网络运维管理

第07讲 防火墙应用

河南中医药大学信息技术学院

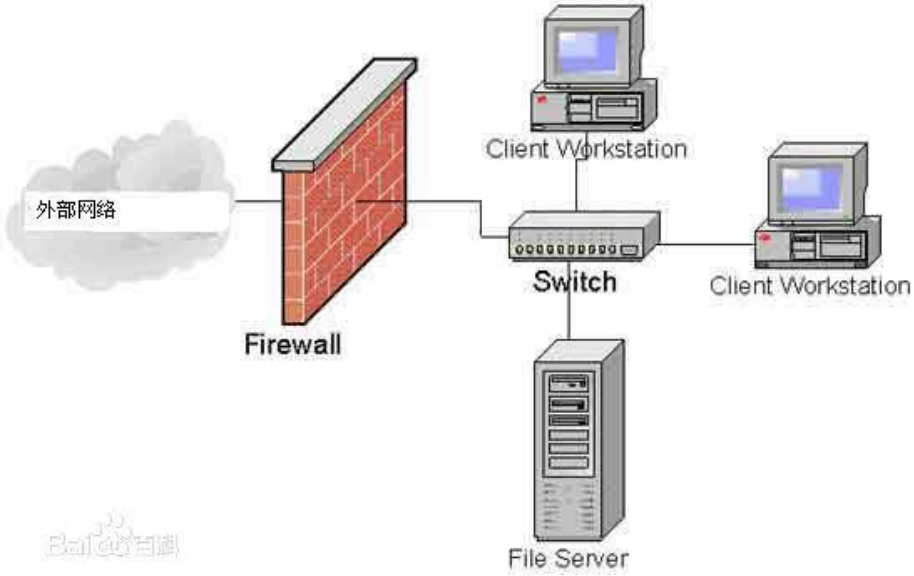
《网络运维管理》课程教学组

防火墙

防火墙是什么

1.防火墙是什么?

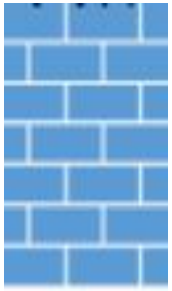
- 设置在不同网络（如可信任的企业内部网络和不可信的公共网络）或网络安全域之间的一系列部件的组合。在逻辑上，防火墙是一个分离器、一个分析器，也是一个限制器，能够有效地监控流经防火墙的数据，保证内部网络和隔离区的安全。



防火墙是什么?

- 防火墙是在两个网络之间执行访问控制策略的一个或一组系统，包括硬件和软件，其目的是保护网络不被他人侵扰。
- 本质上，防火墙遵循的是一种允许或阻止业务来往的网络通信安全机制，也就是提供可控的、能过滤的网络通信。

运行 / 阻止



防火墙是什么?

- 防火墙最常用的应用是防止Internet（或其他外部网络）上的危险（非法访问或攻击等）传播到需要保护的内部网络。
- 通常防火墙就是位于内部网或Web站点与互联网之间的一个路由器或一台计算机。

防火墙在网络中的位置

防火墙

防火墙管理

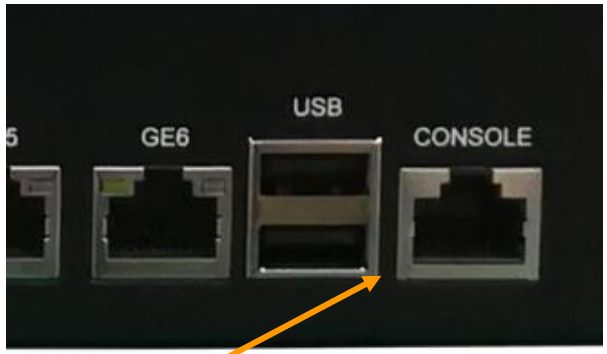
防火墙管理

- 防火墙的管理方式
  - 带外管理——首次登录
  - 带内管理
    - Web管理
    - CLI管理

防火墙的首次登录——带外管理

防火墙的CONSOLE接口

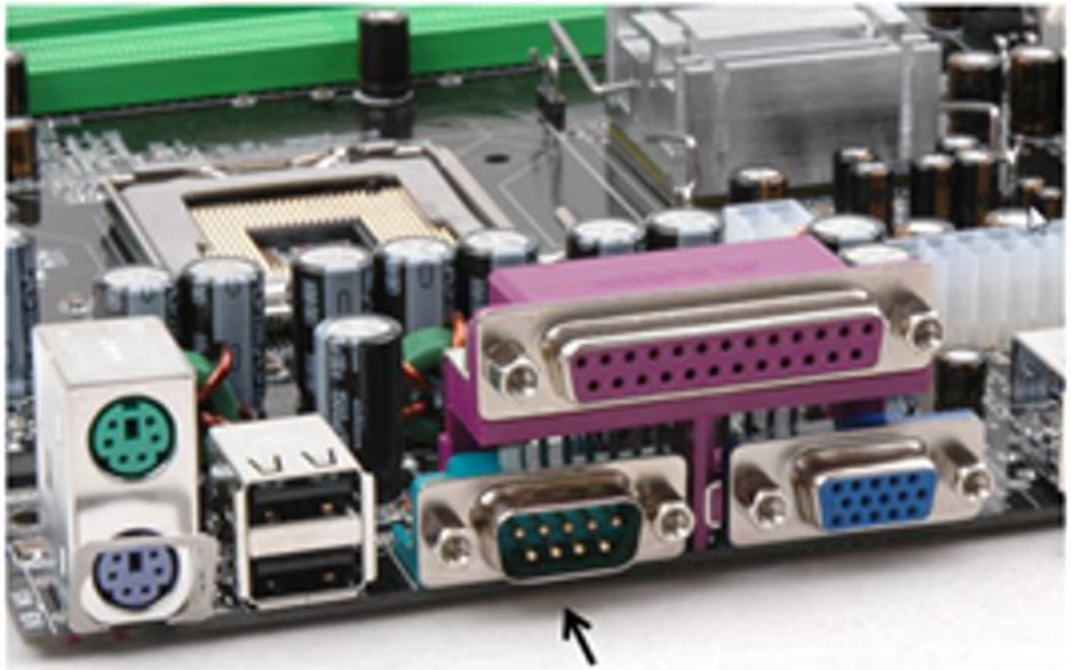
防火墙的首次登录——带外管理



CONSOLE接口

防火墙的CONSOLE接口

防火墙的首次登录——带外管理



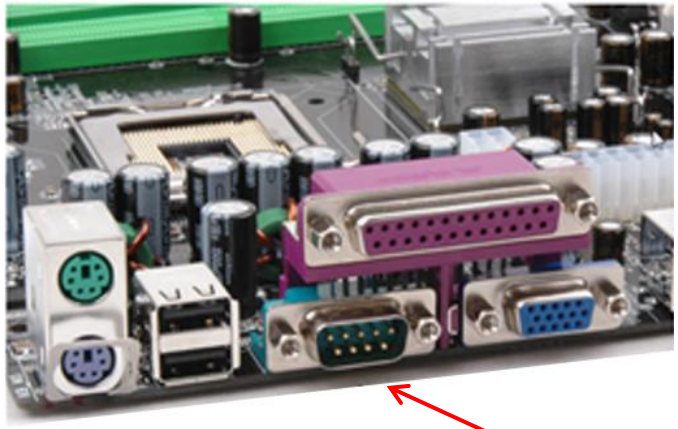
电脑上的COM口

防火墙的首次登录——带外管理

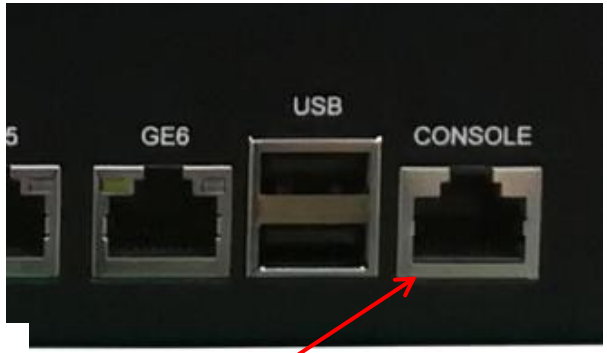
- Console线
  - 无论交换机的Console口是采用串行接口（com口），还是采用RJ-45接口，都需要通过专门的Console线连接至计算机的串行口，然后进行配置。
  - 由于交换机的Console口有两种，Console线也分为两种：
    - (1) 两端均为串行接口；
    - (2) 一端是RJ-45,另一端是串行口。

防火墙的首次登录——带外管理

- 注意，带外管理不需要使用IP地址（即管理双方都不需要配置IP地址），也不需要使用防火墙的网络接口（例如GE6）



COM口

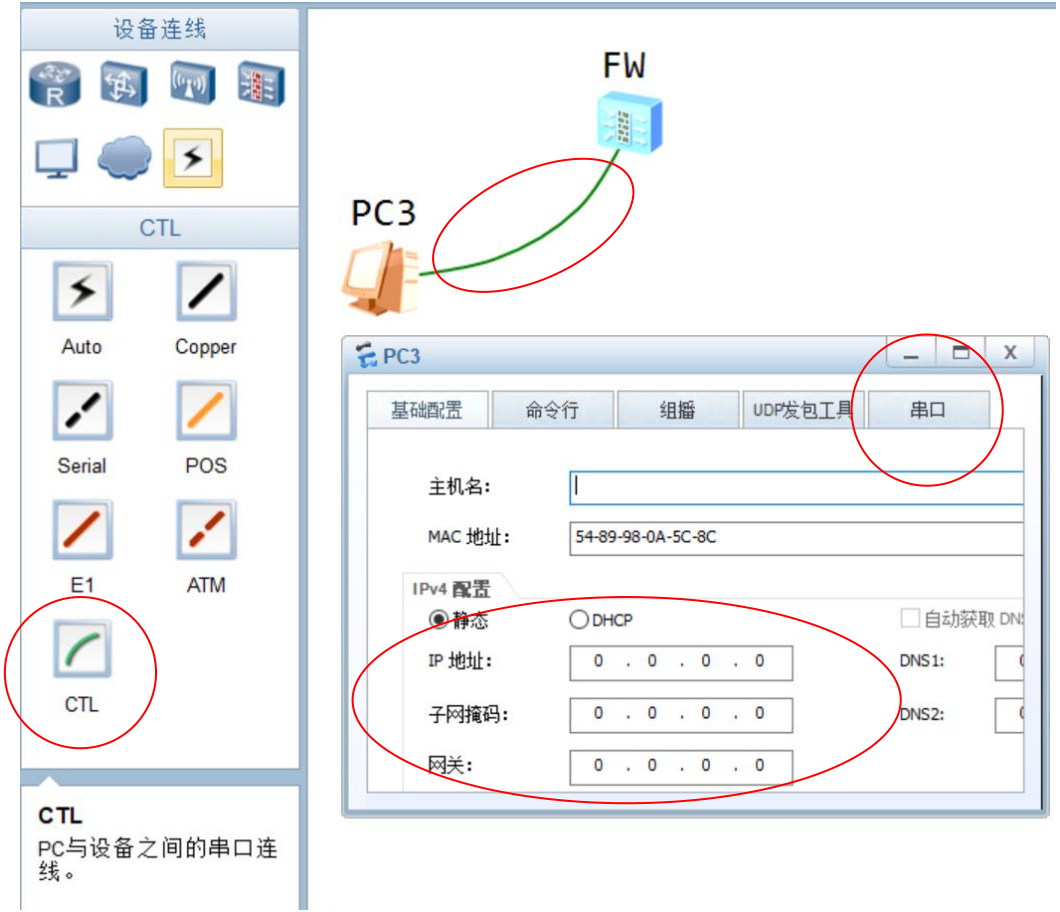


console口

Console线

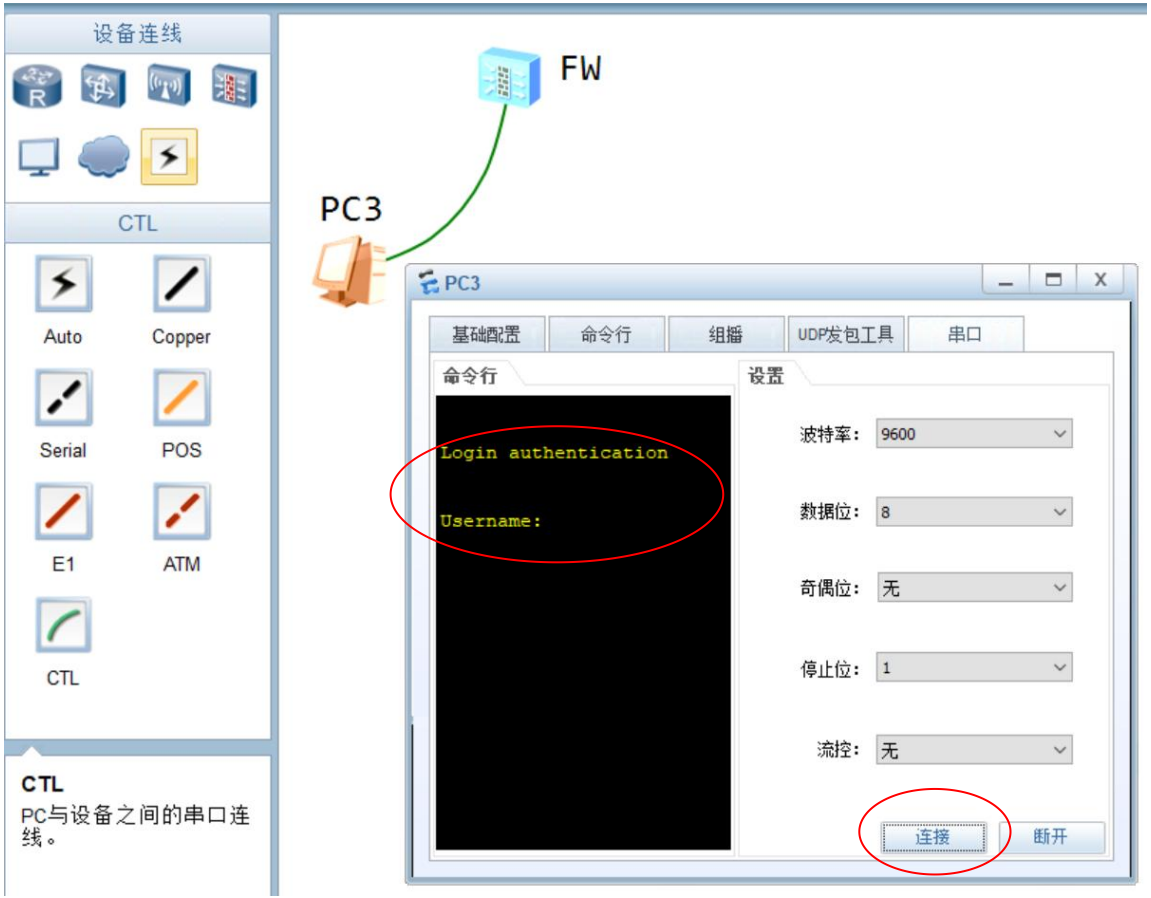
防火墙的首次登录——带外管理

- eNSP中也仿真了带外管理的方式
- 注意，此时PC3并未配置IP地址。



防火墙的首次登录——带外管理

- 点击“连接”，登录防火墙，需要输入用户名和登录密码



防火墙的首次登录——带外管理

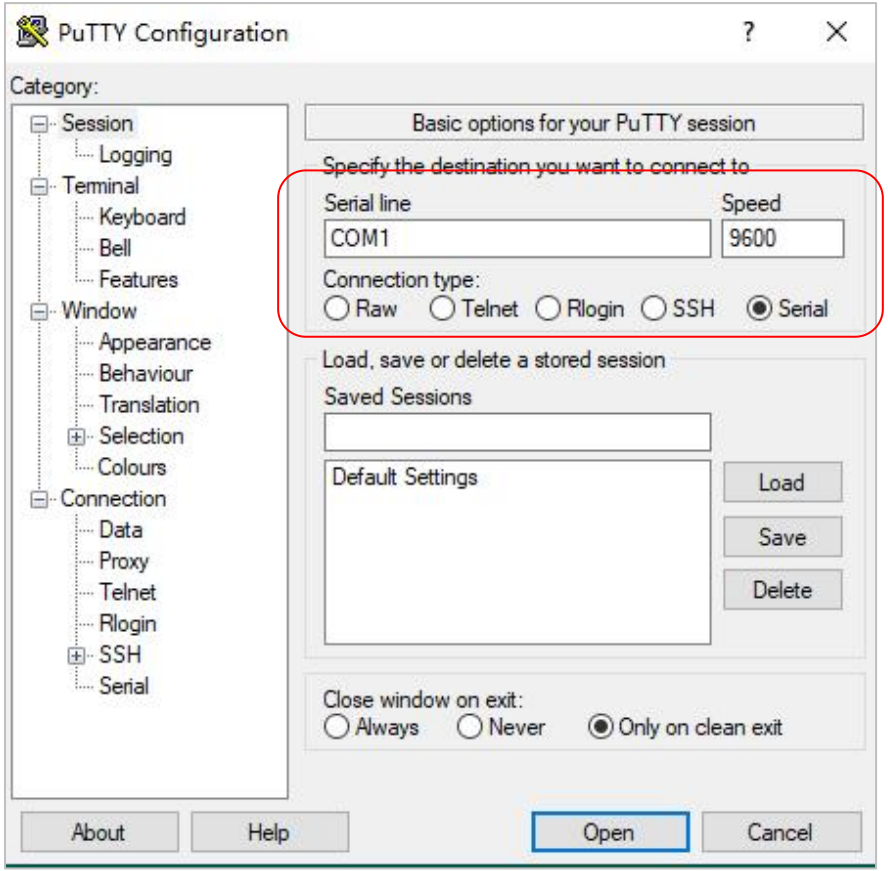
- 带外管理所用到的软件
  - 可以使用“超级终端”程序，登录FW（Windows7以前的版本自带，后期的版本需要自行下载）；

