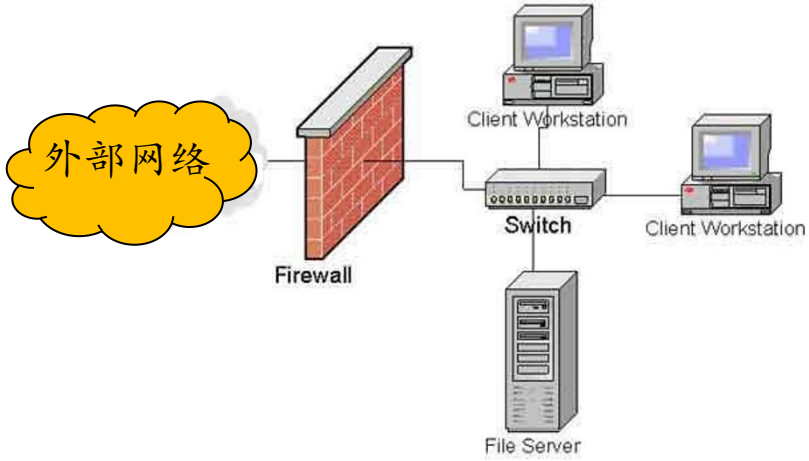
网络技术与信息安全

第6讲　使用防火墙加强网络安全

河南中医药大学信息技术学院

许成刚

一、认识防火墙


外部网络
Firewall
Client Workstation
Switch
Client Workstation
File Server

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

- 通过防火墙能实现什么？

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。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。
3. **网络地址转换（NAT）**：防火墙通常包含NAT功能，从而隐藏内部网络的真实结构，减少外网对内网的攻击。
4. **VPN支持**：许多防火墙还支持虚拟专用网络（VPN）技术，允许互联网远程用户通过加密通道安全地访问内部网络资源。

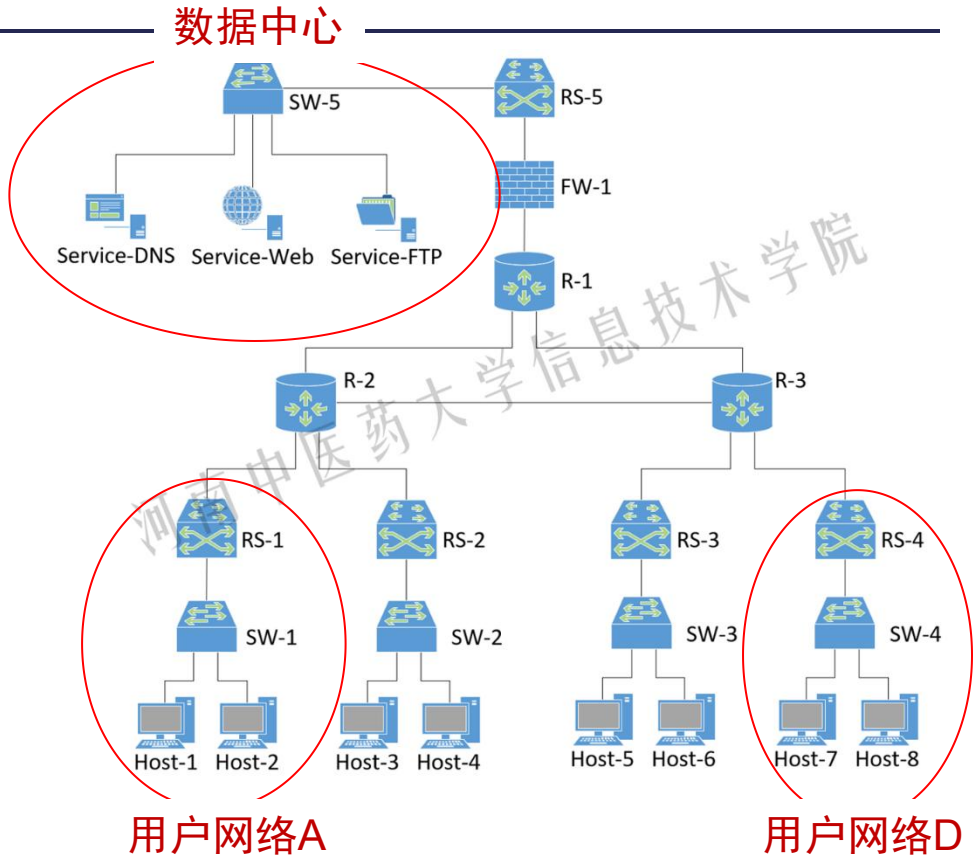
认识防火墙

- 防火墙能做什么？

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。
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，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. **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）。否则报文会被丢弃。

➢ 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访问Web服务
  3. 不允许网络A中的主机以ping命令方式访问数据中心的服务器
  4. ……



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

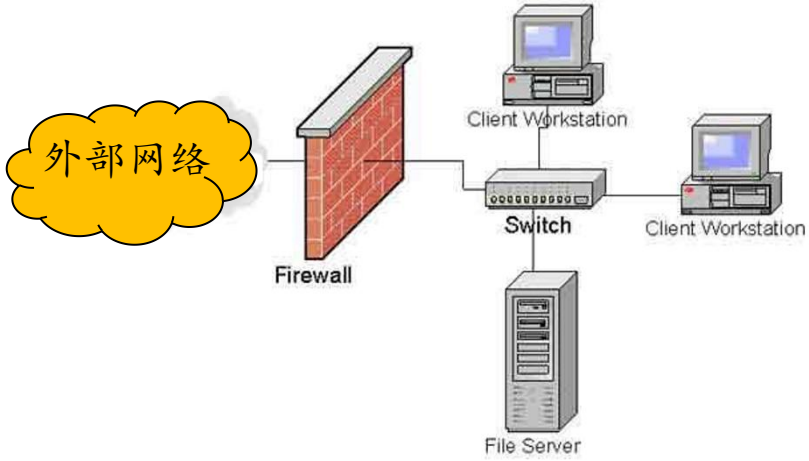
- 按防火墙的保护对象划分：
  - 单机防火墙
    - 单机防火墙的设计目的是为了保护单台主机网络访问操作的安全，一般是以装载到受保护主机硬盘里的软件程序的形式存在的。
  - 网络防火墙
    - 网络防火墙的设计目的是为了保护相应网络的安全，一般采用软件与硬件相结合的形式，也有纯软件的网络防火墙存在。

