连接两个网络，即属于两个安全区域

防火墙的安全区域

□ 安全区域配置

■ 举例2：子接口接入安全区域

- 在接口G1/0/0创建两个子接口G1/0/0.1和G1/0/0.2，分别对应VLAN10和VLAN20，然后将两个子接口划分到不同安全区域。
- 完成上述配置，PC_A被划分到trust1区域，PC_B划分到trust2区域。

```
[FW1]interface GigabitEthernet 1/0/0.1  
[FW1-GigabitEthernet1/0/0.1]vlan-type dot1q 10  
[FW1-GigabitEthernet1/0/0.1]ip address 192.168.10.254 24
```

```
[FW1]interface GigabitEthernet 1/0/0.2  
[FW1-GigabitEthernet1/0/0.2]vlan-type dot1q 20  
[FW1-GigabitEthernet1/0/0.2]ip address 192.168.20.254 24
```

```
[FW1]firewall zone name trust1  
[FW1-zone-trust1]set priority 10  
[FW1-zone-trust1]add interface GigabitEthernet 0/0/0.1
```

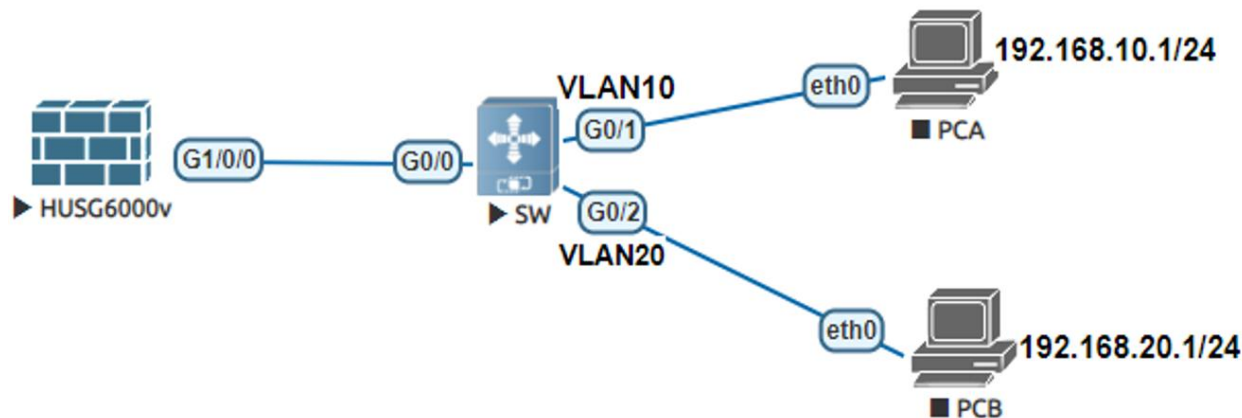
```
[FW1]firewall zone name trust2  
[FW1-zone-trust1]set priority 20  
[FW1-zone-trust1]add interface GigabitEthernet 0/0/0.2
```

防火墙的安全区域

安全区域配置

■ 举例3：VLANIF接入安全区域

➤ 假设防火墙采用透明接入，即G1/0/0接口没有配置IP地址。



防火墙的安全区域

□ 安全区域配置

■ 举例3：VLANIF接入安全区域

- 防火墙创建两个VLAN，配置VLANIF接口IP
- 配置G1/0/0接口工作在交换模式下（透明模式），并允许10和20VLAN报文通过。
- 将VLAN10和VLAN20划分到不同的安全区域。

```
[FW1]vlan batch 2 3
[FW1]interface vlan 2
[FW1-Vlanif2]ip add 1.1.1.1 24
[FW1]interface vlan 3
[FW1-Vlanif3]ip add 2.2.2.1 24
```

```
[FW1]interface g1/0/0
[FW1-GigabitEthernet1/0/0]portswitch //变为二层接口
[FW1-GigabitEthernet1/0/0]port link-type trunk
[FW1-GigabitEthernet1/0/0]port trunk allow-pass vlan 2 3
```

```
[FW1]firewall zone trust
[FW1-zone-trust]add interface vlanif 2
```

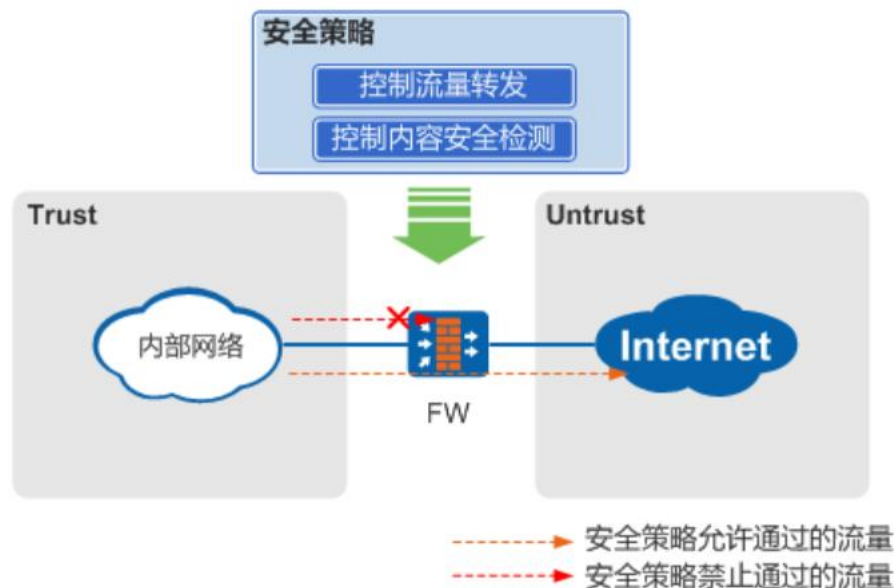
```
[FW1]firewall zone untrust
[FW1-zone-untrust]add interface vlanif 3
```