【开始】→【所有程序】→【附件】→【通讯】

建立连接，然后登录交换机

防火墙的首次登录——带外管理

- 带外管理所用到的软件
  - PuTTY：此工具为第三方软件，能支持串口登录。



防火墙的带内管理

防火墙管理—— 带内管理

- 带内管理的界面
  - CLI（命令行界面）
    - 通过Telnet或SSH登录，使用命令行对FW进行配置管理。
  - Web界面
    - 通过http（即通过浏览器）登录FW，则可通过Web界面管理交换机。在Web界面中，用户只需点击相应的选项即可实现管理操作，通常不需要输入具体的命令单词。

防火墙管理—— 带内管理

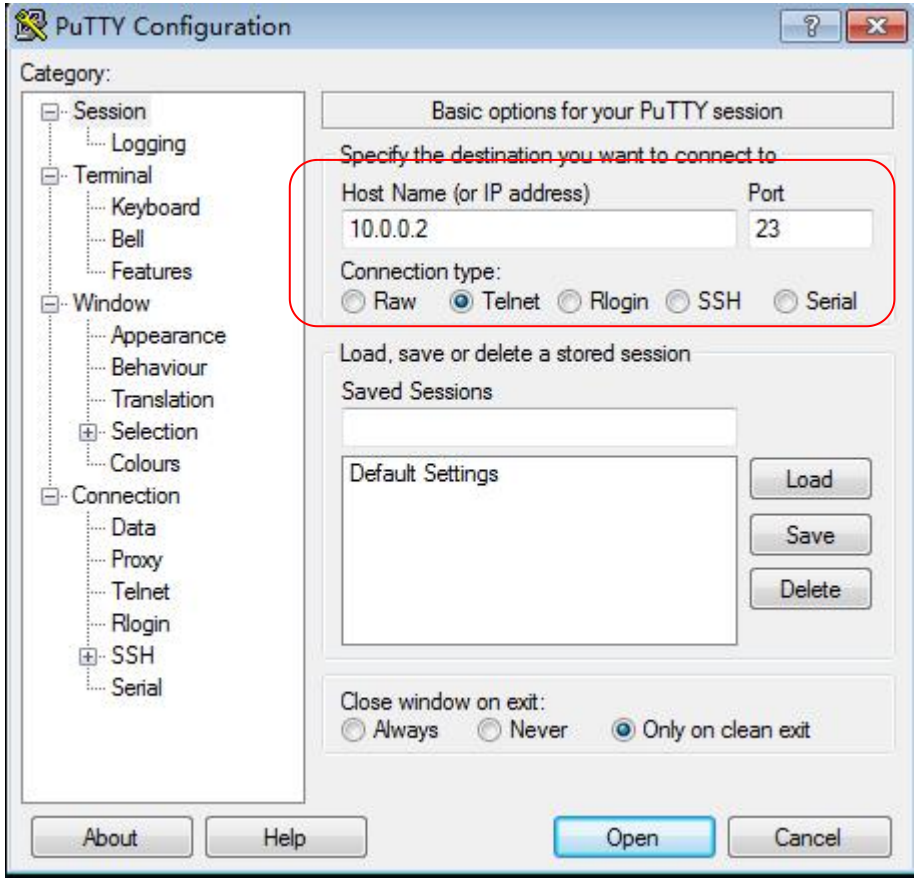
- 通过带内方式管理FW的前提条件：
  1. FW已配置IP地址（通过带外管理方式）；
  2. 管理客户端的IP地址，与其要管理的交换机的IP地址在相同网段；
  3. 若不满足2，则管理客户端必须可以通过路由设备访问到交换机。
  4. FW启动http服务或Telnet/SSH服务；
  5. 在FW上设置相应服务的授权用户（例如http用户），并设置用户名和密码。
  6. 以带内方式登录FW时，需要输入正确的用户名和口令

防火墙管理—— 带内管理

- 通过带内方式管理FW的前提条件：
  1. FW已配置IP地址（通过带外管理方式）；
  2. 管理客户端的IP地址，与其要管理的交换机的IP地址在相同网段；
  3. 若不满足2，则管理客户端必须可以通过路由设备访问到交换机。
  4. FW启动http服务或Telnet/SSH服务；
  5. 在FW上设置相应服务的授权用户（例如http用户），并设置用户名和密码。
  6. 以带内方式登录FW时，需要输入正确的用户名和口令

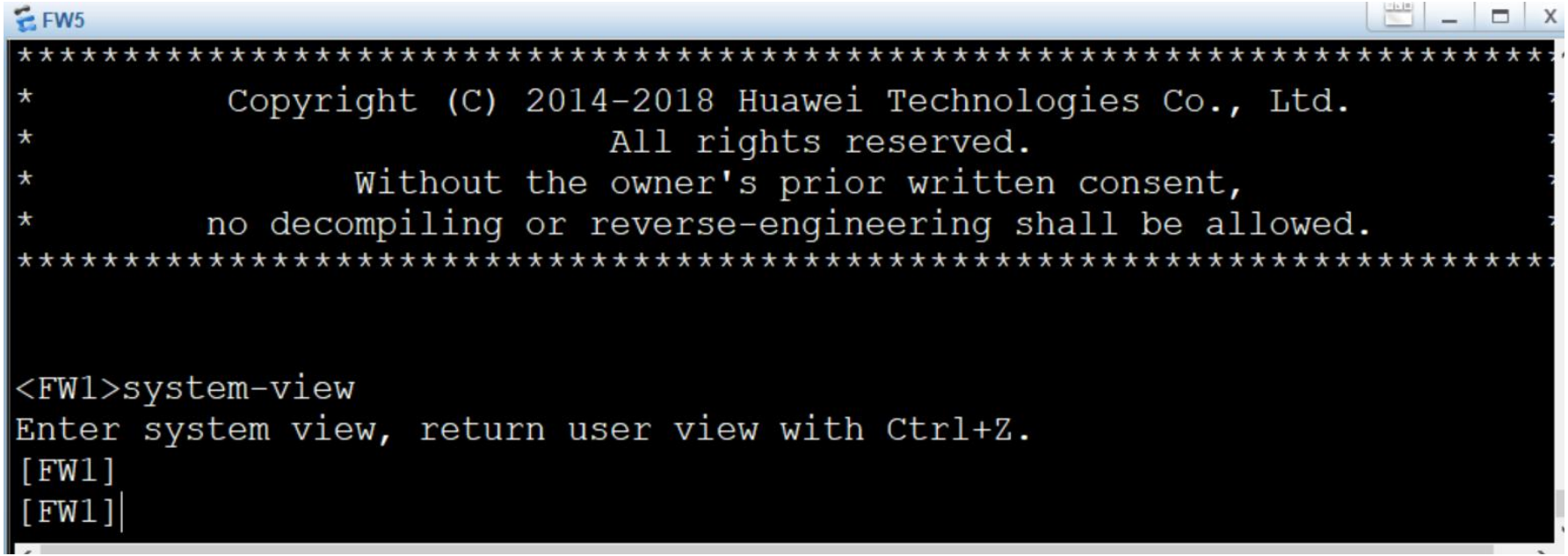
防火墙管理—— 带内管理

- 通过TELNET登录FW
  - 可以使用Putty程序，以telnet方式登录交换机



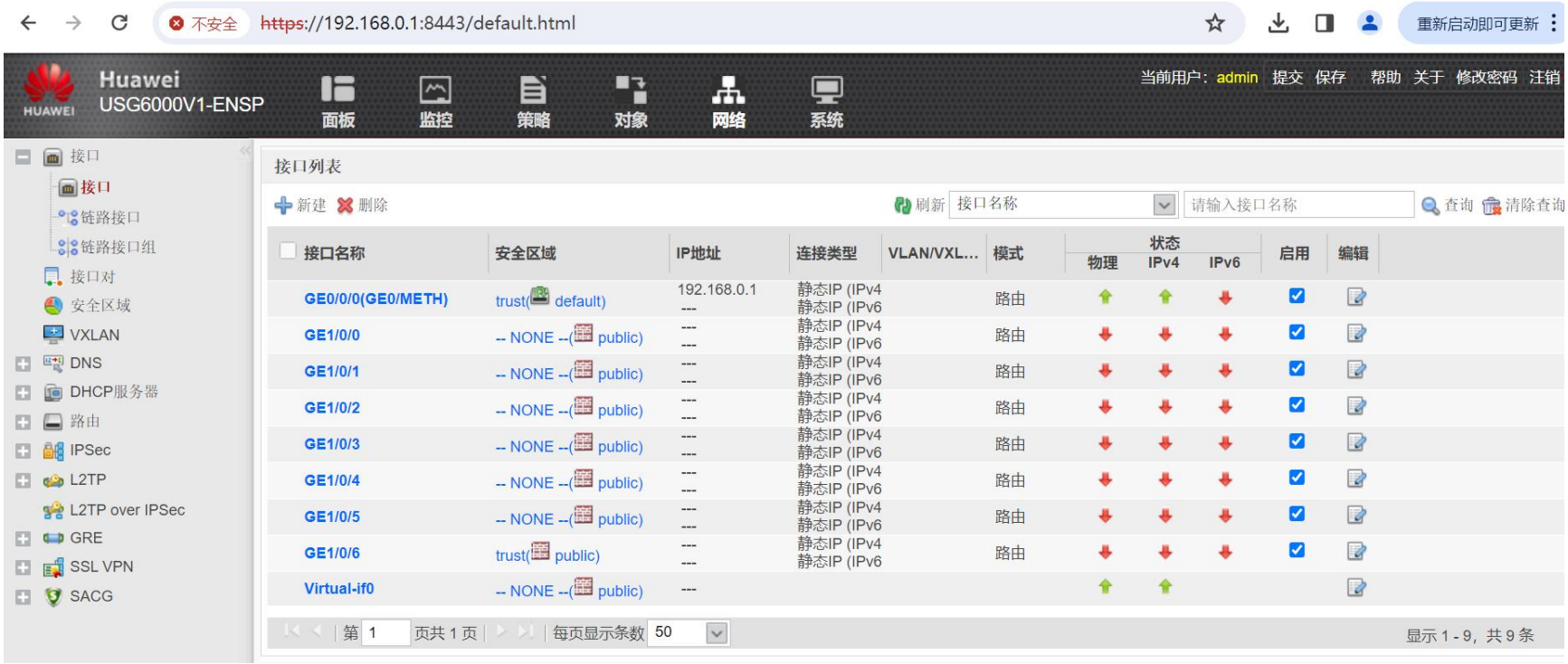
防火墙管理—— 带内管理

- CLI方式配置FW



防火墙管理—— 带内管理

- Web方式配置FW



防火墙应用

防火墙的安全区域

2.防火墙——安全区域

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。

2.防火墙—— 安全区域

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。

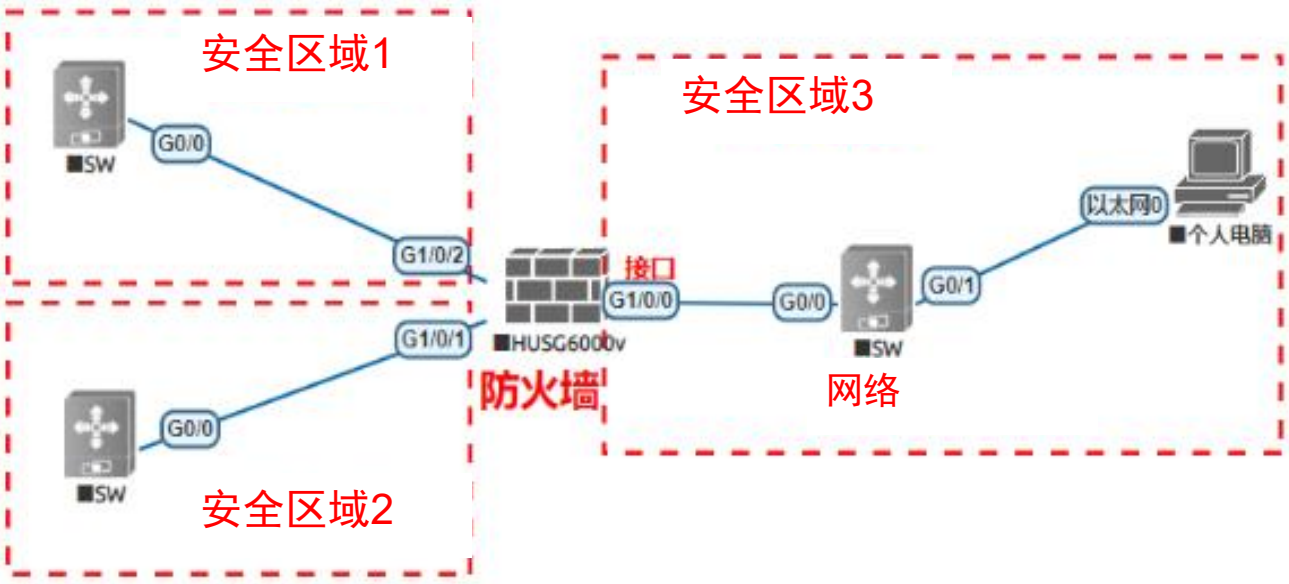
2.防火墙—— 安全区域

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，一般来说，当报文在不同的安全区域之间流动时才会受到控制。
- 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，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。

2.防火墙—— 安全区域

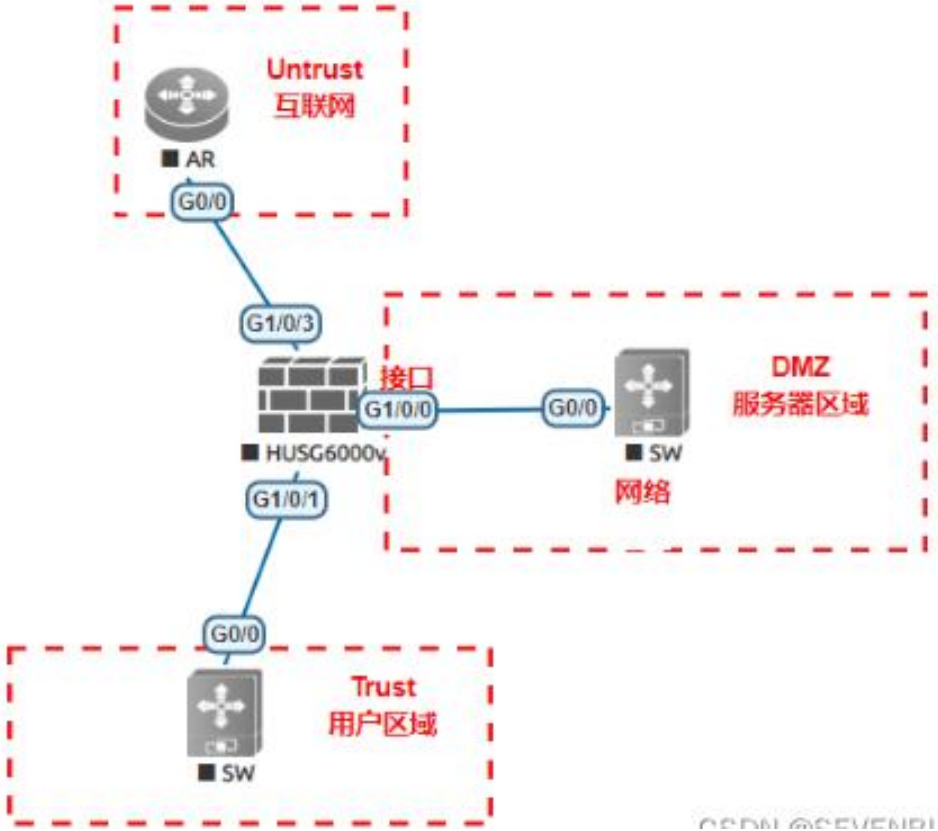
- 接口、网络、安全区域的关系
  - 在华为防火墙上，一个接口只能加入到一个安全区域中。
  - 通过接口划分到不同的安全区域中，就可以在防火墙划分不同网络



2.防火墙 —— 安全区域

默认的安全区域

- Trust区域： 网络的受信任程度高，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。



2.防火墙 —— 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）的报文均可认为是从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。**