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、包过滤防火墙的基本原理



包过滤防火墙的基本工作原理

包过滤技术简介

- 包过滤技术是防火墙最基本的技术之一，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

包过滤防火墙的基本工作原理

- 网络层首部：过滤IP数据报首部字段

包过滤防火墙的基本工作原理

- **运输层首部：**过滤TCP报文段首部字段

➢ 举例：在防火墙中设置数据包过滤规则

- 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。
  - 防火墙对收到的数据包进行分析，若数据包首部中的地址符合该策略条件，则允许该数据包通过防火墙

```
[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规则视图中配置具体规则。

包过滤防火墙的基本工作原理

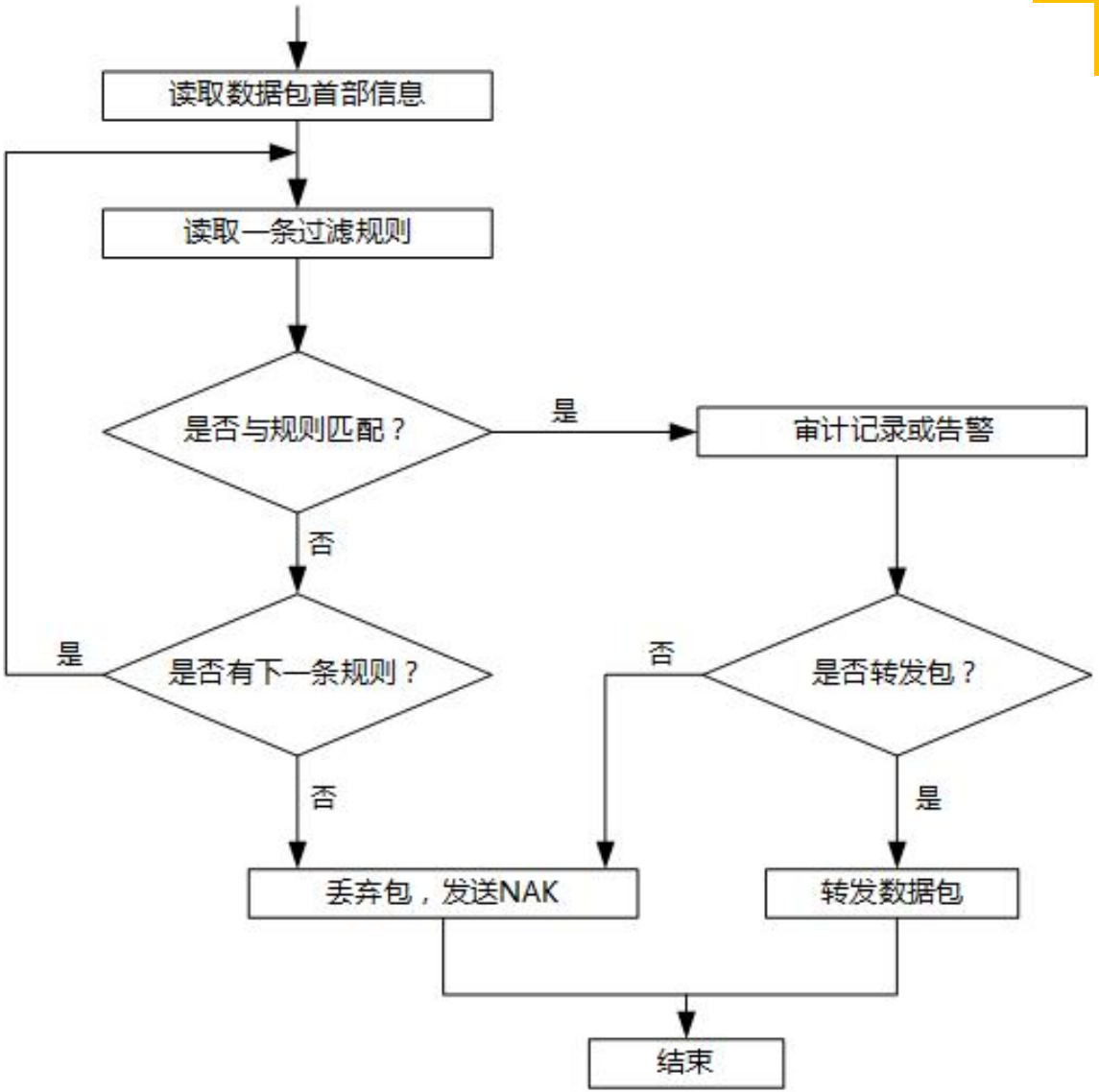
表1 一个过滤规则样表

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


读取数据包首部信息
读取一条过滤规则
是否与规则匹配？
是
审计记录或告警
否
是否有下一条规则？
是
否
是否转发包？
否
是
丢弃包，发送NAK
转发数据包
结束

三、防火墙的安全区域

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安全级别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。
  - 默认情况下，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。

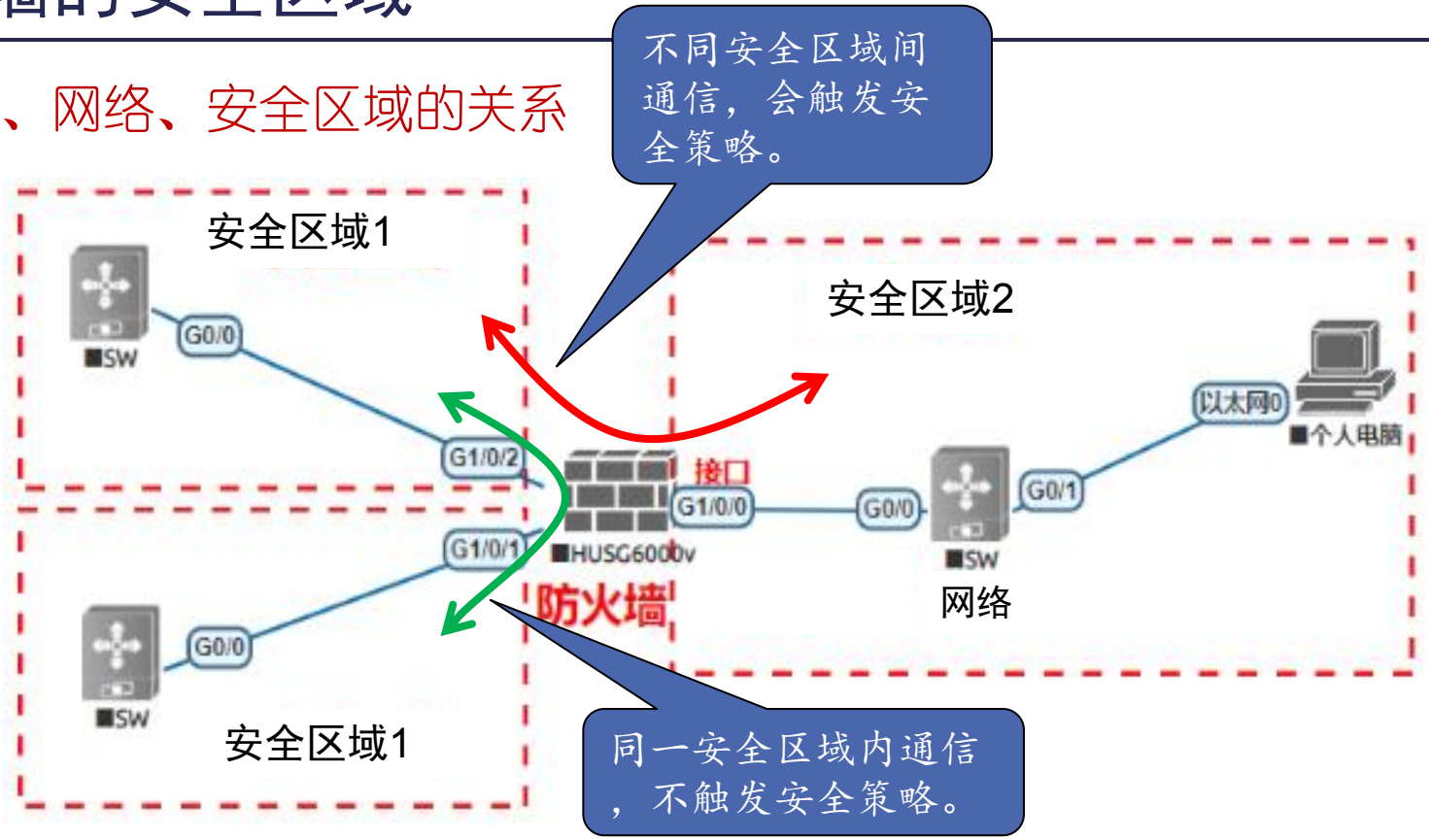
防火墙的安全区域

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。将接口划分到某安全区域后，通过接口就能把安全区域和网络关联起来。