四、防火墙应用 —— 安全策略

防火墙 —— 安全策略

□ 安全策略：是控制防火墙对流量转发的策略

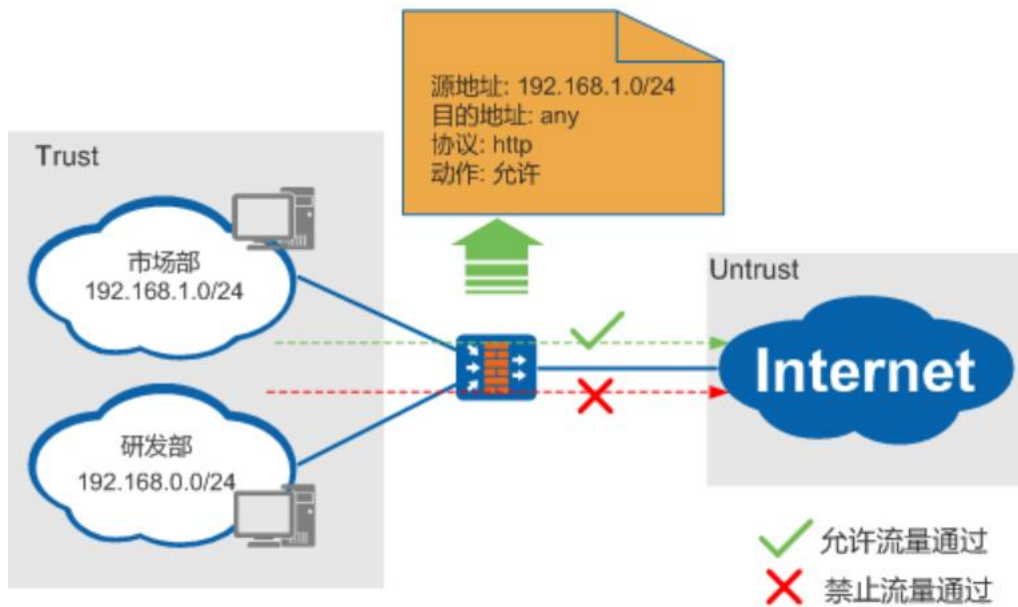
- 设备能够识别出流量的属性，并将流量的属性与安全策略的条件进行匹配。如果此流量成功匹配安全策略。FW将会执行安全策略的动作。
- 动作为“允许”：放行
- 动作为“禁止”：禁止流量通过。



防火墙 —— 安全策略

□ 举例1：传统防火墙的包过滤策略

- 传统防火墙根据五元组（源地址、目的地址、源端口、目的端口、协议类型）来控制流量在安全区域间的转发。



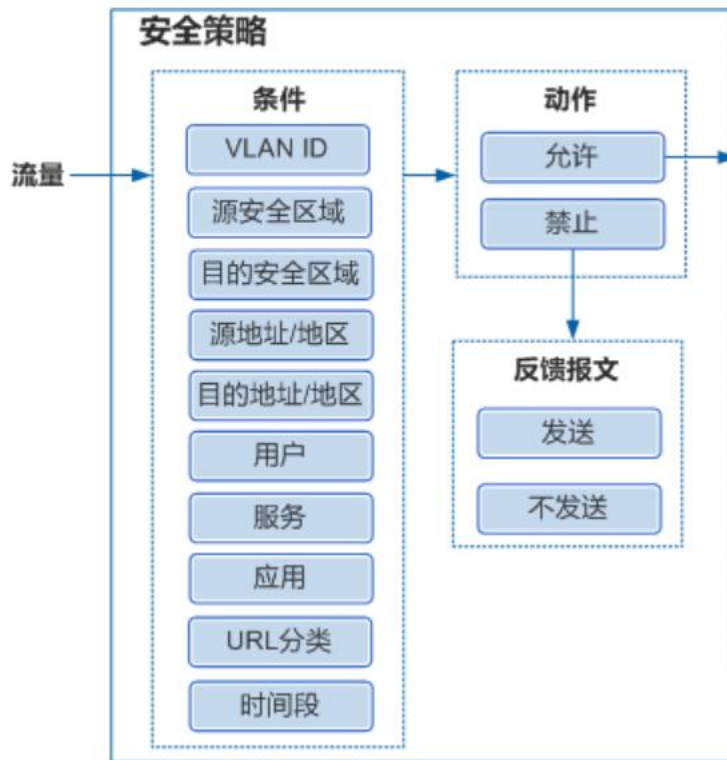
防火墙 —— 安全策略

□ 举例2：新型防火墙的安全策略

- 新型防火墙的安全策略不仅可以完全替代传统包过滤的功能，还进一步实现了基于用户、应用和内容的转发控制，实现更精确的管控。
 - 能够通过“用户”来区分不同部门的员工，使网络管理更加灵活。
 - 能够有效区分协议（例如HTTP）承载的不同应用（例如网页游戏等），使网络的管理更加精细。
 - 能够通过安全策略实现内容安全检测，阻断病毒、黑客等的入侵，更好的保护内部网络。