2.防火墙 —— 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，每个安全区域都必须有1个安全级别，唯一ID，用1-100数字表示，数字越大，越可信。默认的安全区域，安全级别是固定的。
    - Local安全级别100，Trust区域安全级别：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）**

2.防火墙 —— 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，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

2.防火墙 —— 安全区域

安全区域配置

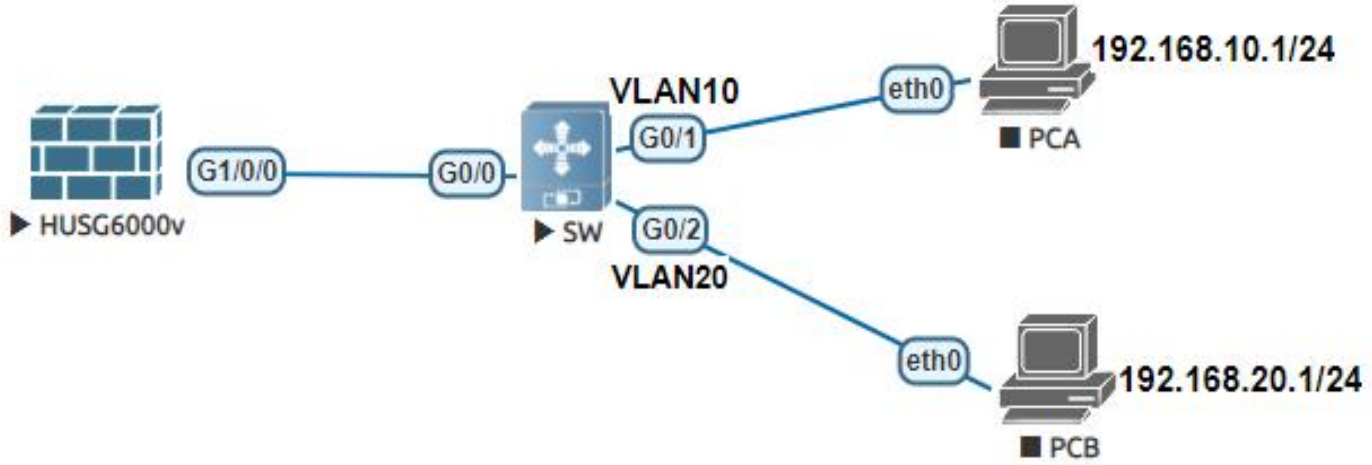
- 安全区域的配置主要包括：创建安全区域及接口加入到安全区域。
  - 举例：创建一个安全区域SecA，将接口G1/0/0加入该安全区域。可以工作在路由模式也可以工作在交换模式。新创建的安全区域没有安全级别，必须先设置安全级别，然后才能加入端口。

```
[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
```

2.防火墙 —— 安全区域

安全区域配置

- 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
- 举例2：子接口接入安全区域



2.防火墙 —— 安全区域

安全区域配置

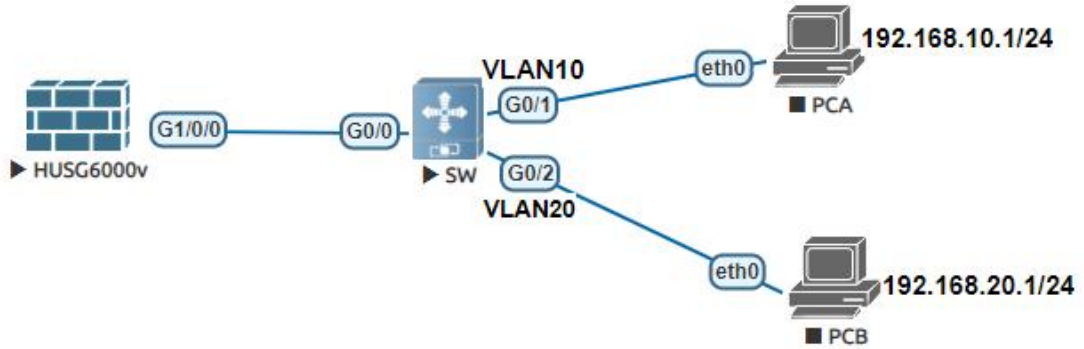
举例2：子接口接入安全区域

- 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，PCA被划分到trust1区域，PCB划分到2区域，此时就可以对PCA和PCB报文进行控制。

```
[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
```

2.防火墙 —— 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。



2.防火墙 —— 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。

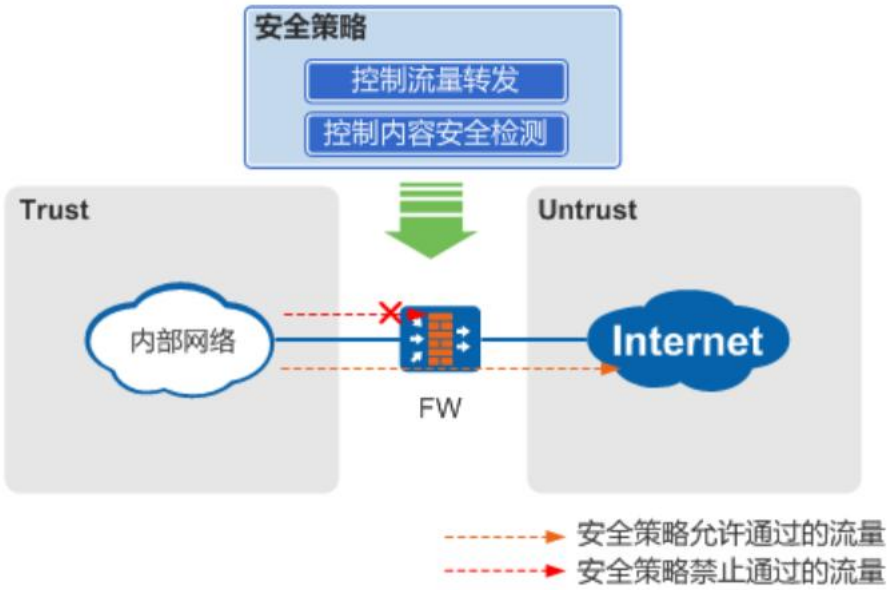
```
[FW1]vlan batch 2 3
[FW1]interface vlan 2
[FW1-Vlanif2]ip add 1.1.1.1 24
[FW1]interface vlan 3
[FW1-Vlanif3]ip add 2.2.2.1 24

[FW1]int g1/0/0
[FW1-GigabitEthernet1/0/0]portswitch
[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
```

防火墙应用

防火墙策略

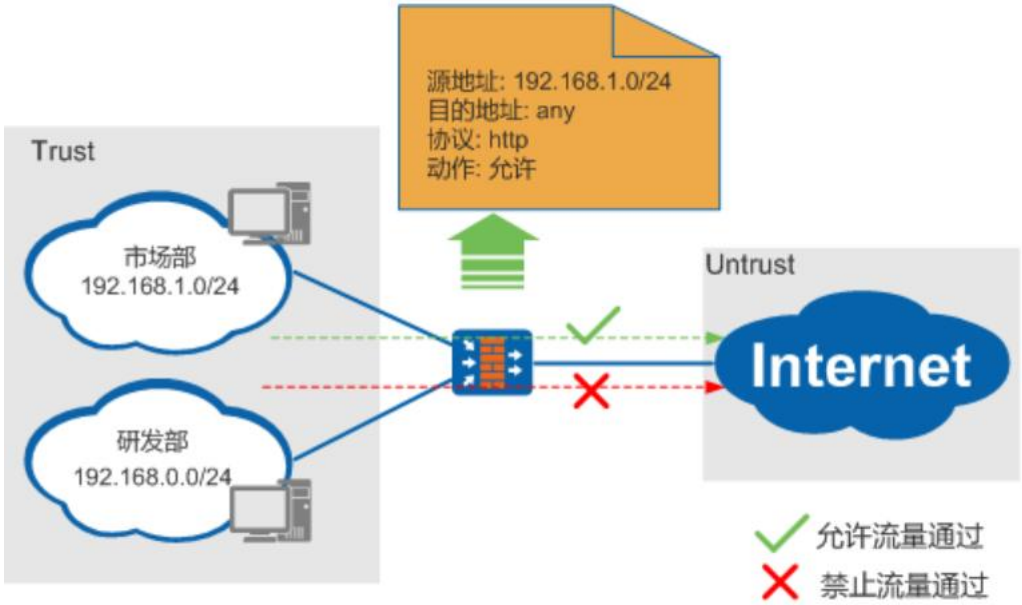
防火墙 —— 安全策略

- 安全策略：是控制设备对流量转发的策略
  - 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

- 传统防火墙的包过滤
  - 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

- 传统防火墙的包过滤
  - 传统防火墙的包过滤反映了传统网络的特点，随着互联网技术的不断发展，新时代网络对网络安全有了新的需求。
  - 传统网络的特点 VS 新时代网络特点

防火墙 —— 安全策略

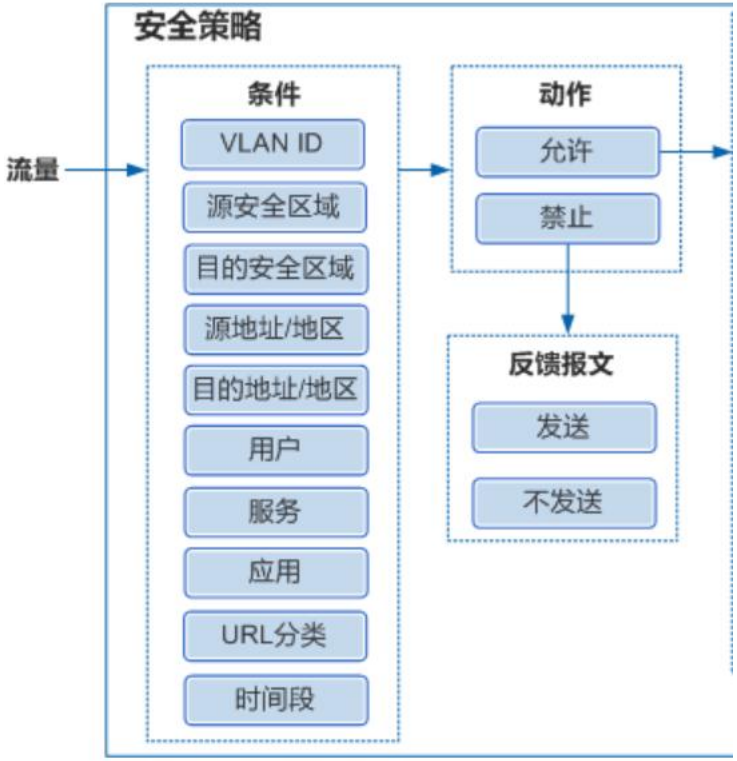
传统网络与新时代网络对比	
传统网络	新时代网络
用户等于IP（例如市场部=192.168.1.0/24），用户的区分只能通过网段或安全区域的划分来实现。如果用户的IP地址不固定，则无法将用户与IP地址关联。	因为用户移动办公，IP地址不固定，所以企业管理者希望将用户与IP地址动态关联起来，从而能够以可视化方式查看用户的活动，根据用户信息来审计和控制穿越网络的应用程序和内容。
应用等于端口，例如浏览网页的端口为80，FTP的端口为21。如果想允许或限制某种应用，直接允许或禁用端口就能解决问题。	大多数应用集中在少数端口（例如80和443），应用程序越来越Web化（例如微博、Web Mail）。允许访问80端口将不仅仅是允许浏览Internet网页，同时也可使用多种多样的基于网页的应用程序。
网络是黑白分明的，只有安全和不安全之分，即要么是安全的应用，要么是不安全的应用。对于不安全的应用全部拒绝即可，不会影响正常业务。	正常的应用程序常常会伴随不安全的流量。网络攻击由传统的单包攻击转为木马、黑客等信息窃取技术，应用和数据库存在大量的风险。

防火墙 —— 安全策略

- 下一代防火墙的安全策略
  - 下一代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



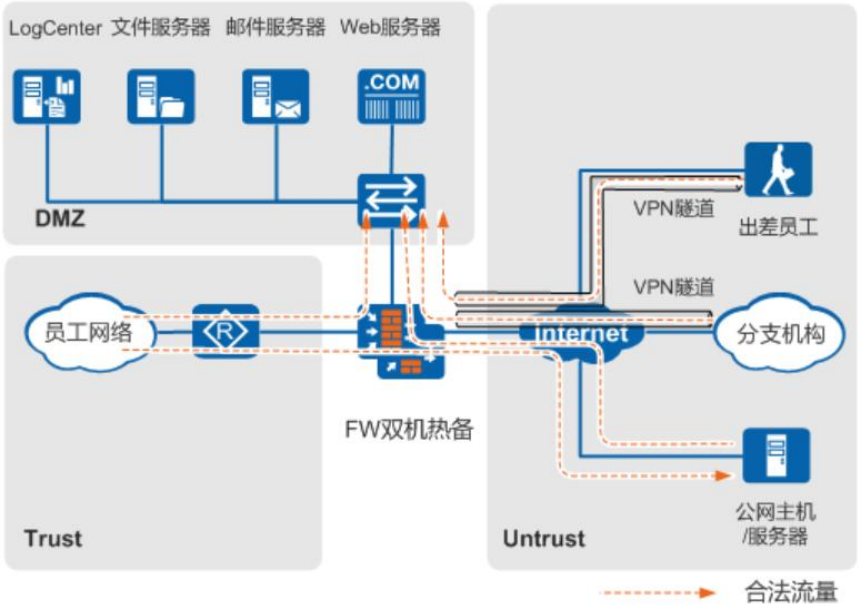
防火墙 —— 安全策略

- 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。

防火墙 —— 安全策略

- 安全策略的应用场景——大中型企业边界防护

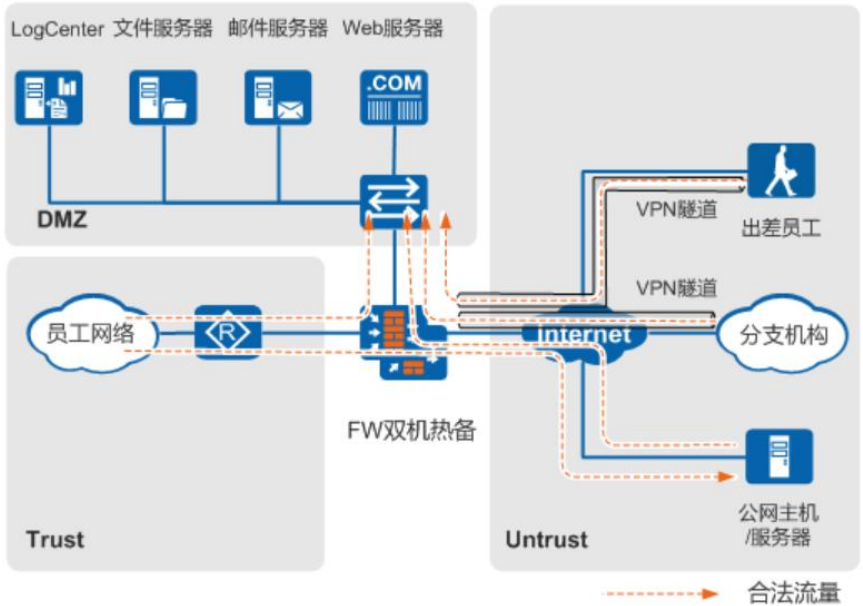
1. 公司将员工网络、服务器网络、外部网络划分到不同安全区域，通过安全策略对安全区域间的流量进行检测，保护公司内部网络。



防火墙 —— 安全策略

- 安全策略的应用场景——大中型企业边界防护

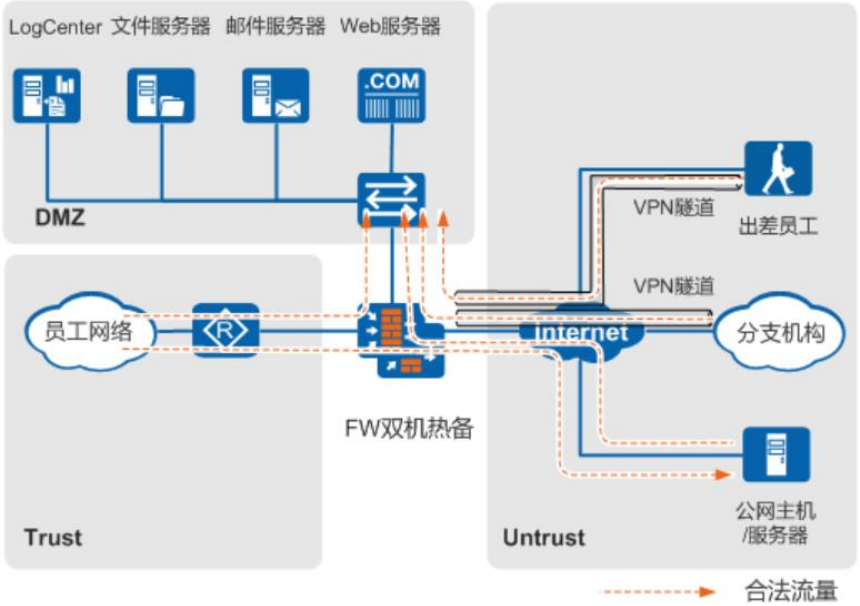
2. 根据公司对外提供的网络服务的类型配置安全策略的内容安全功能。例如针对图中的文件服务器开启文件过滤和内容过滤，针对邮件服务器开启邮件过滤，并且针对所有服务器开启反病毒和入侵防御。