- 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，园区网部署了防火墙，将服务器网络所接入的防火墙e1接口，划分属于安全区域A。将用户网络所接入的防火墙e2接口划分属于安全区域B。则某用户主机PC1访问服务器的报文，在经过防火墙时，可理解为从安全区域B发往安全区域A，此行为会触发防火墙中的安全策略。防火墙会通过包过滤，来匹配相应的安全策略。

防火墙的安全区域

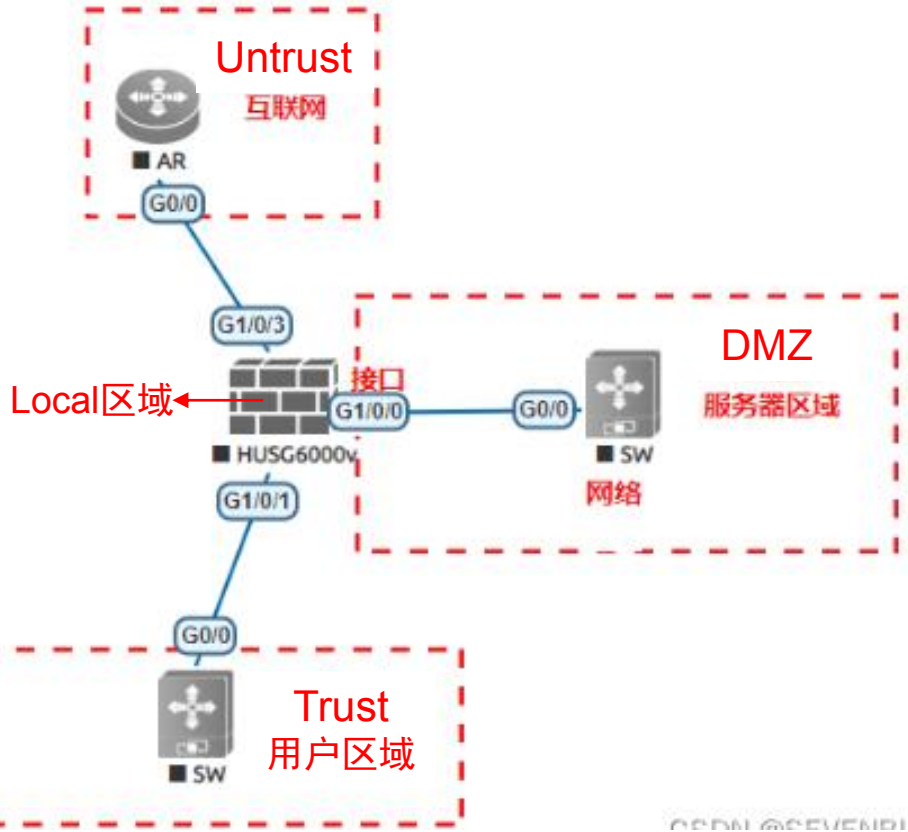
- 接口、网络、安全区域的关系



防火墙的安全区域

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

- 若某次网络访问的出发点或目的地是防火墙本身，例如通过数据中心的管理机登录防火墙进行配置，或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。
- 管理员不能在Local区域中添加任何接口，但防火墙所有接口本身都隐含属于Local区域。

防火墙的安全区域

默认的安全区域 — 安全级别ID值

- 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

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

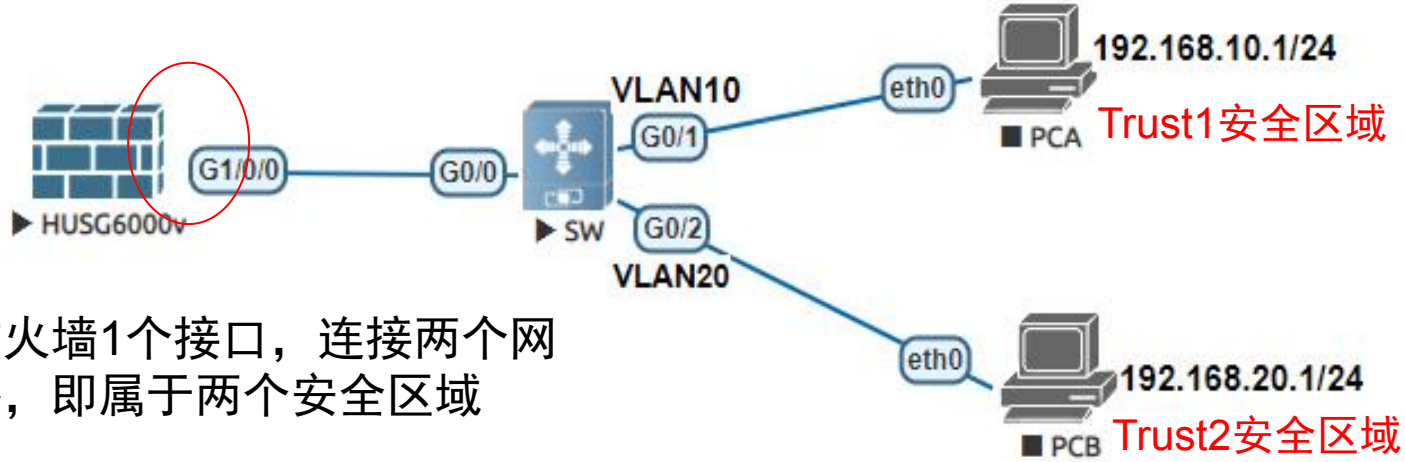
```
[FW1]firewall zone name SecA                          // 创建安全区域SecA
[FW1-zone-SecA]set priority 10                        //  将安全级别设置为10
[FW1-zone-SecA]add interface GigabitEthernet 1/0/0    // 将接口G1/0/0加入安全区域
```

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。

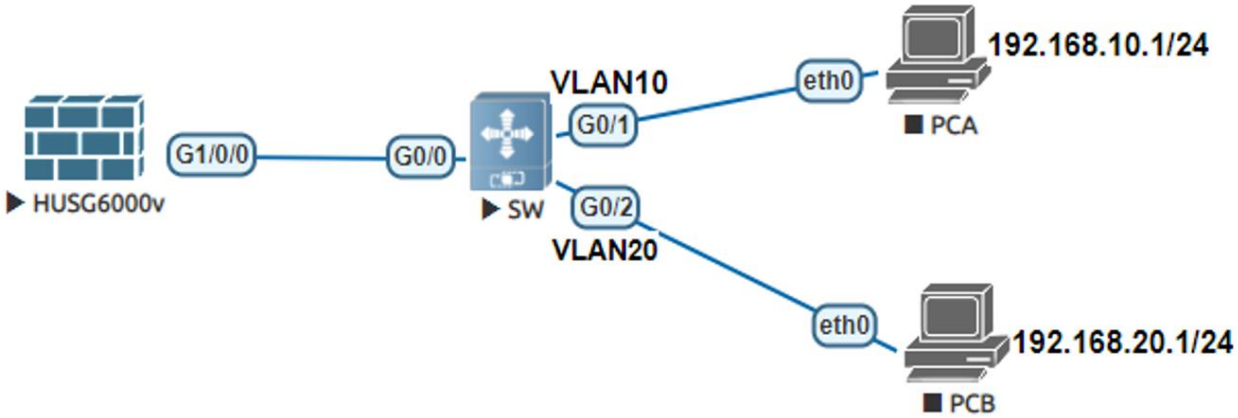
```
[FW1]interface GigabitEthernet 1/0/0.1
[FW1-GigabitEthernet1/0/0.1]vlan-type dot1q 10
[FW1-GigabitEthernet1/0/0.1]ip address 192.168.10.254 24