防火墙 —— 安全策略

□ 防火墙的安全策略处理流程



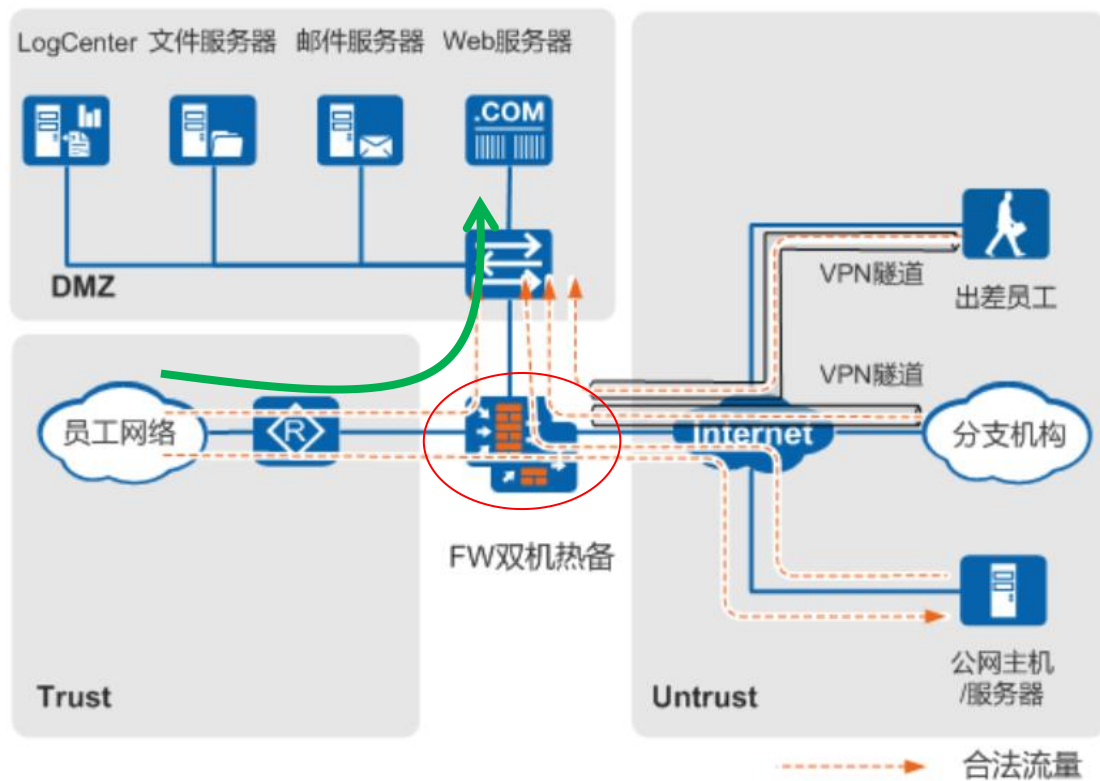
防火墙 —— 安全策略

□ 安全策略的应用场景

- 防火墙部署的场景不同，使用安全策略的侧重点也有所不同。
- FW主要部署场景包括：
 - 大中型企业边界防护
 - 内网管控与安全隔离
 - 数据中心边界防护。