防火墙 —— 安全策略

- 安全策略的应用场景——大中型企业边界防护

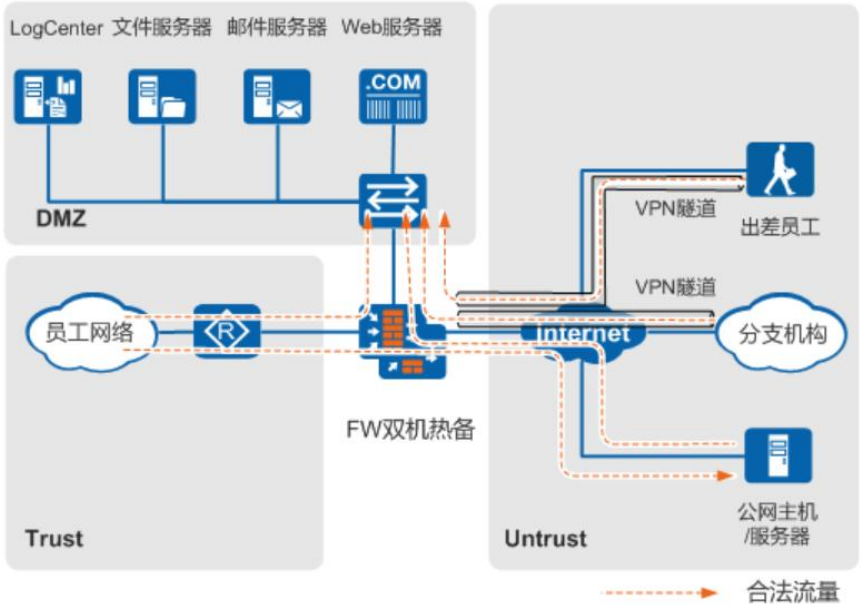
3. 针对内网员工访问外部网络的行为，配置URL过滤、DNS过滤、文件过滤、内容过滤、应用行为控制和反病毒等内容安全功能，既保护内网主机不受外网病毒和入侵的威胁，又可以防止企业机密信息的泄露



防火墙 —— 安全策略

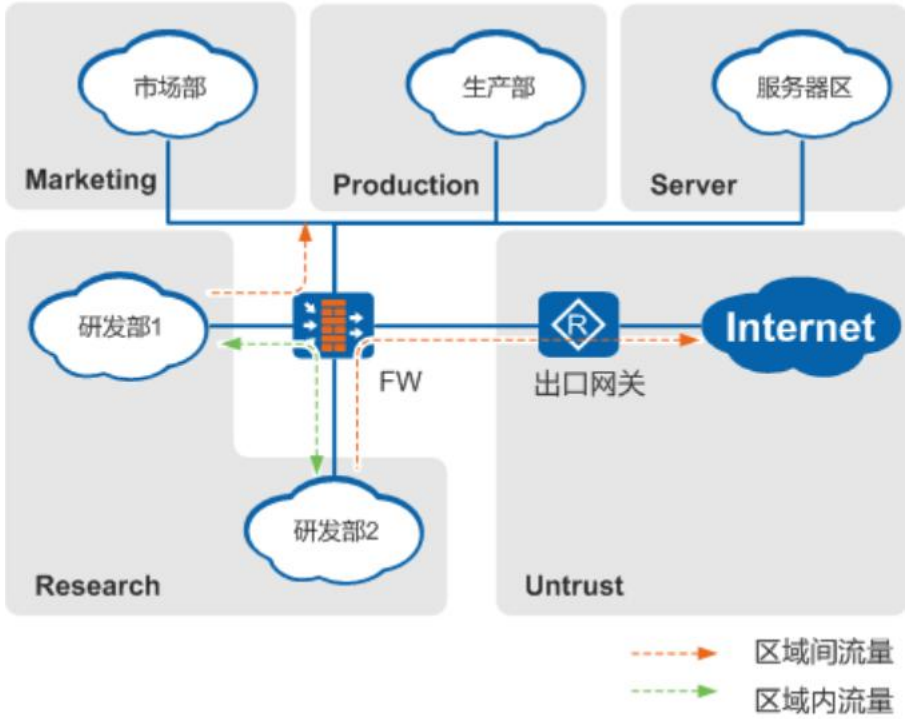
- 安全策略的应用场景——大中型企业边界防护

4. 在FW与出差员工、分支机构间建立VPN隧道，使用VPN保护公司业务流量，保证流量在Internet上安全传输。这时可以配置安全策略控制出差员工和分支机构访问总部内网的权限，并对分支机构和移动办公用户访问总部的流量进行内容安全检测，保护总部网络的安全。



防火墙 —— 安全策略

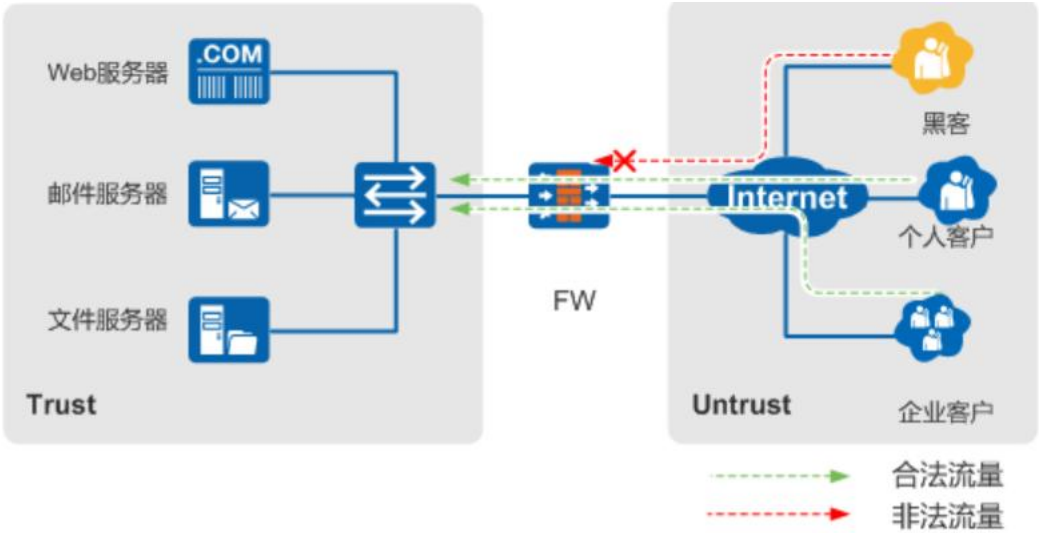
- 安全策略的应用场景——内网管控与安全隔离
  - 不同安全等级的网络划分到不同的安全区域，根据业务需求配置不同的安全策略，例如仅允许部分研发部的主机访问指定的市场部主机。
  - 在内网各个区域与外网之间配置安全策略。



防火墙 —— 安全策略

- 安全策略的应用场景——数据中心边界防护

1. 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。
2. 对Internet用户访问服务器的流量进行内容安全检测，保证内网服务器的安全。



防火墙 —— 安全策略

- 安全策略的应用场景——数据中心边界防护

3. 配置入侵防御、反病毒、APT防御功能，使服务器免受黑客入侵以及蠕虫、木马等病毒危害。
4. 配置文件过滤和内容过滤，避免数据泄露

防火墙 —— 安全策略

- 安全策略的匹配规则

1. 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。
2. 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（包括域内流量）均可以命中该策略。
3. 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。所以需要先配置条件精确的策略，再配置宽泛的策略。**防火墙的策略规则是从上到下依次遍历，当一些规则的范围发生冲突时，防火墙会以上面的规则为准进行过滤，因此在创建防火墙规则时，若实现其实验目的，则需调整规则顺序。**

防火墙 —— 安全策略

- 安全策略的匹配规则

4. 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）。

5. 不同安全区域间传输的流量（包括但不限于从FW发出的流量、FW接收的流量、不同安全区域间传输的流量），受缺省安全策略控制，缺省转发动作为禁止。

6. 同一安全区域内传输的流量不受缺省安全策略控制，缺省转发动作为允许。

防火墙应用

部署方式

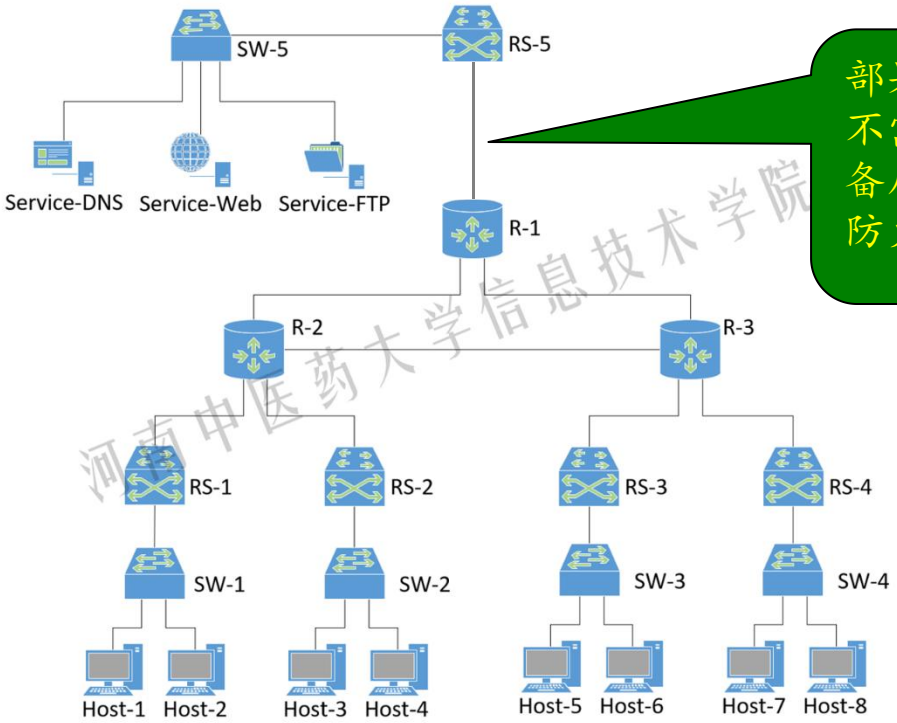
防火墙部署

- 透明接入
- 直路部署（路由方式）
- 旁挂方式
- 双机热备

防火墙部署 —— 透明接入

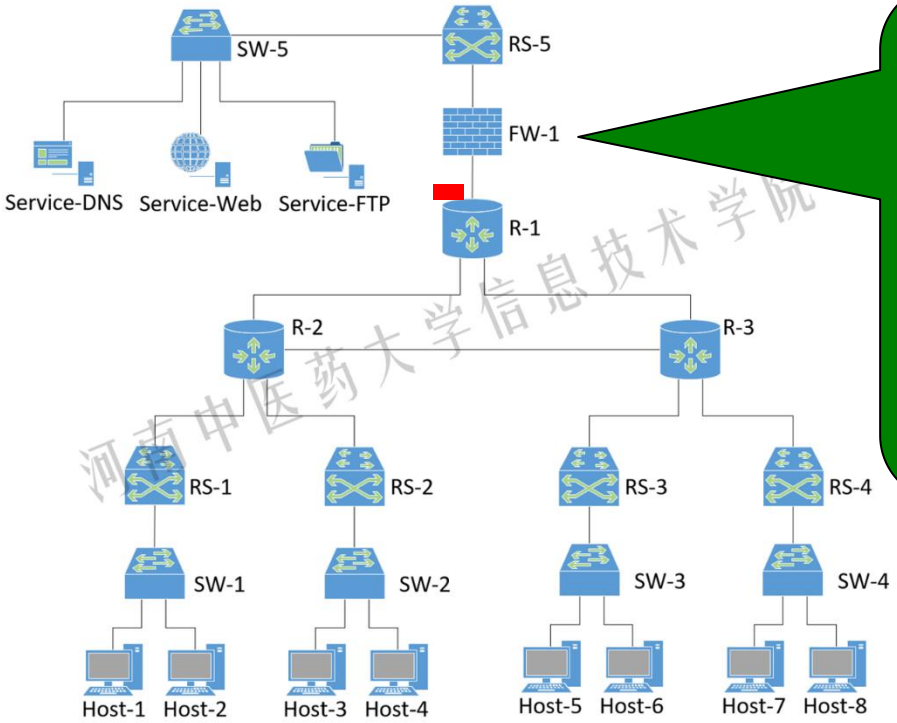
防火墙部署 —— 透明接入

- 透明接入



防火墙部署 —— 透明接入

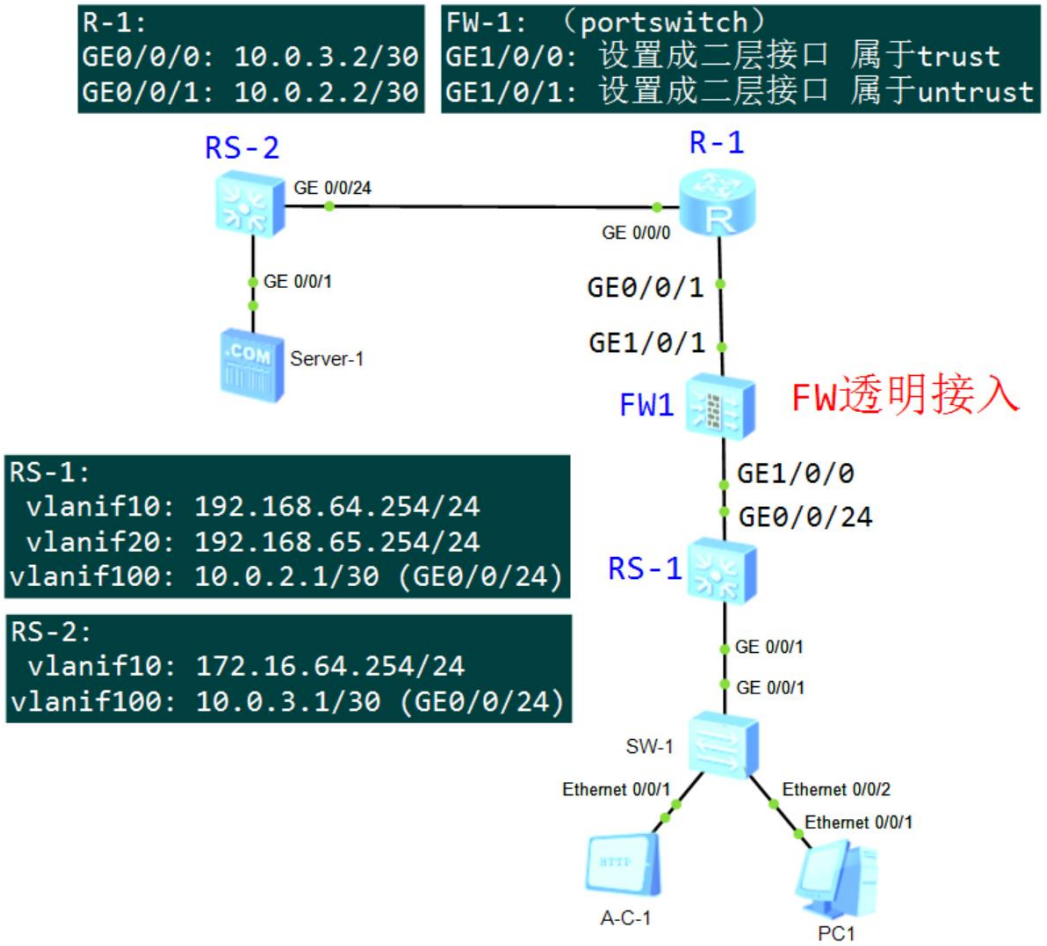
- 透明接入



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

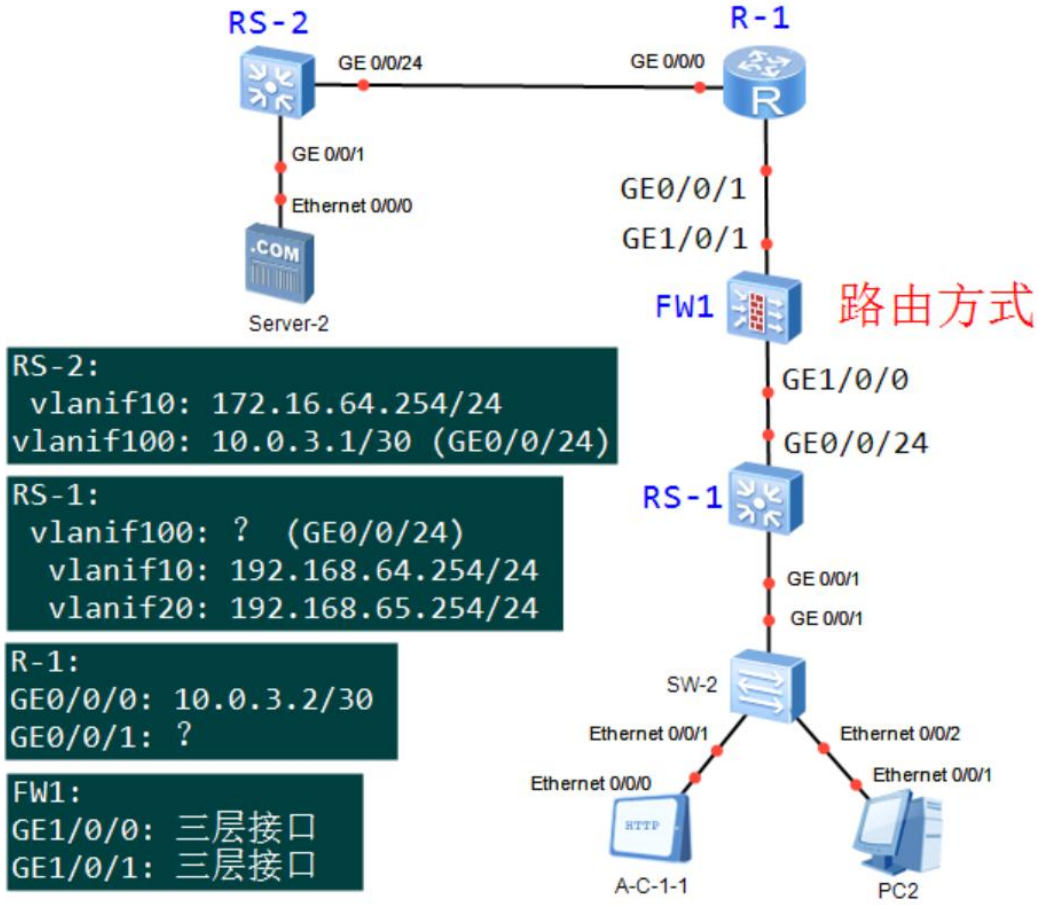
- 透明接入
  - FW接口配置分析
  - 上下行设备接口分析
  - 路由配置