[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

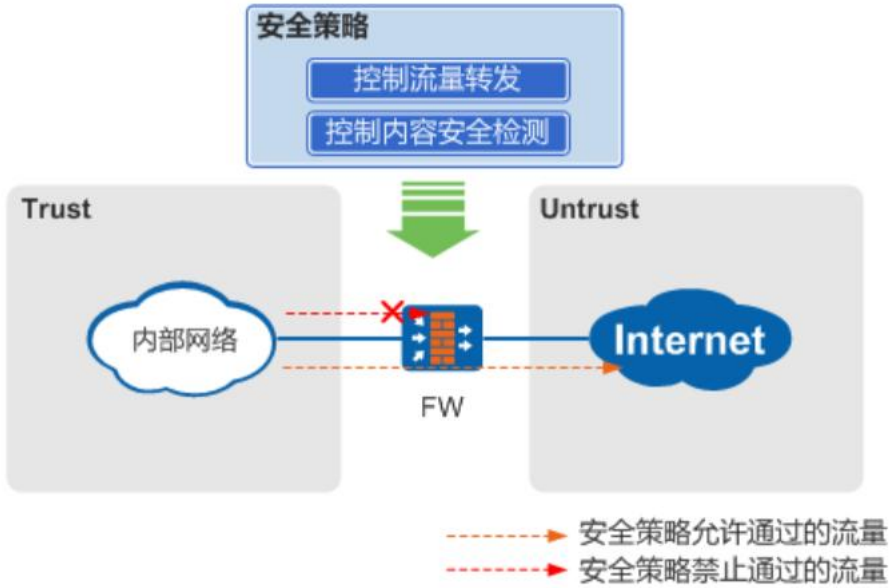
- 防火墙创建两个VLAN，配置VLANIF接口IP
- 配置G1/0/0接口工作在交换模式下（透明模式），并允许10和20VLAN报文通过。
- 将VLAN10和VLAN20划分到不同的安全区域。

```
[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、防火墙的安全策略

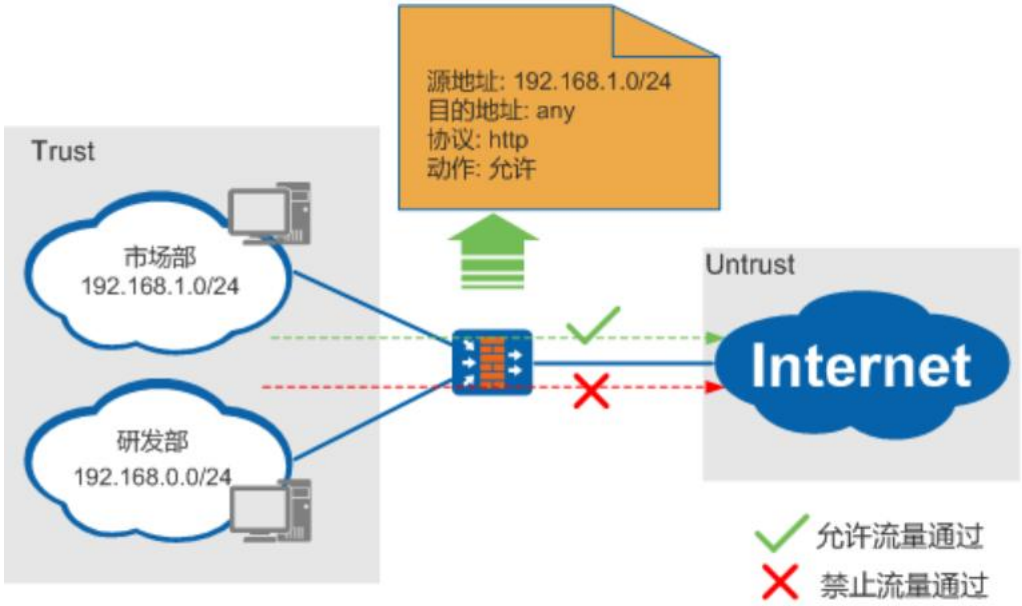
防火墙 —— 安全策略

- 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。



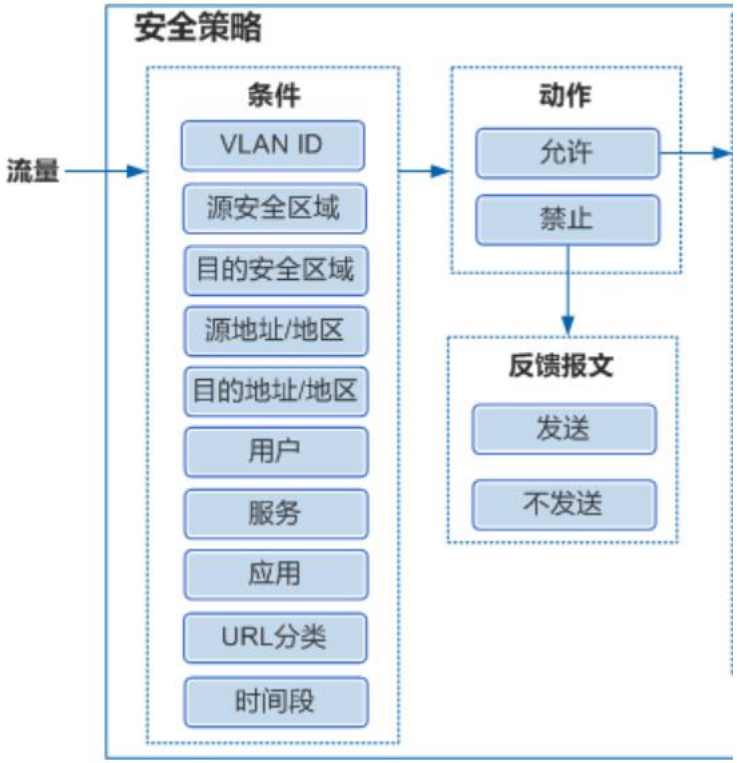
防火墙 —— 安全策略

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



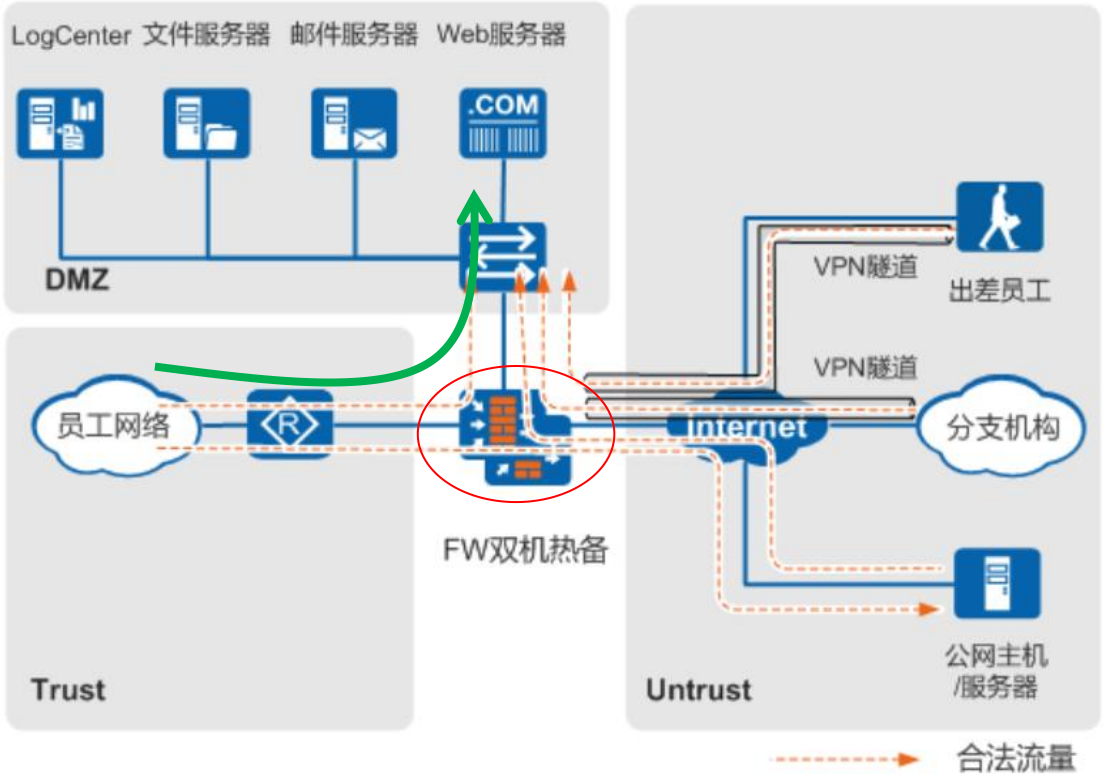
防火墙 —— 安全策略