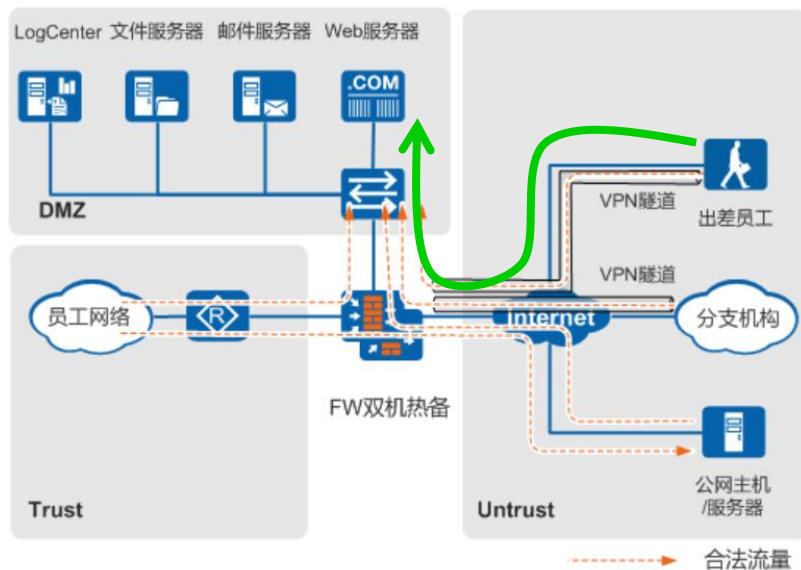
➤ 应用场景1 ——大中型企业边界防护

1. 公司将员工网络、服务器网络、外部网络划分到不同安全区域，通过安全策略对安全区域间的流量进行检测，保护公司内部网络。



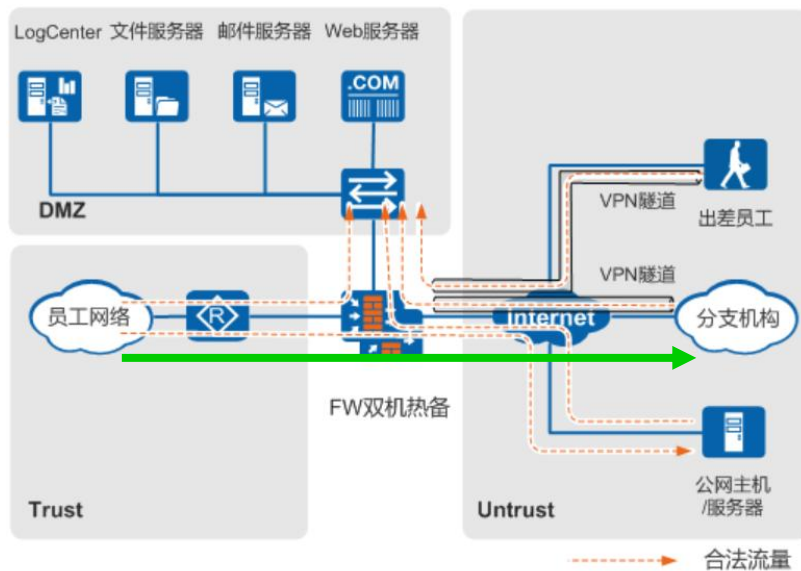
➤ 应用场景1 ——大中型企业边界防护

2. 根据公司对外提供的网络服务的类型配置安全策略功能。例如，针对图中的文件服务器开启文件过滤和内容过滤，并且针对所有服务器开启反病毒和入侵防御。



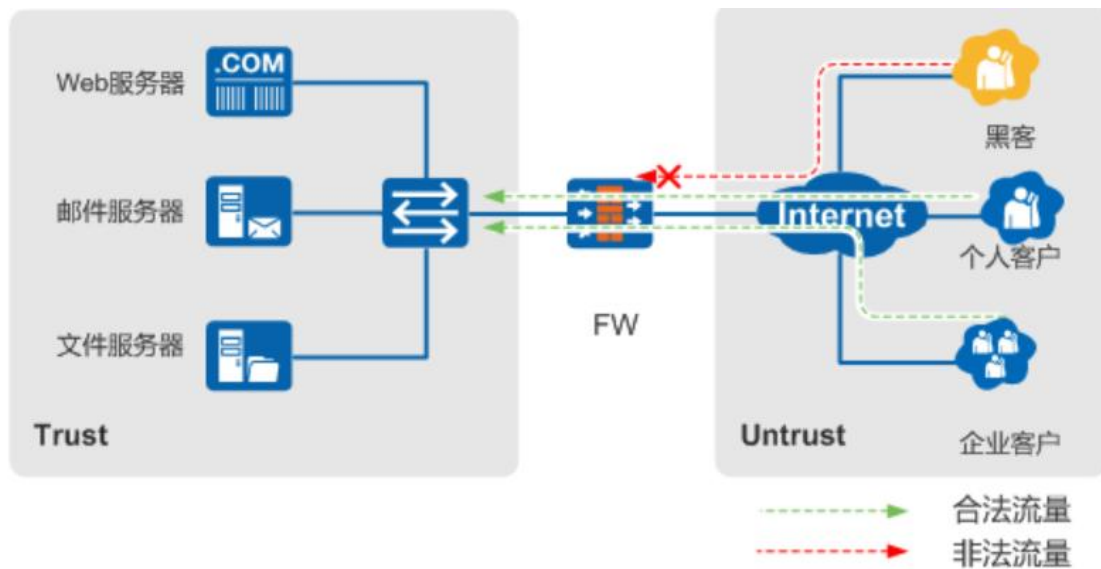
➤ 应用场景1 ——大中型企业边界防护

2. 根据公司对外提供的网络服务的类型配置安全策略功能。例如，针对图中的文件服务器开启文件过滤和内容过滤，并且针对所有服务器开启反病毒和入侵防御。
3. 针对内网员工访问外部网络的行为，配置URL过滤、DNS过滤、文件过滤、内容过滤等安全功能，既保护内网主机不受外网的威胁，又可以防止企业机密信息的泄露，提高企业网络的安全性。