防火墙部署 —— 直路接入（路由方式）

防火墙部署 —— 直路部署（路由方式）

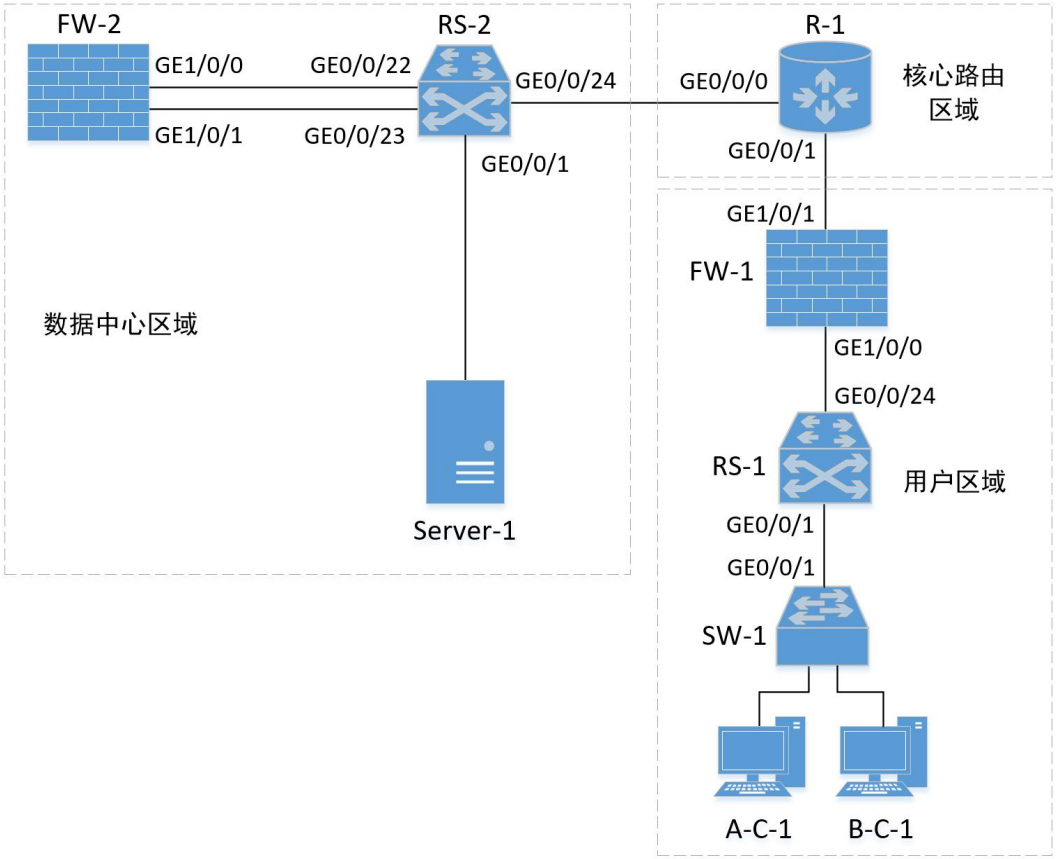
- 路由方式
  - FW接口配置分析
  - 上下行设备接口分析
  - 路由配置（OSPF区域）



防火墙部署 —— 旁挂方式

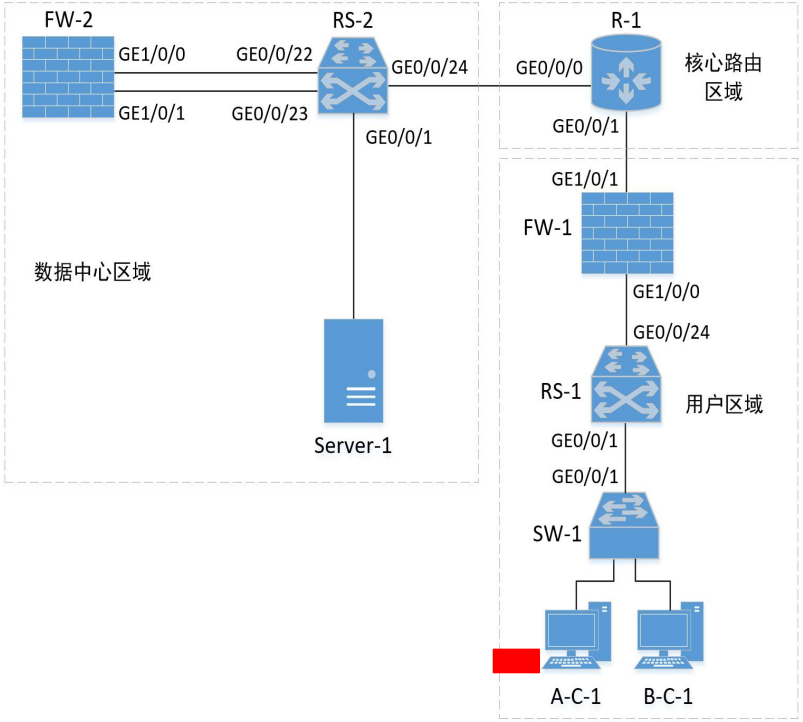
防火墙部署 —— 旁挂方式

- 防火墙旁挂



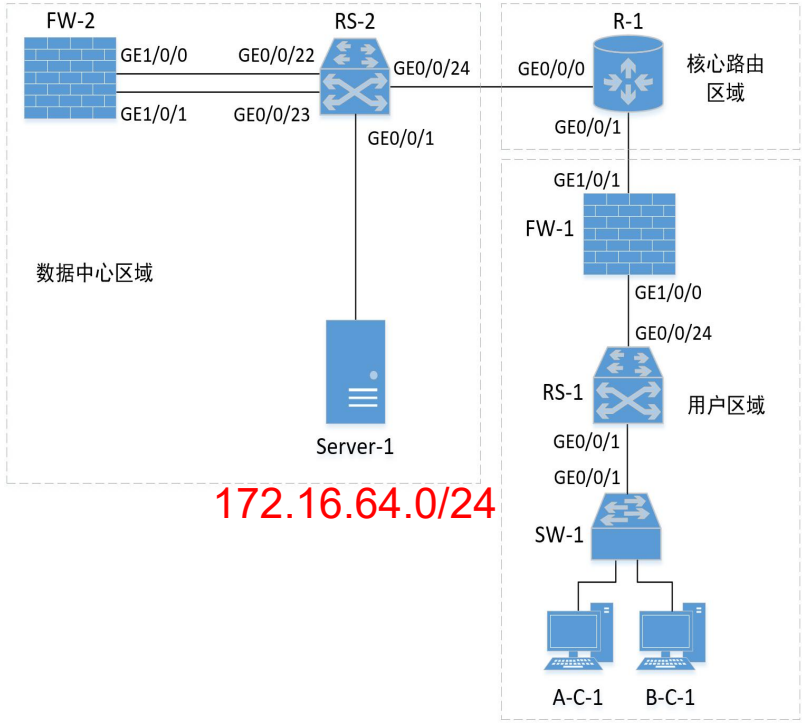
防火墙部署 —— 旁挂方式

- 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。



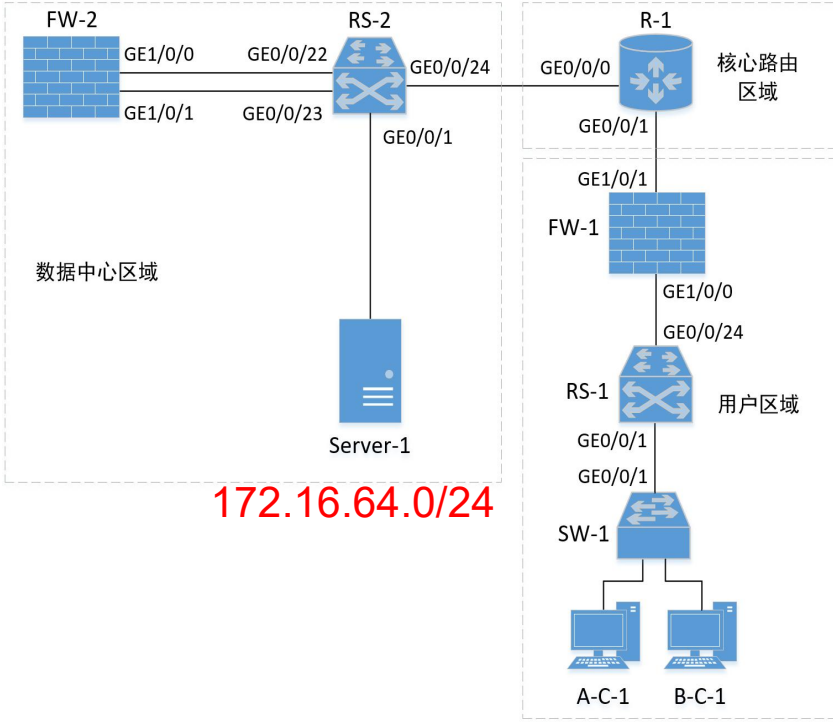
防火墙部署 —— 旁挂方式

- 思考：如何引流？
  - 使用静态路由？
  - 路由优先级的问题
    - 不同厂商的路由设备，其路由协议的优先级可能不同。例如Cisco设备的静态路由（度量值：1）、OSPF（度量值：110）路由协议。
    - 华为的设备是OSPF（度量值：10）路由协议优先于静态路由（度量值：60）。



防火墙部署 —— 旁挂方式

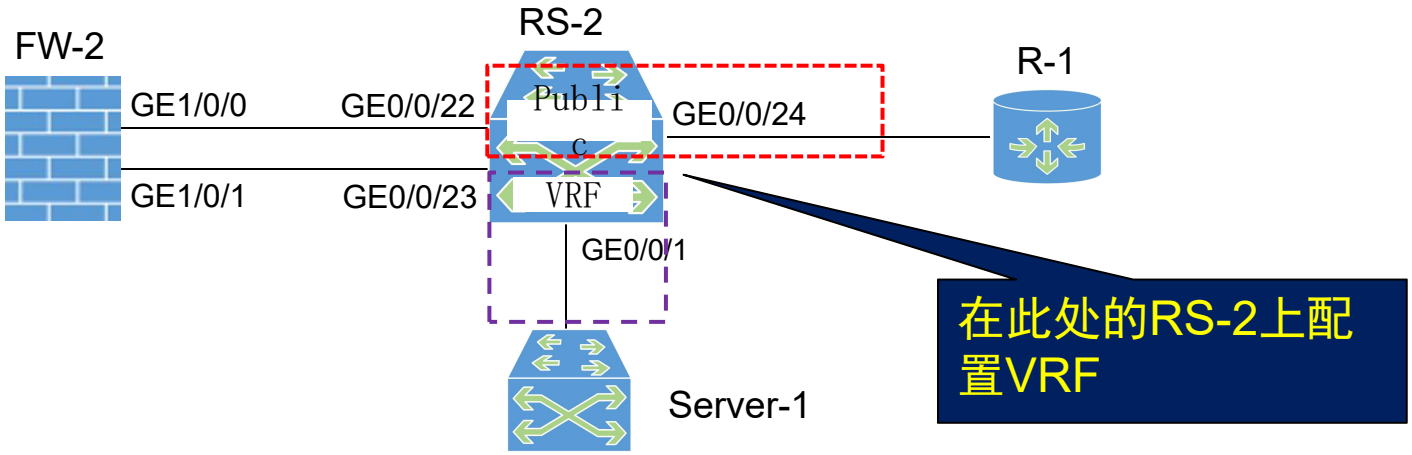
- 思考：如何引流？
  - 使用静态路由？
  - 分别在RS-2和FW-2上使用静态路由。
    - RS-2上：目的网络（172.16.64.0/24）下一跳为防火墙FW-2的GE1/0/0接口。
    - FW-2上：目的网络（172.16.64.0/24）下一跳为RS-2的GE0/0/23接口。
    - 接下来呢？
    - 从服务器返回用户区域呢？



防火墙部署 —— 旁挂方式

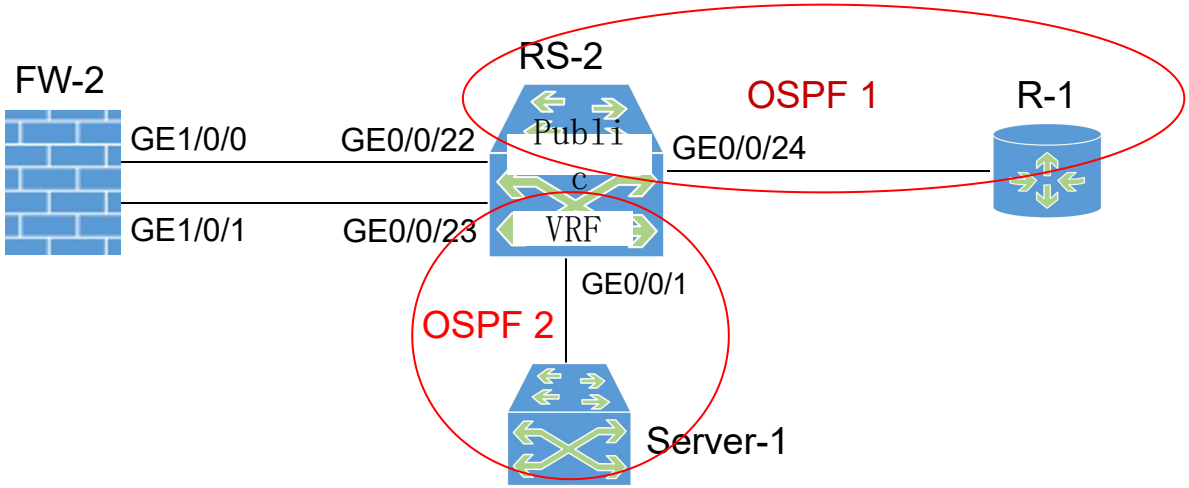
在此处的RS-2上配置VRF

- VRF的作用
  - VRF：Virtual Routing Forwarding，虚拟路由转发
  - 功能：VRF可将一台路由交换机虚拟成连接上行设备的交换机（根交换机Public）和连接下行设备的交换机（虚拟交换机VRF）。