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。

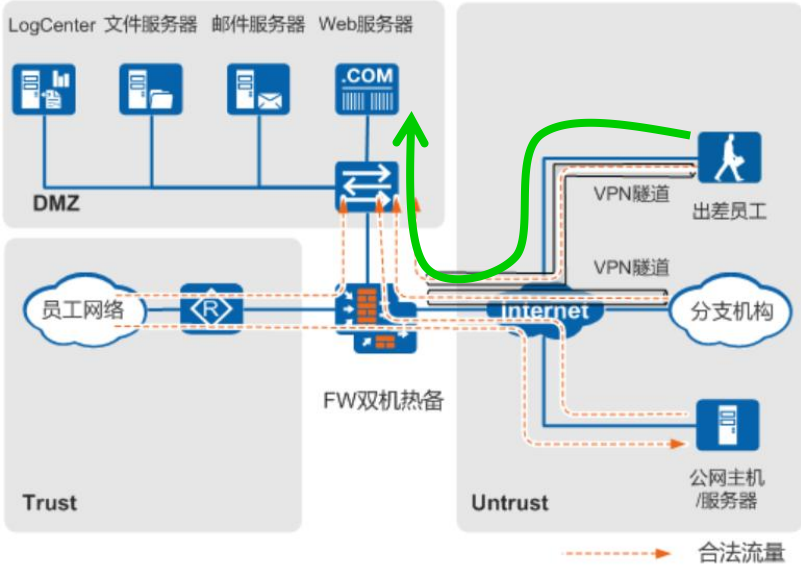
➢ 应用场景1 ——大中型企业边界防护

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。



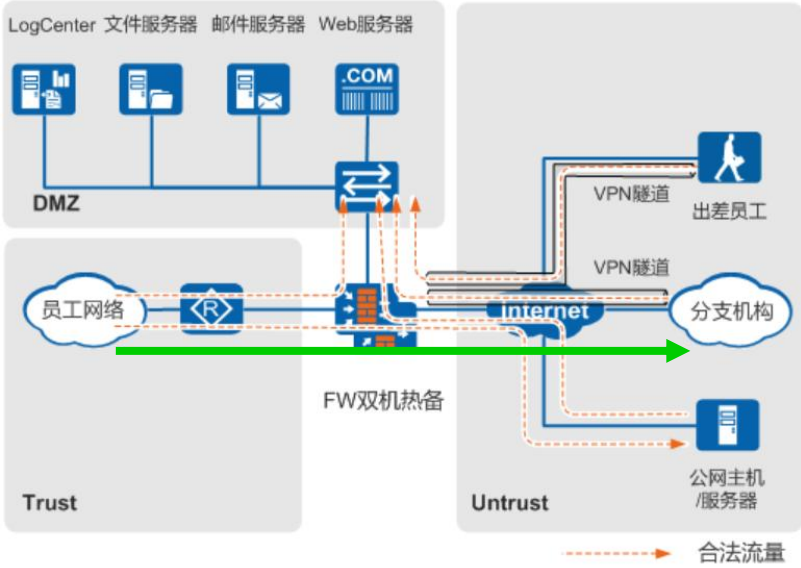
➢ 应用场景1 ——大中型企业边界防护

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。



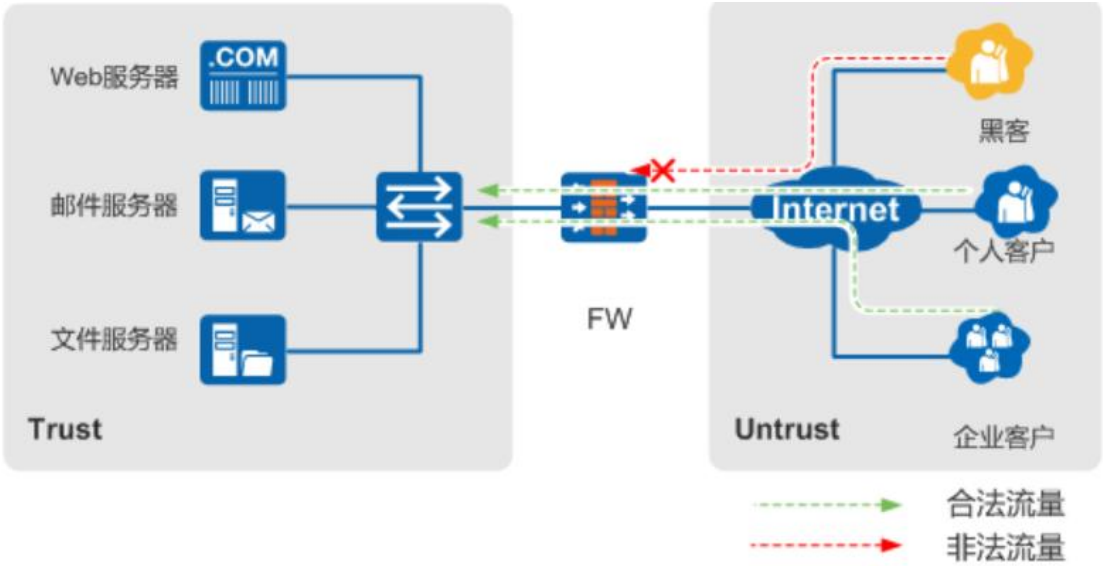
➢ 应用场景1 ——大中型企业边界防护

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。



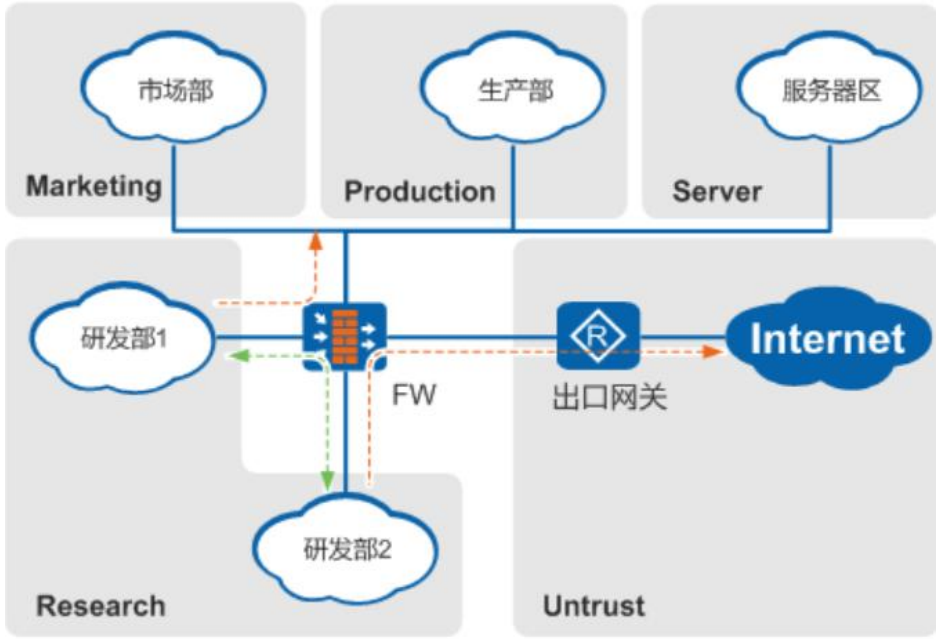
➢ 应用场景2 ——数据中心边界防护

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

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网段或B网段或C网段）