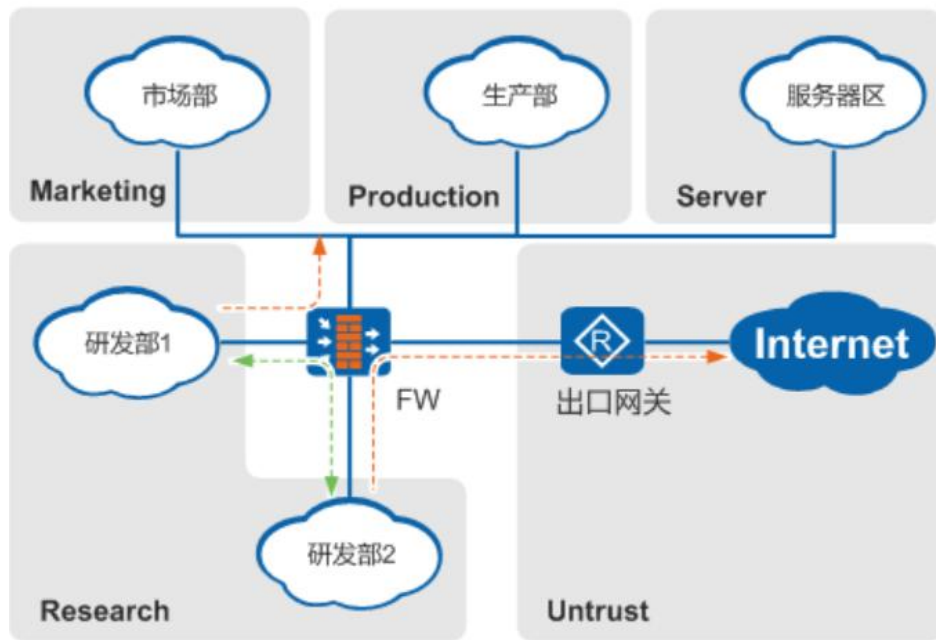
➤ 应用场景2 ——数据中心边界防护

控制Internet用户访问数据中心服务器的权限，包括：只允许访问特定的服务器，只开放服务器的特定端口，只允许用户使用特定应用程序访问服务器，根据用户级别不同允许访问的内容不同等



➤ 应用场景3 ——内网管控与安全隔离

- 不同安全等级的网络划分到不同的安全区域，相互之间的通信可根据业务需求配置不同的安全策略。例如仅允许部分研发部的主机访问指定的市场部主机。
- 在内网各个区域与外网之间配置安全策略，包括能访问外网的部门、DNS过滤、内容过滤、URL过滤、应用行为控制等功能。



此处的Marketing、Production、Server、Research是自定义安全区域

——> 区域间流量
——> 区域内流量

防火墙 —— 安全策略

□ 安全策略的匹配规则

1. 每条策略中都包含了多个匹配条件，如安全区域、用户、应用等。各个匹配条件之间是“与”的关系，报文的属性与各个条件必须全部匹配，才认为该报文匹配这条规则。缺省情况下所有的条件均为any，即所有流量均可以命中该策略。（例如，报文来源地址source-address是A网段、目的地址destination-address 是B网段）
2. 一个匹配条件中可以配置多个值，多个值之间是“或”的关系，报文的属性只要匹配任意一个值，就认为报文的属性匹配了这个条件。（例如，报文来源地址source-address是A网段、B网段、C网段）

防火墙 —— 安全策略

□ 安全策略的匹配规则

3. 系统默认存在一条缺省安全策略，如果不同安全区域间的流量没有匹配到管理员定义的安全策略，就会命中缺省安全策略（条件均为any，动作默认为禁止）。
4. 同一安全区域内传输的流量一般不受缺省安全策略控制，缺省转发动作为允许。
5. 如果配置了多条安全策略，会从上到下依次进行匹配。如果流量匹配了某个安全策略，将不再进行下一个策略的匹配。所以安全策略的配置**顺序很重要**，需要先配置条件精确的策略，再配置宽泛的策略。

➤ 举例：防火墙安全策略配置

//进入安全策略配置视图

```
[FW-1]security-policy
```

// 创建一条名为 abc 的安全策略，使得源地址是 192.168.64.0/21，目的地址是 172.16.1.11/32 的 DNS 服务都被允许通过（permit）。即允许 192.168.64.0/21 网段的主机能够访问 172.16.1.11（DNS 服务器）提供的 DNS 服务。

```
[FW-1-policy-security]rule name abc
```

```
[FW-1-policy-security-rule-abc]source-address 192.168.64.0 mask 21
```

```
[FW-1-policy-security-rule-abc]destination-address 172.16.100.11 32
```

```
[FW-1-policy-security-rule-abc]service dns
```

```
[FW-1-policy-security-rule-abc]action permit
```

```
[FW-1-policy-security-rule-abc]quit
```