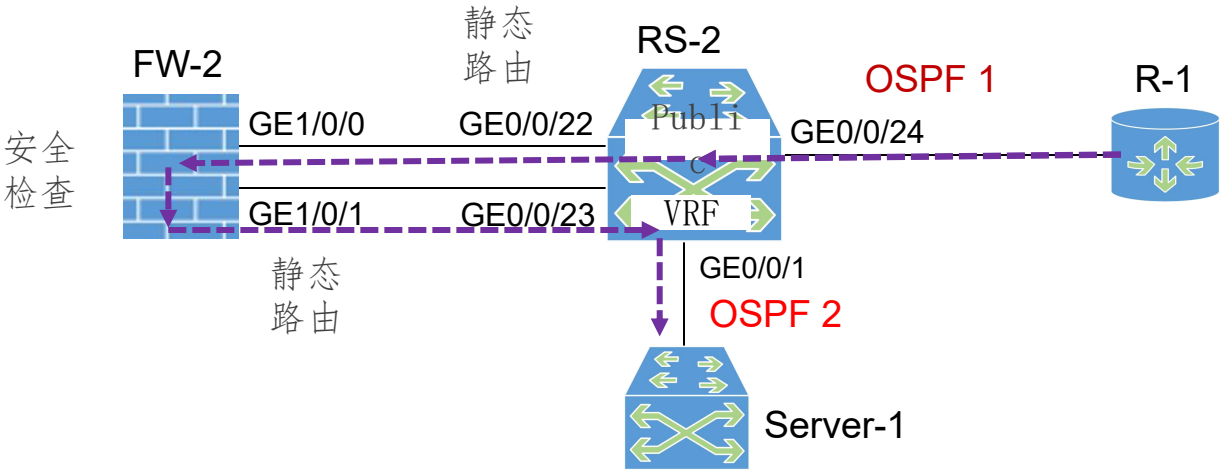
防火墙部署 —— 旁挂方式

- VRF的作用
  - 虚拟出的两个交换机（即Public和VRF）是完全隔离的，即Public和上行设备（例如R-1）之间的OSPF信息，与VRF和下行设备（此处用Server-1表示）之间的OSPF信息是完全隔离的。



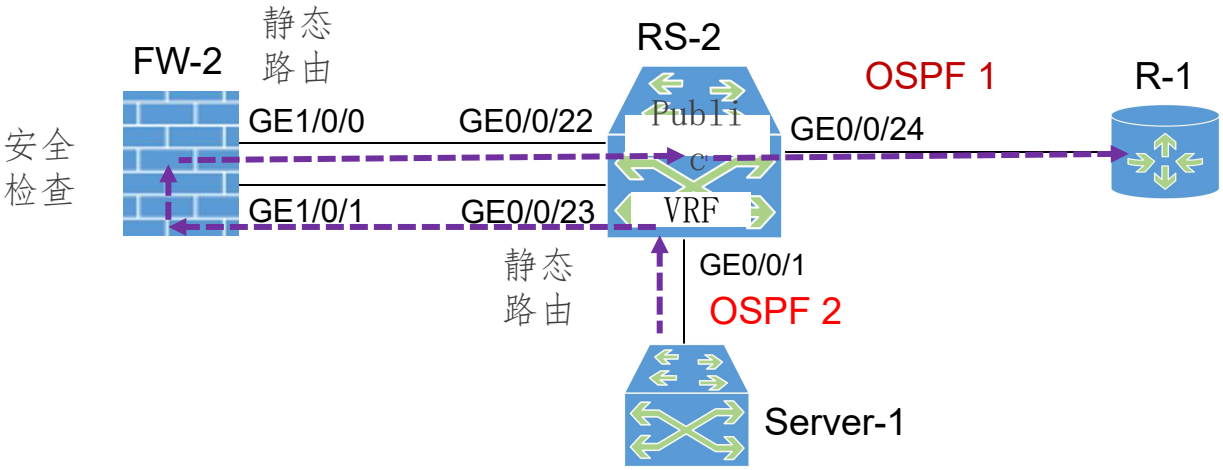
防火墙部署 —— 旁挂方式

- VRF的作用——对于下行流量
  - 当流量从上行设备R-1转发到RS-2（Public）时，不会被直接转发到RS-2（VRF），而是首先被配置在RS-2（Public）中的静态路由引流到防火墙FW-2上，经过防火墙安全策略过滤后，再被配置在FW-2上的静态路由转发到RS-2（VRF），并通过RS-2（VRF）中的OSPF信息，被进一步转发到下行设备（例如此处的Server-1）。



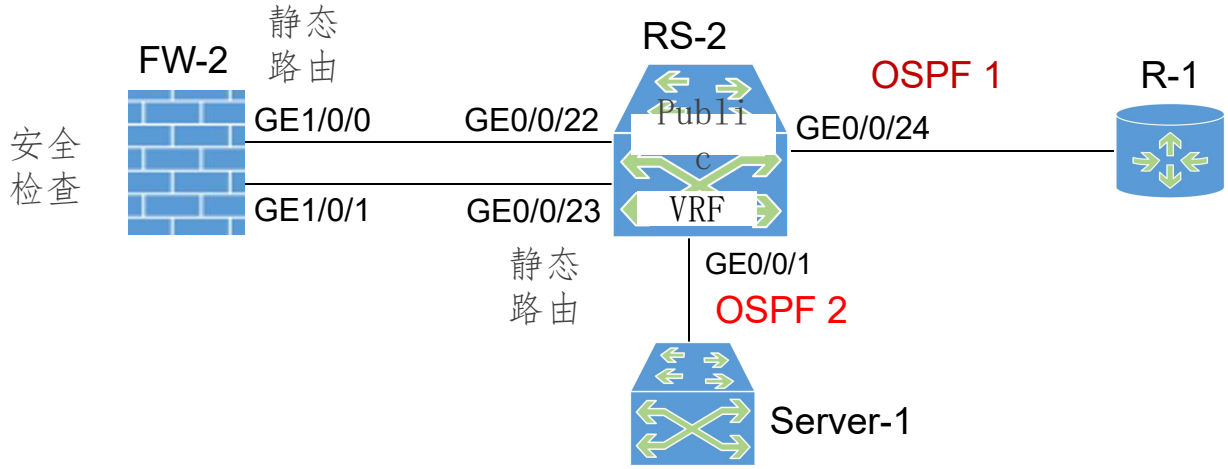
防火墙部署 —— 旁挂方式

- VRF的作用——对于上行流量
  - 当流量从下行设备（Server-1）发送到RS-2（VRF）时，不会被直接转发到RS-2（Public），而是首先被配置在RS-2（VRF）中的静态路由引流到防火墙FW-2上，经过防火墙安全策略过滤后，再被配置在FW-2上的静态路由转发到RS-2（Public），并通过RS-2（Public）中的OSPF信息，转发到上行设备（R-1）。



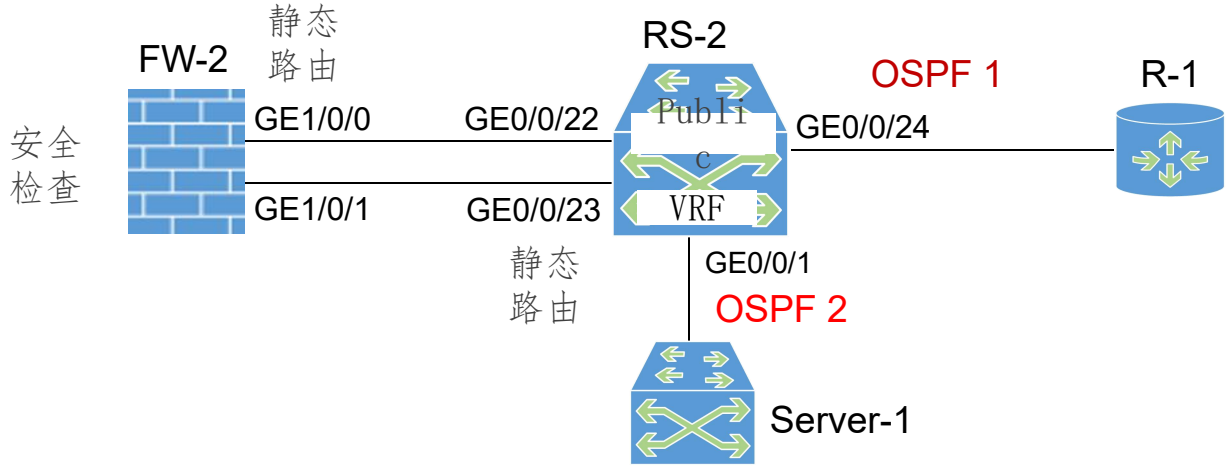
防火墙部署 —— 旁挂方式

- VRF的配置—— 要点1：在RS-2上创建名为VRF的VPN实例
  - 创建名为VRF的VPN实例。执行该命令，相当于创建了一个虚拟的路由转发表，
  - [RS-2]ip vpn-instance VRF



防火墙部署 —— 旁挂方式

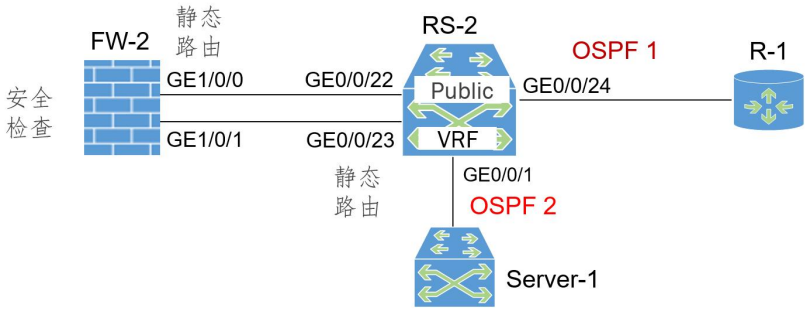
- VRF的配置—— 要点2：在RS-2上配置属于Public的接口
  - 将GE0/0/22和GE0/0/24所属VLAN的虚拟接口设置为Public接口。其配置方法与普通三层虚拟接口的配置过程相同
    - 创建VLAN200，并将GE0/0/22添加到VLAN200，设置为Access类型，配置VLANIF200接口的IP；
    - 同理，配置GE0/0/24



防火墙部署 —— 旁挂方式

- VRF的配置—— 要点3：在RS-2上配置属于VRF的接口
  - 将GE0/0/1和GE0/0/23所属VLAN的三层虚拟接口设置为VRF接口，即通过配置接口与VPN实例绑定，使该接口成为私网接口，从该接口进入的报文使用VPN实例，也就是RS-2（VRF）中的路由信息进行转发。

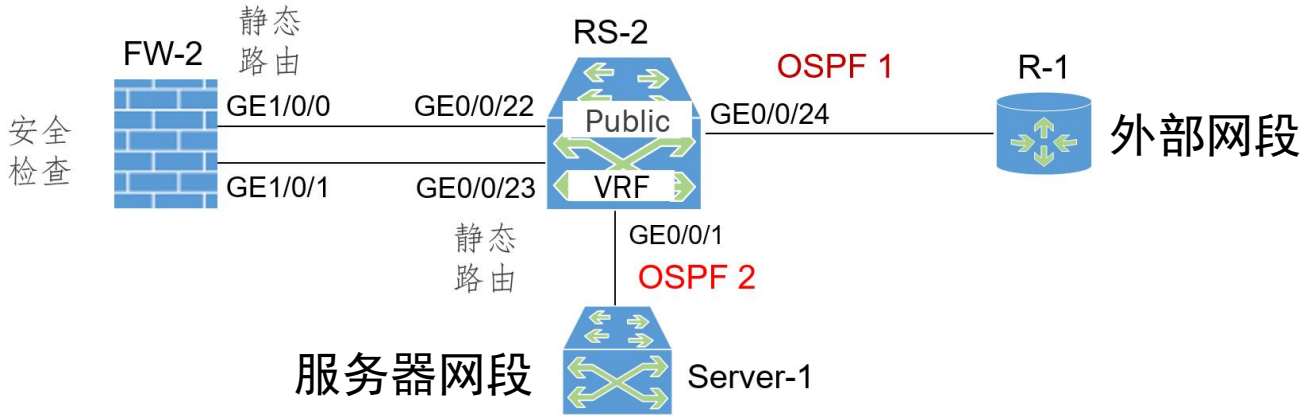
```
interface GigabitEthernet 0/0/1
port link-type access
Port default vlan 10
//将VLAN10与所创建的VPN实例绑定，即将VLANIF10设为VRF的接口，然后配置VLANIF10接口的IP地址
interface vlanif 10
ip binding vpn-instance VRF
ip address 172.16.64.254 24

同理配置GE0/0/23
```



防火墙部署 —— 旁挂方式

- VRF的配置——要点4：在RS-2上配置静态路由

静态路由所在设备	目的网络	下一跳	说明
RS-2（VRF）	0.0.0.0 /0	10.0.5.2	默认路由，从服务器网络发往外部网络的报文，到达RS-2（VRF）后，根据本路由被转发到FW-2的GE1/0/1接口（即10.0.5.2）
RS-2（Public）	172.16.64.0 /24	10.0.4.2	从外部网络发往服务器网段的报文，到达RS-2（Public）后，根据本静态路由被转发到FW-2的GE1/0/0接口（即10.0.4.2）



防火墙部署 —— 旁挂方式

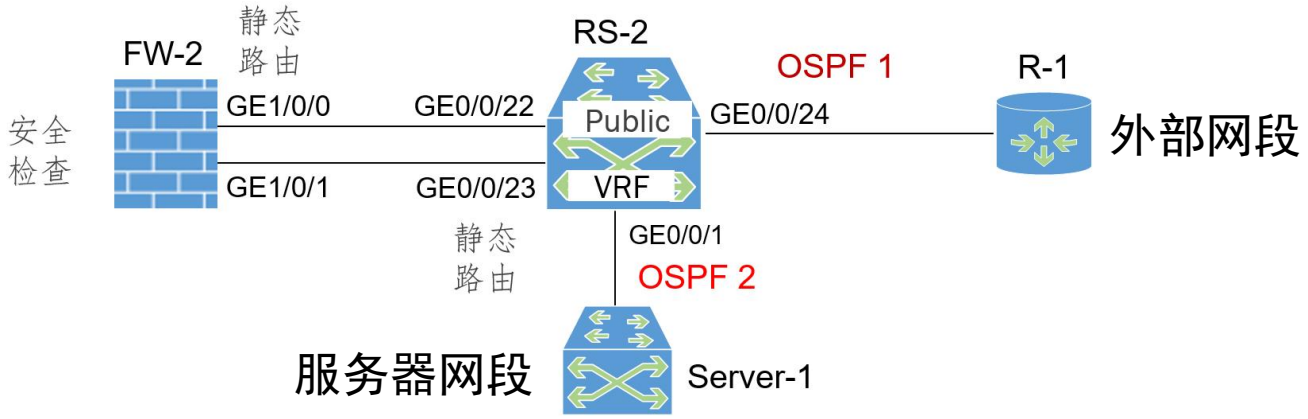
- VRF的配置—— 要点4：在RS-2上配置静态路由（命令）

//在VPN实例（VRF）中，配置一条默认路由。

[RS-2]ip route-static vpn-instance VRF 0.0.0.0 0.0.0.0 10.0.5.2

//在RS-2的Public中，配置一条静态路由

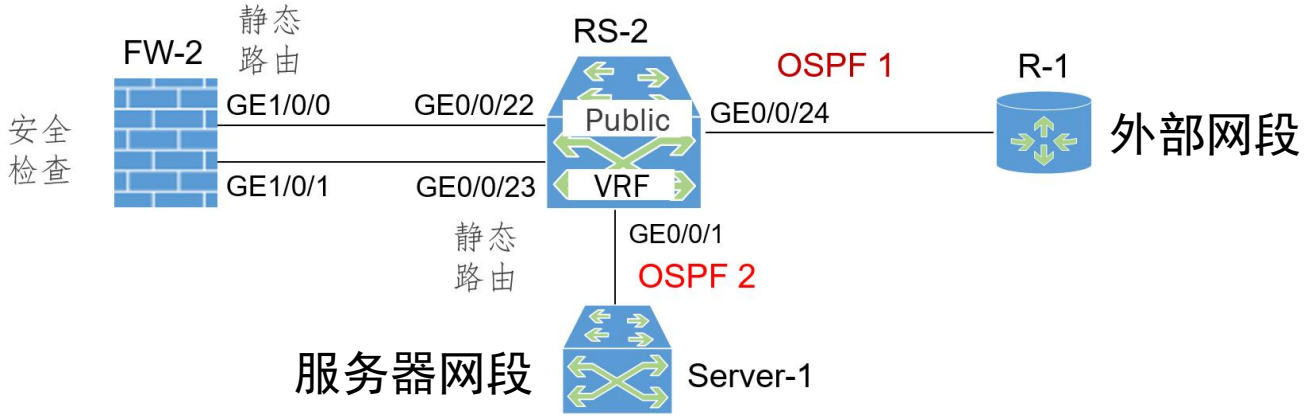
[RS-2]ip route-static 172.16.64.0 255.255.255.0 10.0.4.2



防火墙部署 —— 旁挂方式

- VRF的配置——要点5：在FW-2上配置静态路由

设备	目的网络	下一跳	说明
FW-2	0.0.0.0 /0	10.0.4.1	从服务器网络发往外部网络的报文，从RS-2（VRF）转发到FW-2，然后根据本路由，被转发到RS-2（Public）的三层虚拟接口（GE0/0/22）
FW-2	172.16.64.0 /24	10.0.5.1	从外部网络发往服务器的报文，从RS-2（Public）转发到FW-2，然后根据本静态路由，被转发到RS-2（VRF）的三层虚拟接口（GE0/0/23）