```
[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
```

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（匹配条件1）
[FW-1-policy-security-rule-abc]destination-address 172.16.100.11 32（匹配条件2）
[FW-1-policy-security-rule-abc]service dns    （匹配条件3）
[FW-1-policy-security-rule-abc]action permit  （匹配后的行为是“允许通过”）
[FW-1-policy-security-rule-abc]quit
```

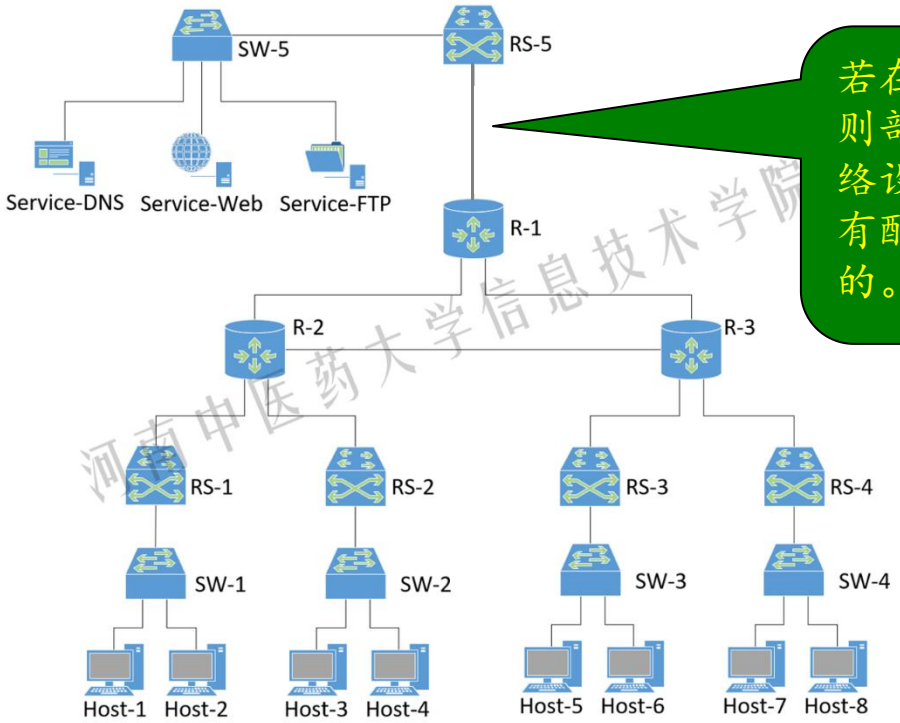
【注】一条安全策略中，各个匹配条件之间是“与”关系，即所有条件都满足，才算是匹配该策略，执行action后面的动作。