五、防火墙应用 —— 部署方式

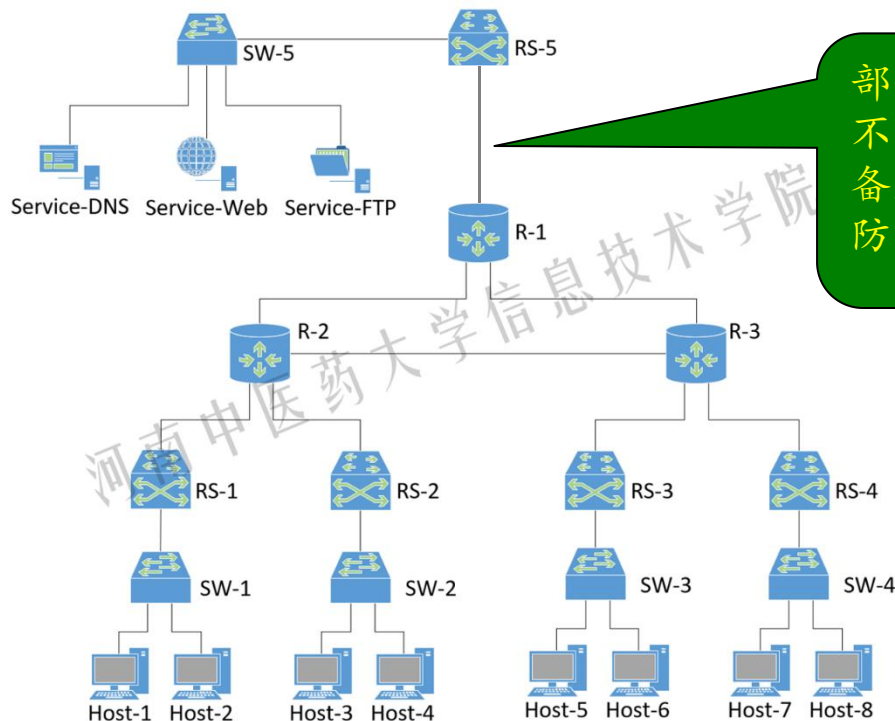
防火墙部署

- 透明方式
- 路由方式
- 旁挂方式

防火墙部署 —— 透明方式

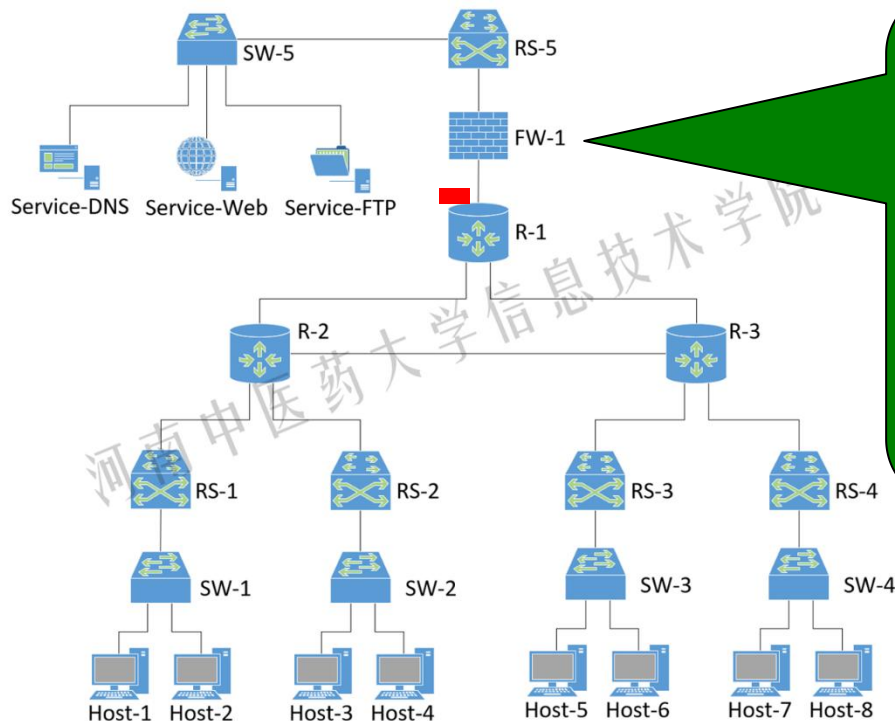
防火墙部署 —— 透明方式

□ 透明方式



防火墙部署 —— 透明方式

□ 透明方式



添加防火墙，但是RS-5和R-1的配置不变，防火墙仿佛是一座直通的“桥”，但它能通过安全策略控制访问，即过滤通过它的数据包。

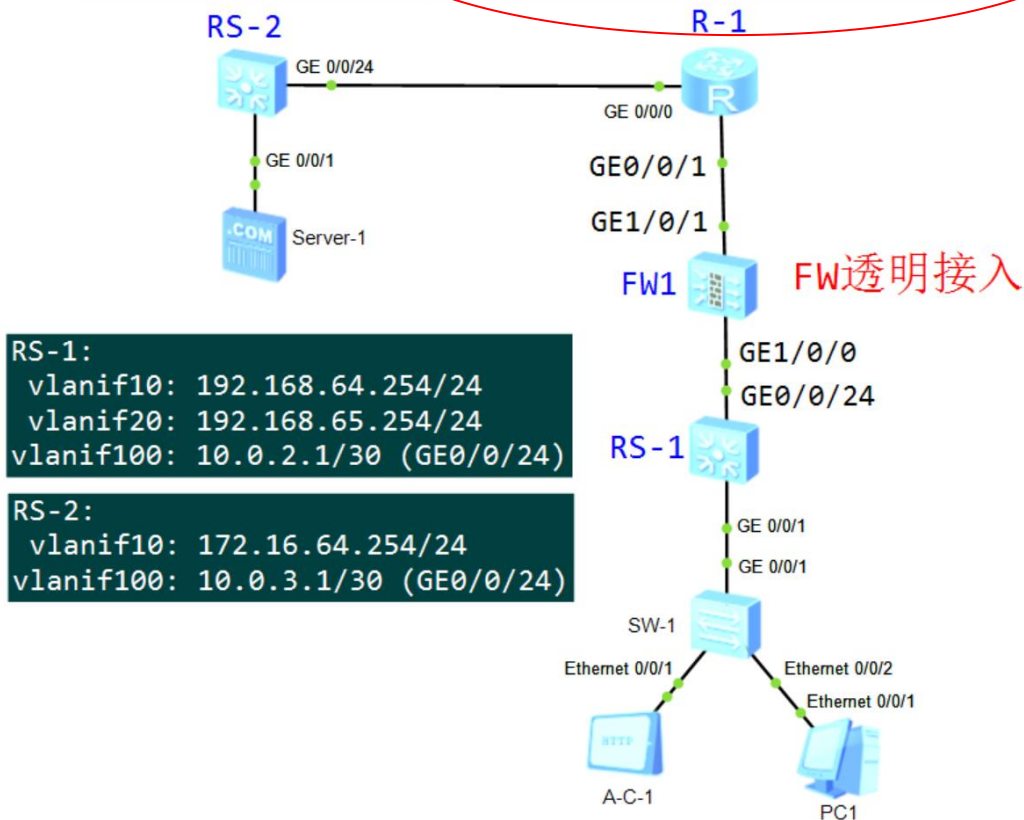
防火墙部署 —— 透明接入

□ 透明接入

- FW接口配置分析
- 上下行设备接口分析
- 路由配置

R-1:
GE0/0/0: 10.0.3.2/30
GE0/0/1: 10.0.2.2/30

FW-1: (portswitch)
GE1/0/0: 设置成二层接口 属于trust
GE1/0/1: 设置成二层接口 属于untrust



RS-1:
vlanif10: 192.168.64.254/24
vlanif20: 192.168.65.254/24
vlanif100: 10.0.2.1/30 (GE0/0/24)

RS-2:
vlanif10: 172.16.64.254/24
vlanif100: 10.0.3.1/30 (GE0/0/24)