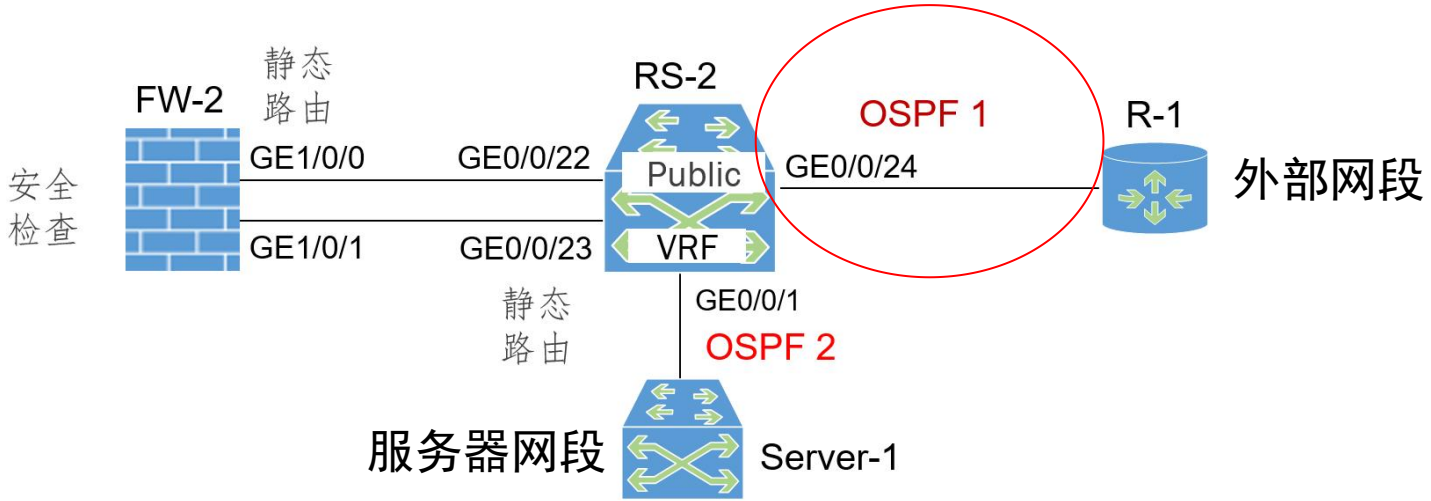


防火墙部署 —— 旁挂方式

- VRF的配置—— 要点6：在RS-2上配置动态路由（上行）

#在RS-2（Public）和其上行路由器R-1之间，配置OSPF路由协议，使得RS-2（Public）
#可以获取外部网络（例如用户区域网络）的路由信息。

```
[RS-2]ospf 1
[RS-2-ospf-1]area 0
[RS-2-ospf-1-area-0.0.0.0]network 10.0.3.0 0.0.0.3
```

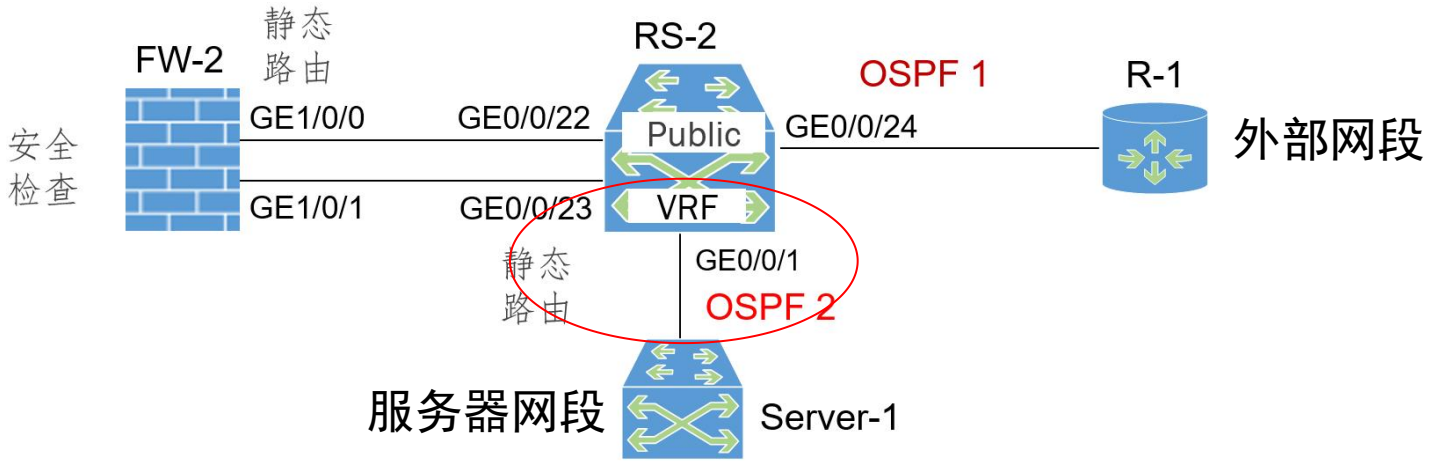


防火墙部署 —— 旁挂方式

- VRF的配置—— 要点7：在RS-2上配置动态路由（下行）

#在RS-2（VRF）和其下行路由设备之间，配置OSPF路由协议，使得RS-2（VRF）可以获取服务器网络的路由信息。（注意，此处不需要在VRF中配置OSPF，因为下行是服务器）

```
[RS-2]ospf 2 vpn-instance VRF
[RS-2-ospf-2]area 0
[RS-2-ospf-2-area-0.0.0.0]network *.*.*.* *.*.*.*
```



防火墙部署 —— 旁挂方式

- VRF的配置——要点8：显示RS-2（Public）的路由表信息

```
<RS-2>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Ro

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.0/30  OSPF    10   3           D   10.0.3.2        Vlanif100
        10.0.2.0/30  OSPF    10   2           D   10.0.3.2        Vlanif100
        10.0.3.0/30  Direct  0    0           D   10.0.3.1        Vlanif100
        10.0.3.1/32  Direct  0    0           D   127.0.0.1       Vlanif100
        10.0.4.0/30  Direct  0    0           D   10.0.4.1        Vlanif200
        10.0.4.1/32  Direct  0    0           D   127.0.0.1       Vlanif200
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    172.16.64.0/24   Static  60   0          RD   10.0.4.2        Vlanif200
   192.168.64.0/24   OSPF    10   4           D   10.0.3.2        Vlanif100
   192.168.65.0/24   OSPF    10   4           D   10.0.3.2        Vlanif100
```

display ip routing-table

防火墙部署 —— 旁挂方式

- VRF的配置—— 要点9：显示RS-2（VRF）的路由表信息

```
<RS-2>dis ip routing-table vpn-instance VRF
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: VRF
         Destinations : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD  10.0.5.2        Vlanif201
       10.0.5.0/30  Direct  0    0           D   10.0.5.1        Vlanif201
       10.0.5.1/32  Direct  0    0           D   127.0.0.1       Vlanif201
    172.16.64.0/24  Direct  0    0           D   172.16.64.254   Vlanif10
  172.16.64.254/32  Direct  0    0           D   127.0.0.1       Vlanif10
```

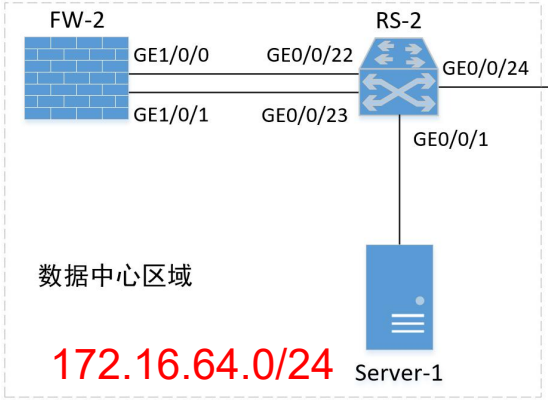
display ip routing-table vpn-instance VRF

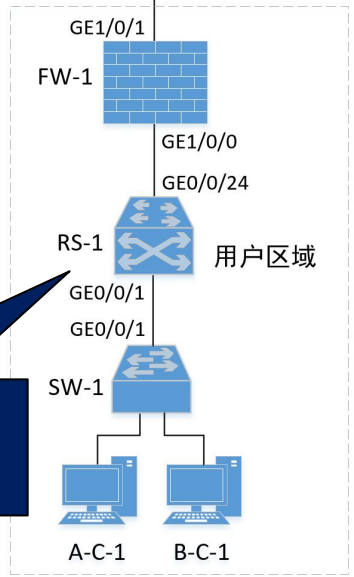
防火墙部署 —— 旁挂方式

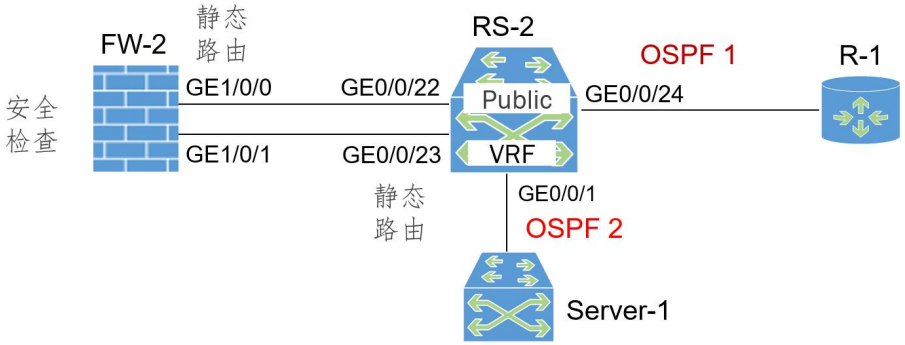
- 一个新情况—— 如何让用户区域获取到服务器网段的路由信息？

  - 由于RS-2的Public和VRF是相互隔离的，因此R-1无法通过OSPF获取服务器网段的路由信息，进而用户区域也获取不到！

  怎么办？



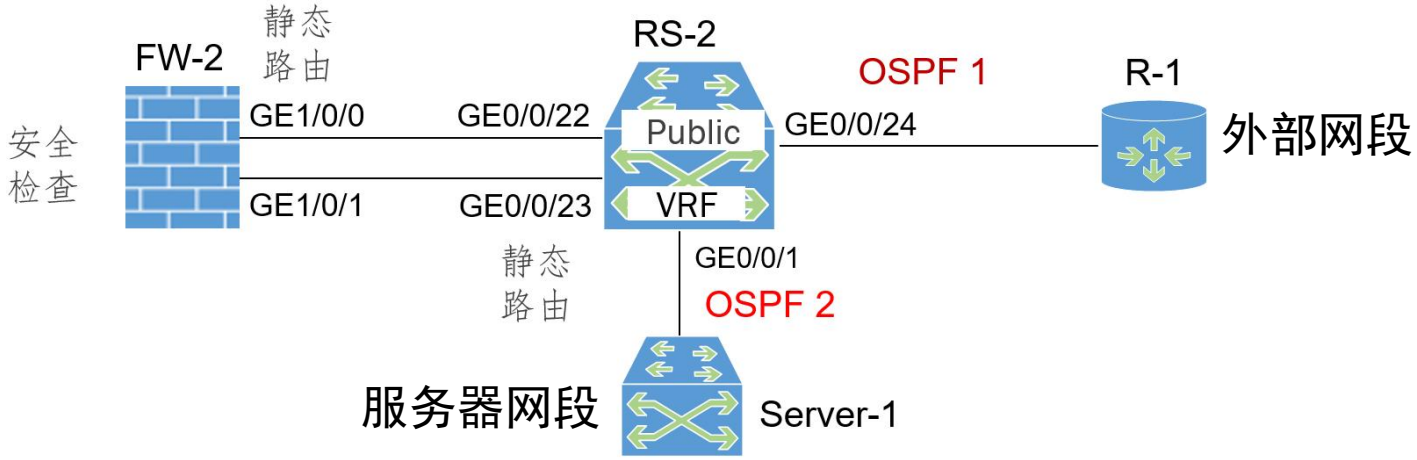




去往服务器网络，该怎么转发？

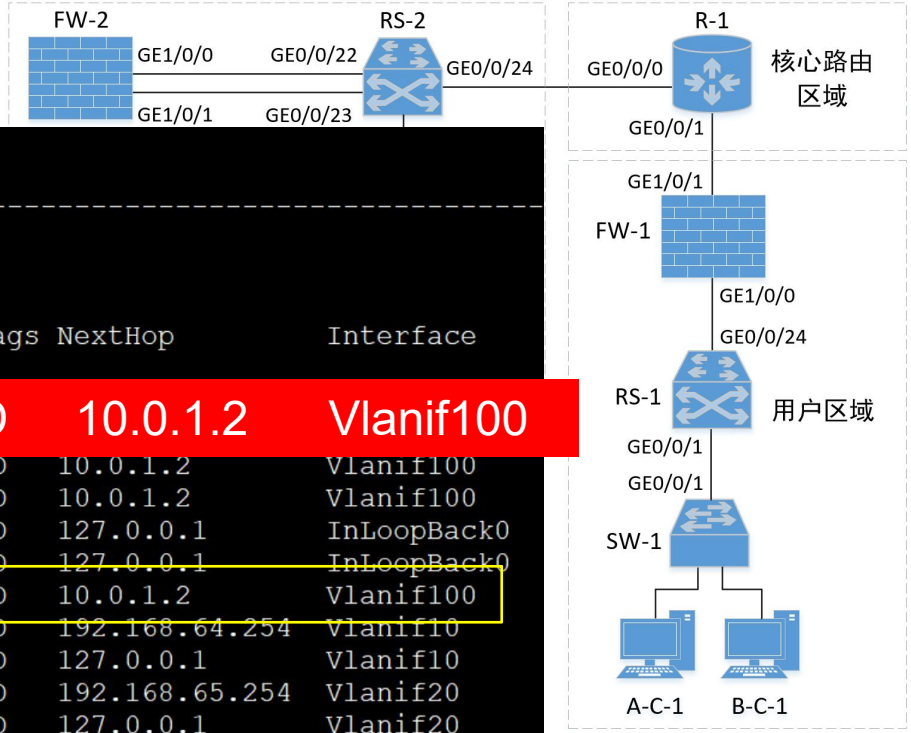
防火墙部署 —— 旁挂方式

- 一个新情况—— 如何让用户区域获取到服务器网段的路由信息？
  - 在R-1上配置静态路由，将目的网络是服务器网段的报文转发至RS-2（Public）。
    [R-1]ip route-static 172.16.64.0 255.255.255.0 10.0.3.1
  - 在R-1上配置ospf路由，并将配置的静态路由引入到OSPF中，使得外部网络中的其他路由设备可通过OSPF获取到该静态路由信息，即知道服务器网段的报文该如何转发。
    [R-1-ospf-1]import-route static



防火墙部署 —— 旁挂方式

- 一个新情况—— 如何让用户区域获取到服务器网段的路由信息？
  - 查看RS-1的路由表




```
<RS-1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

172.16.64.0/24   O_ASE   150  1           D   10.0.1.2        Vlanif100
        10.0.2.0/30  OSPF    10   2           D   10.0.1.2        Vlanif100
        10.0.3.0/30  OSPF    10   3           D   10.0.1.2        Vlanif100
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.16.64.0/24  O_ASE   150  1           D   10.0.1.2        Vlanif100
   192.168.64.0/24   Direct  0    0           D   192.168.64.254  Vlanif10
 192.168.64.254/32   Direct  0    0           D   127.0.0.1       Vlanif10
   192.168.65.0/24   Direct  0    0           D   192.168.65.254  Vlanif20
 192.168.65.254/32   Direct  0    0           D   127.0.0.1       Vlanif20
```