五、防火墙部署方式

防火墙部署 —— 透明方式

防火墙部署 —— 透明方式

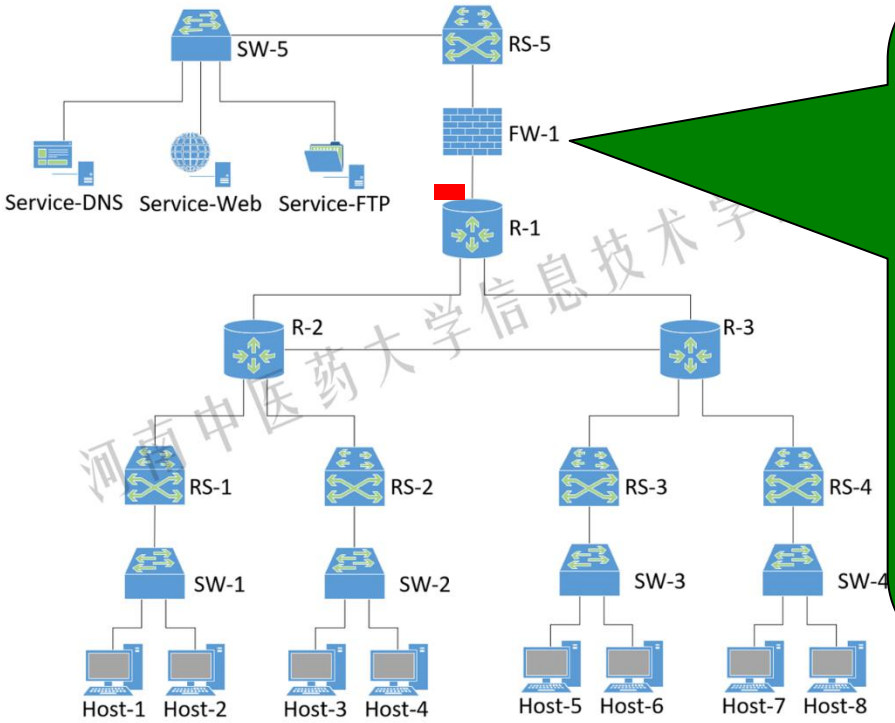
- 透明方式



若在此处添加部署防火墙，则部署前后，不需要改变网络设备（例如RS-5和R-1）原有配置，仿佛防火墙是透明的。

防火墙部署 —— 透明方式

- 透明方式



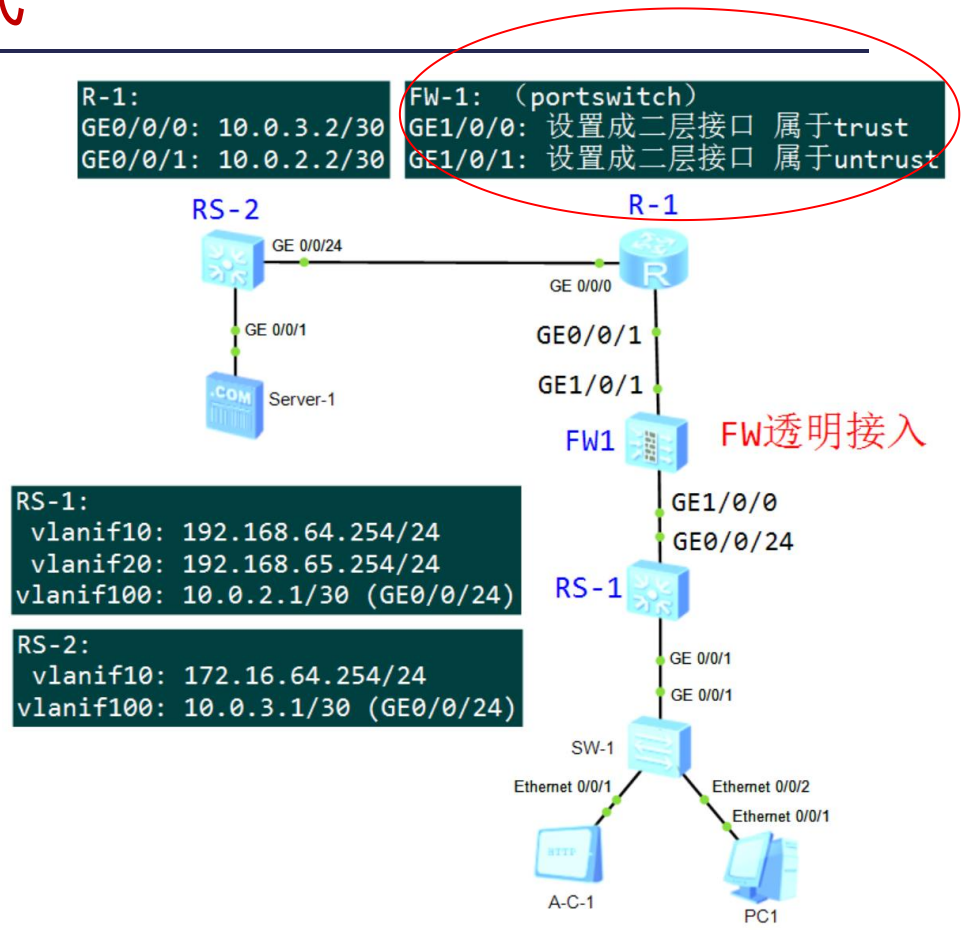
若防火墙配置成透明方式，则其上、下接口配置成二层接口，不需要配置IP地址，防火墙仿佛是一座直通的“桥”，但它能通过安全策略控制访问，即过滤通过它的数据包。

此时，对于R-1而言，其路由表中，到达服务器网络，其下一跳是RS-5，不是防火墙。

防火墙部署 —— 透明方式

- 透明方式
  - FW接口配置分析
  - 上下行设备接口分析
  - 路由配置

- FW上下接口不需要配置IP地址
- 对于RS-1而言，到达服务器网络，下一跳是R-1；
- 对于R-1而言，到达用户网络，下一跳是RS-1；
- FW1不需要配置ospf