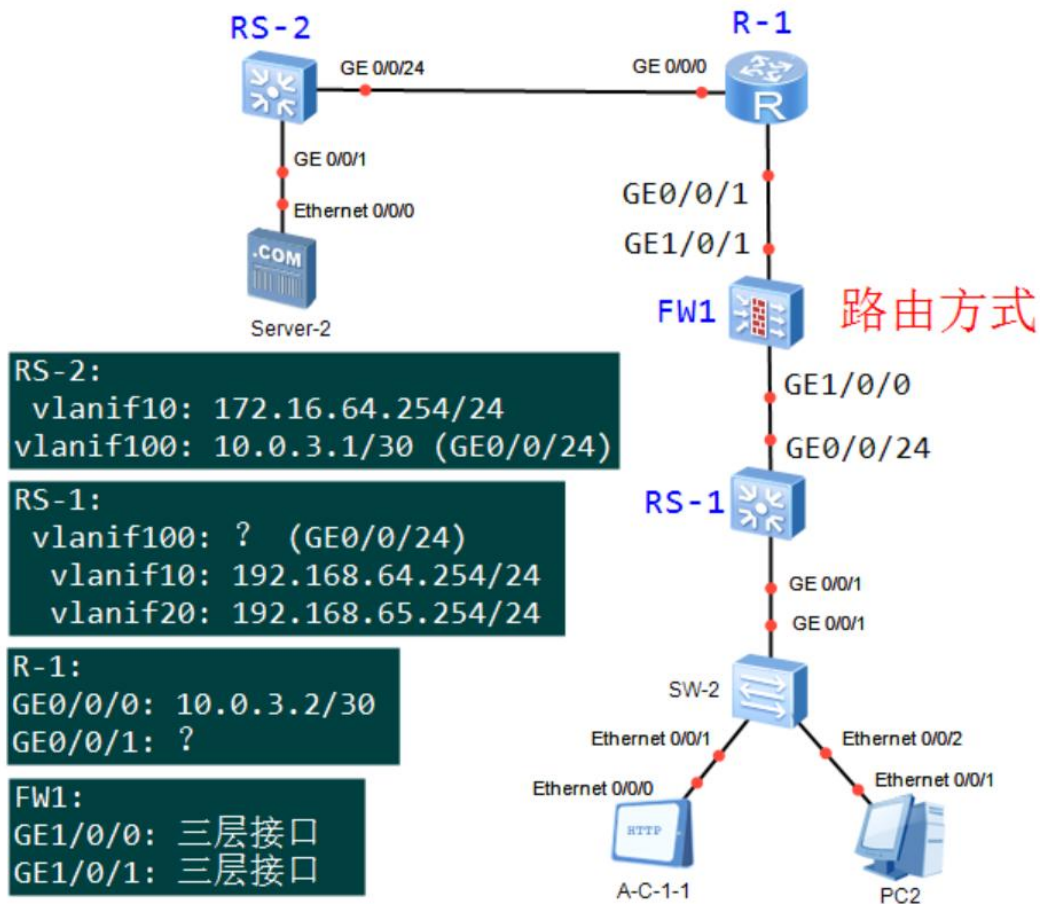
防火墙部署 —— 路由方式

防火墙部署 —— 路由方式

□ 路由方式

- FW接口配置分析
- 上下行设备接口分析
- 路由配置（OSPF区域）

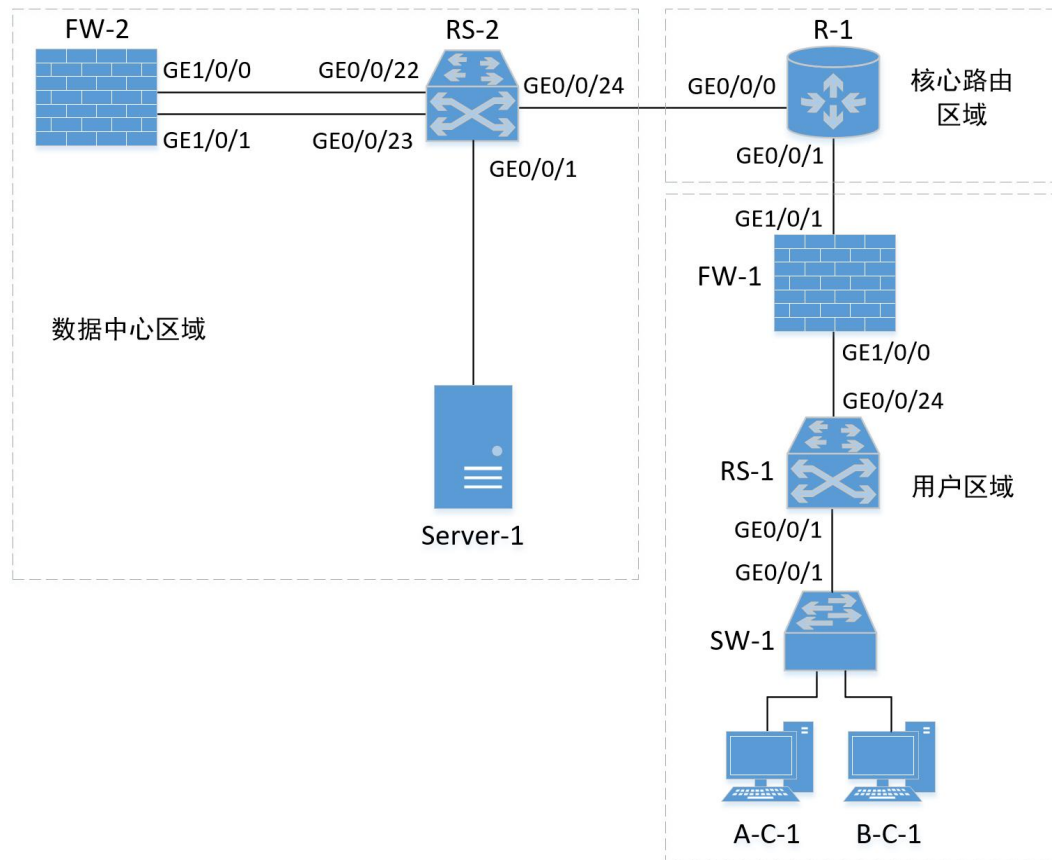
FW的上下接口需要配置IP地址，RS-1的下一跳变成FW1的GE1/0/0接口，R-1的下一跳变为FW1的GE1/0/1接口。FW1上也需要配置ospf



防火墙部署 —— 旁挂方式

防火墙部署 —— 旁挂方式

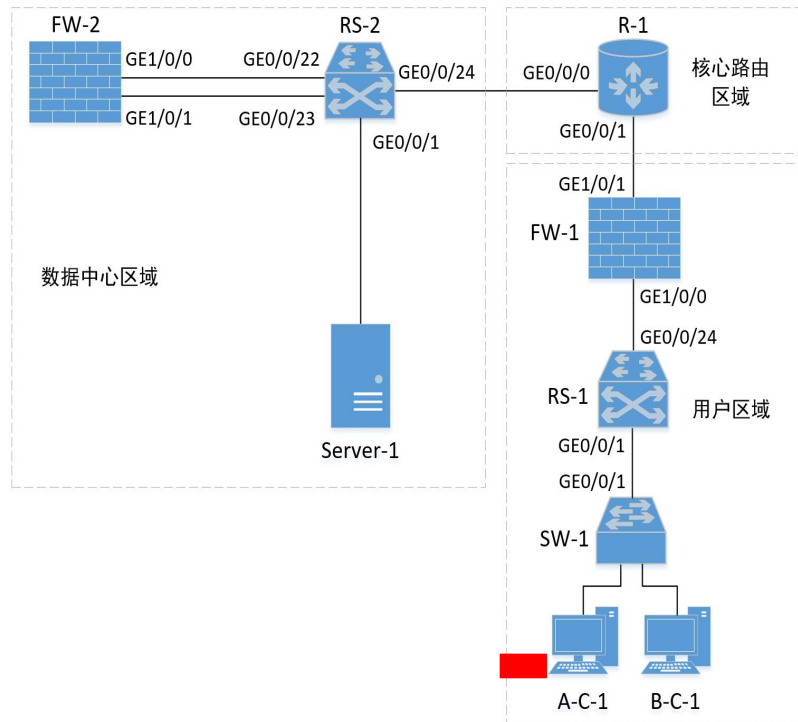
□ 防火墙旁挂



防火墙部署 —— 旁挂方式

□ 防火墙旁挂方式

- 不改变原有网络的拓扑结构；
- 通过RS-2的流量会被首先**引流到**旁挂的防火墙上进行安全策略检测，而不是直接转发至R-1或者Server-1。
- 只有安全策略允许通过的流量才会被防火墙发送回RS-2，然后进一步转发至目的地。
- 不允许通过防火墙的流量则在防火墙处被阻断。



第10讲 使用防火墙加强网络通信控制

(完)