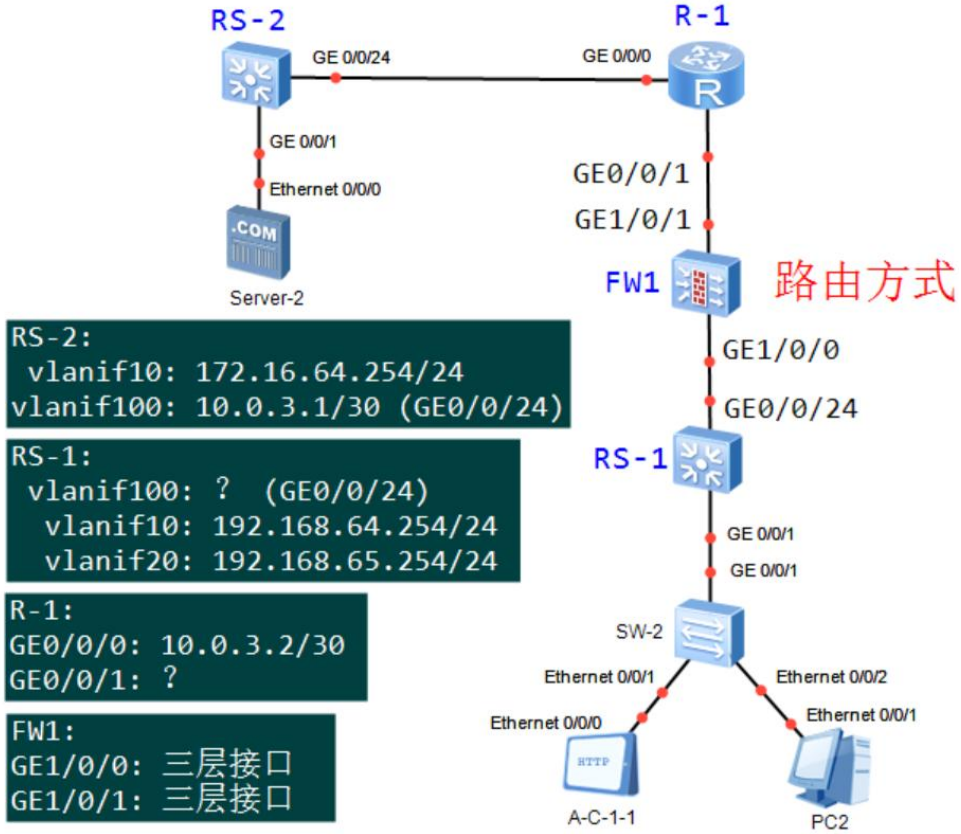
防火墙部署 —— 路由方式

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）

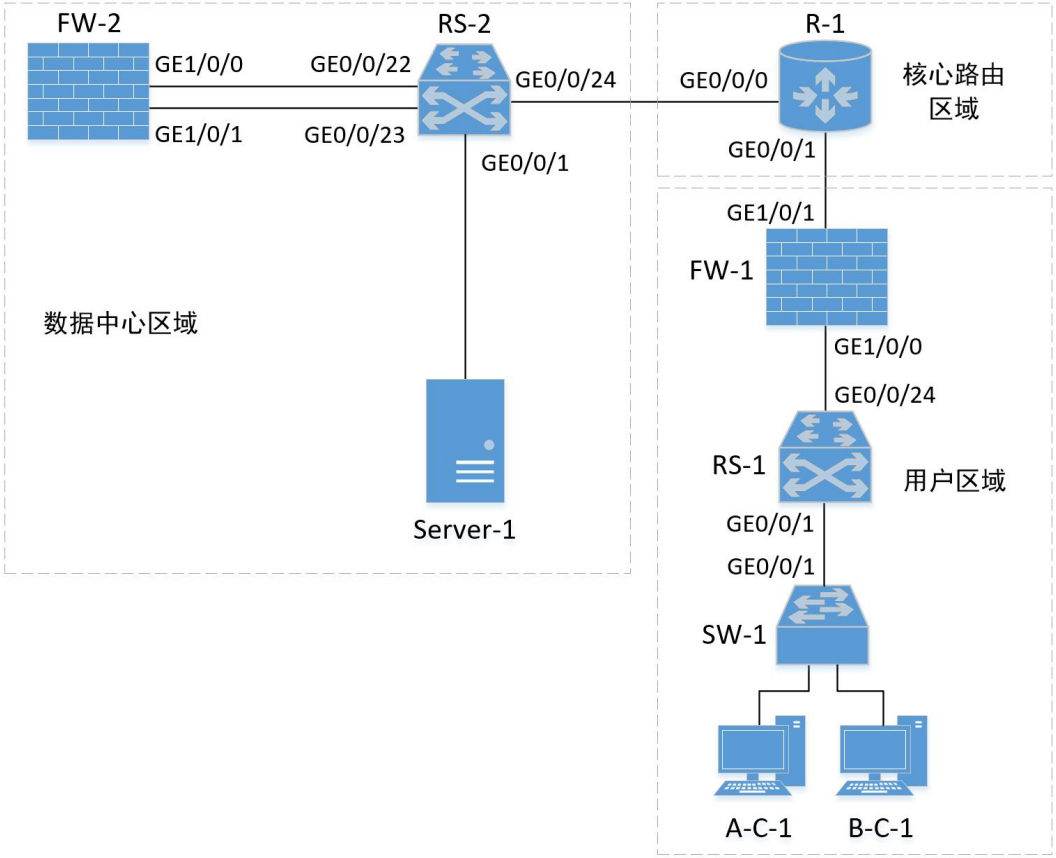
- FW上下接口需要配置IP地址
- 对于RS-1而言，到达服务器网络，下一跳是FW1的GE1/0/0接口；
- 对于R-1而言，到达用户网络，下一跳是FW1的GE1/0/1接口；
- FW1上也需要配置ospf



防火墙部署 —— 旁挂方式

防火墙部署 —— 旁挂方式

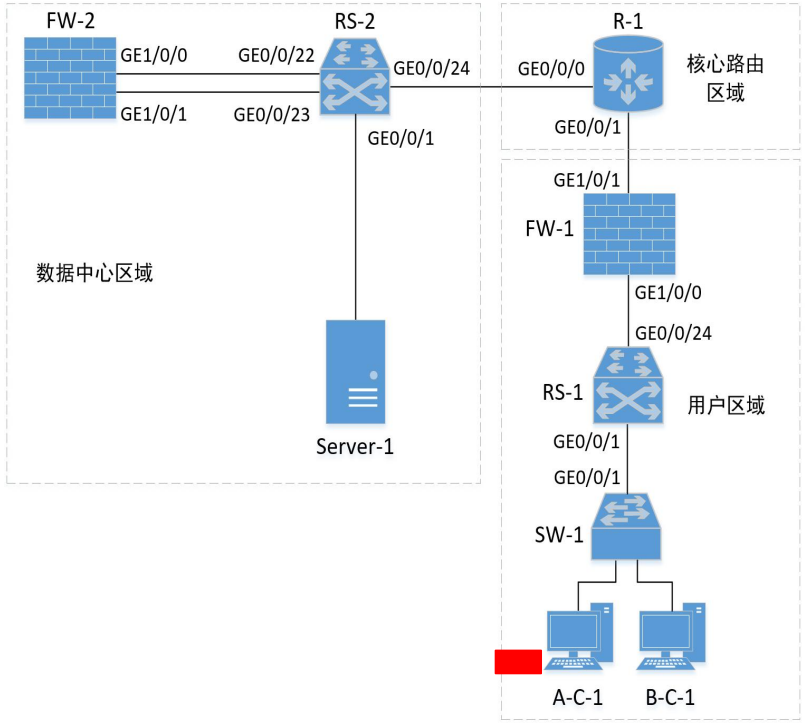
- 防火墙旁挂



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6讲　使用防火墙加强网络安全

（完）