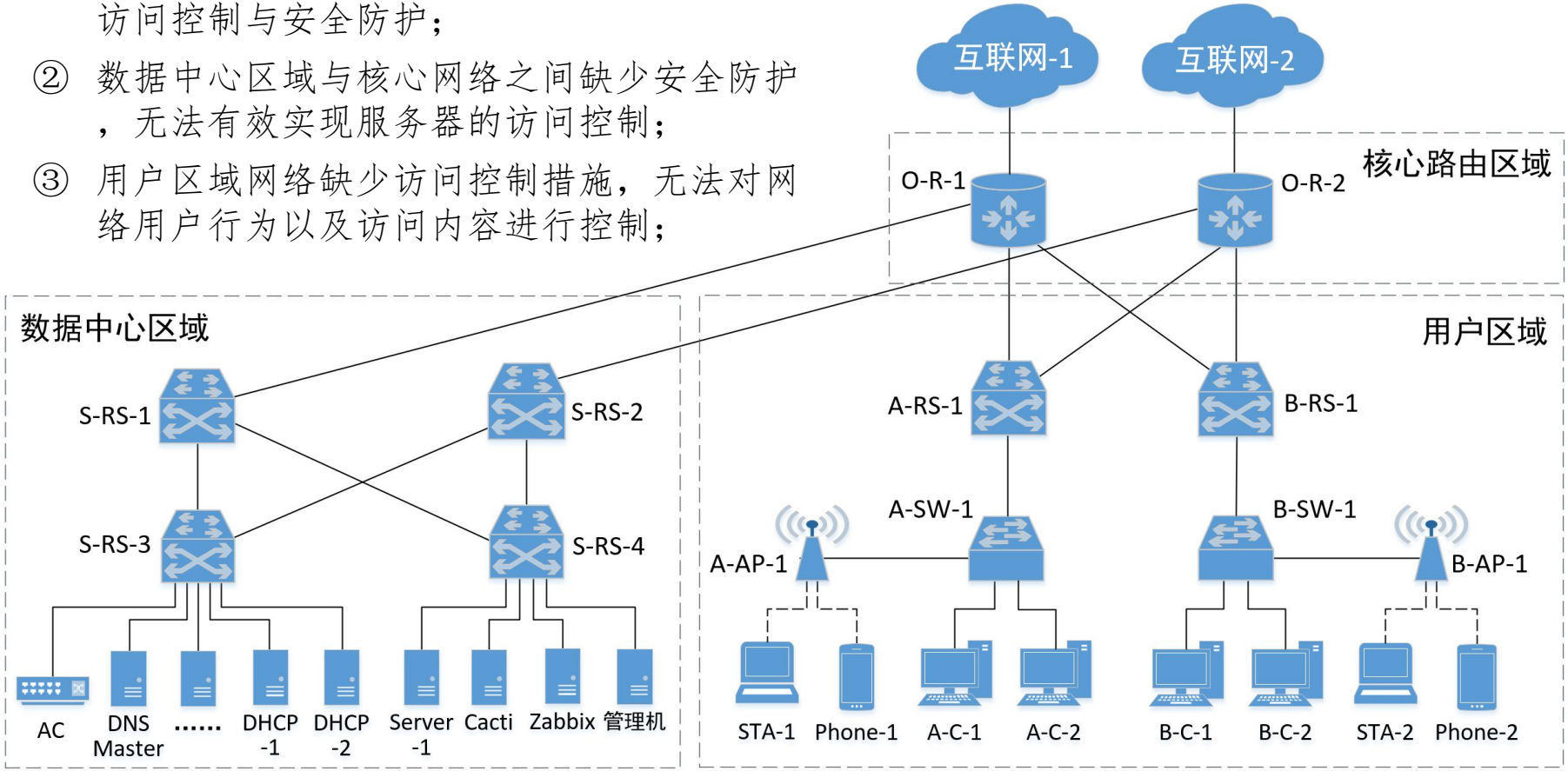
防火墙部署 —— 双机热备

分析：

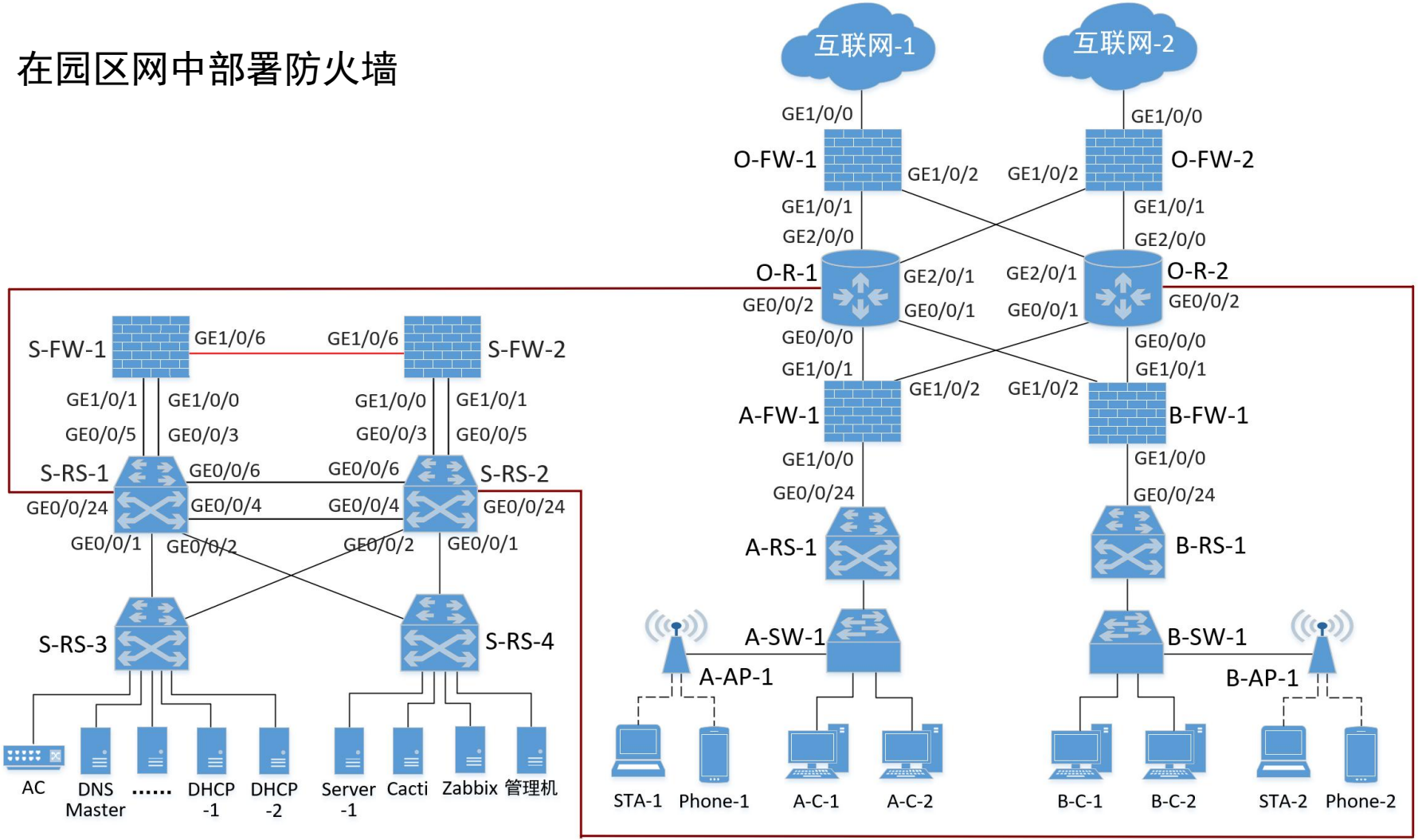
① 园区网接入互联网区域无法实现边界网络的访问控制与安全防护；

② 数据中心区域与核心网络之间缺少安全防护，无法有效实现服务器的访问控制；

③ 用户区域网络缺少访问控制措施，无法对网络用户行为以及访问内容进行控制；



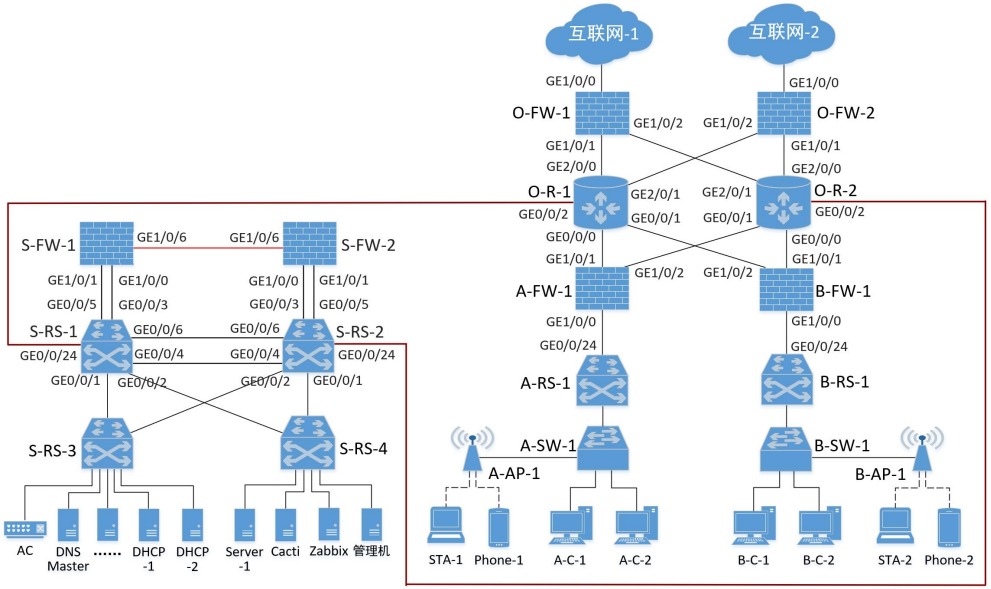
在园区网中部署防火墙


互联网-1
互联网-2
GE1/0/0
GE1/0/0
O-FW-1
GE1/0/2
GE1/0/2
O-FW-2
GE1/0/1
GE1/0/1
GE2/0/0
GE2/0/0
O-R-1
GE2/0/1
GE2/0/1
O-R-2
GE0/0/2
GE0/0/1
GE0/0/1
GE0/0/2
GE0/0/0
GE0/0/0
GE1/0/1
GE1/0/1
A-FW-1
GE1/0/2
GE1/0/2
B-FW-1
GE1/0/0
GE1/0/0
GE0/0/24
GE0/0/24
A-RS-1
B-RS-1
A-SW-1
B-SW-1
A-AP-1
B-AP-1
S-FW-1
GE1/0/6
GE1/0/6
S-FW-2
GE1/0/1
GE1/0/0
GE1/0/0
GE1/0/1
GE0/0/5
GE0/0/3
GE0/0/3
GE0/0/5
S-RS-1
GE0/0/6
GE0/0/6
S-RS-2
GE0/0/24
GE0/0/4
GE0/0/4
GE0/0/24
GE0/0/1
GE0/0/2
GE0/0/2
GE0/0/1
S-RS-3
S-RS-4
AC
DNS Master
.....
DHCP -1
DHCP -2
Server -1
Cacti
Zabbix
管理机
STA-1
Phone-1
A-C-1
A-C-2
B-C-1
B-C-2
STA-2
Phone-2

防火墙部署 —— 双机热备

数据中心区域网络

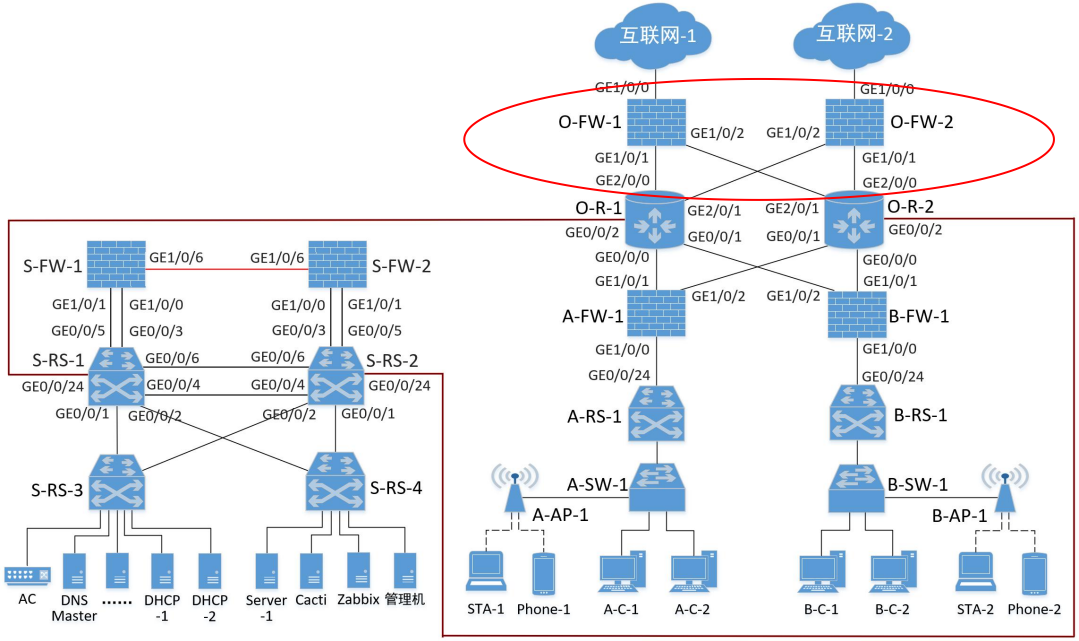
- 防火墙S-FW-1和S-FW-2，分别旁挂在数据中心的汇聚交换机S-RS-1和S-RS-2上。
- 通过配置VRF（虚拟路由转发），配合静态路由，实现进出数据中心区域的流量，首先引流到旁挂的防火墙上进行安全检测。



防火墙部署 —— 双机热备

边界接入网络

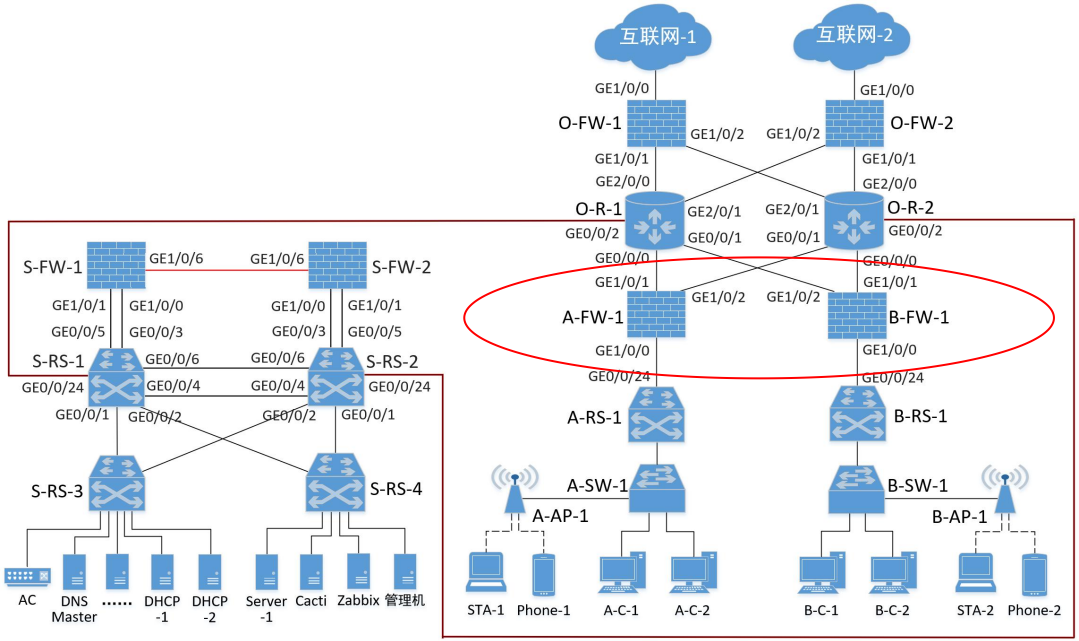
- 在园区网边界的接入网络中增加两台防火墙，通过配置双链路NAT及配置安全策略，实现出口访问控制与设备灾备。
- 当外部网络需要访问内部网络资源时将受到控制，例如必须以VPN方式进行访问。



防火墙部署 —— 双机热备

用户区域网络

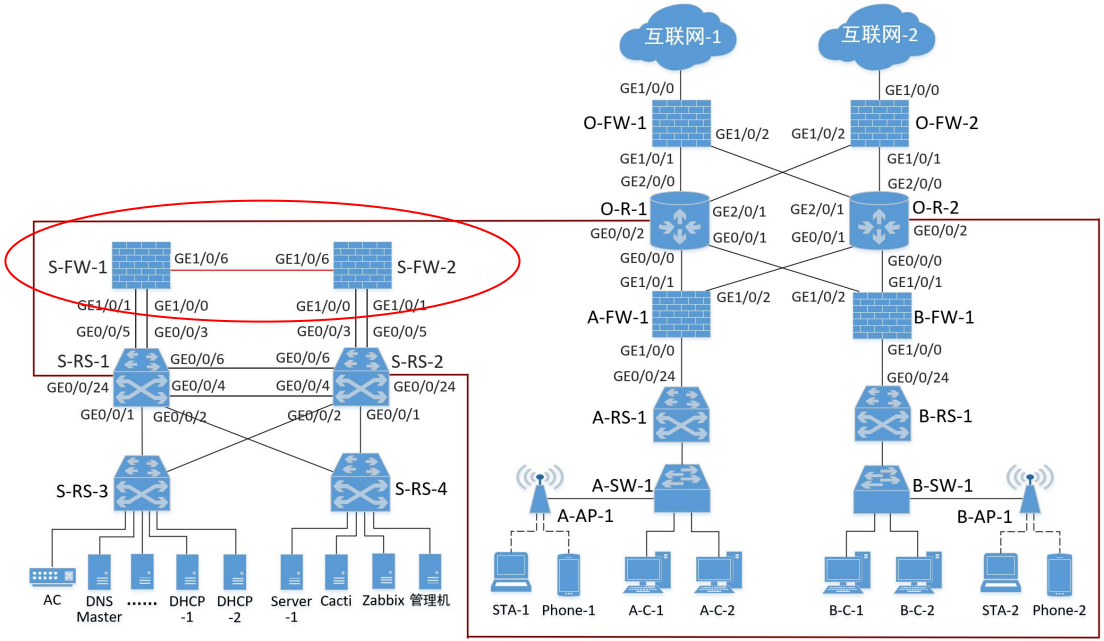
- 每个用户区域通过一台防火墙连接到核心路由器，控制园区网用户对网络资源的访问。



防火墙部署 —— 双机热备

数据中心网络

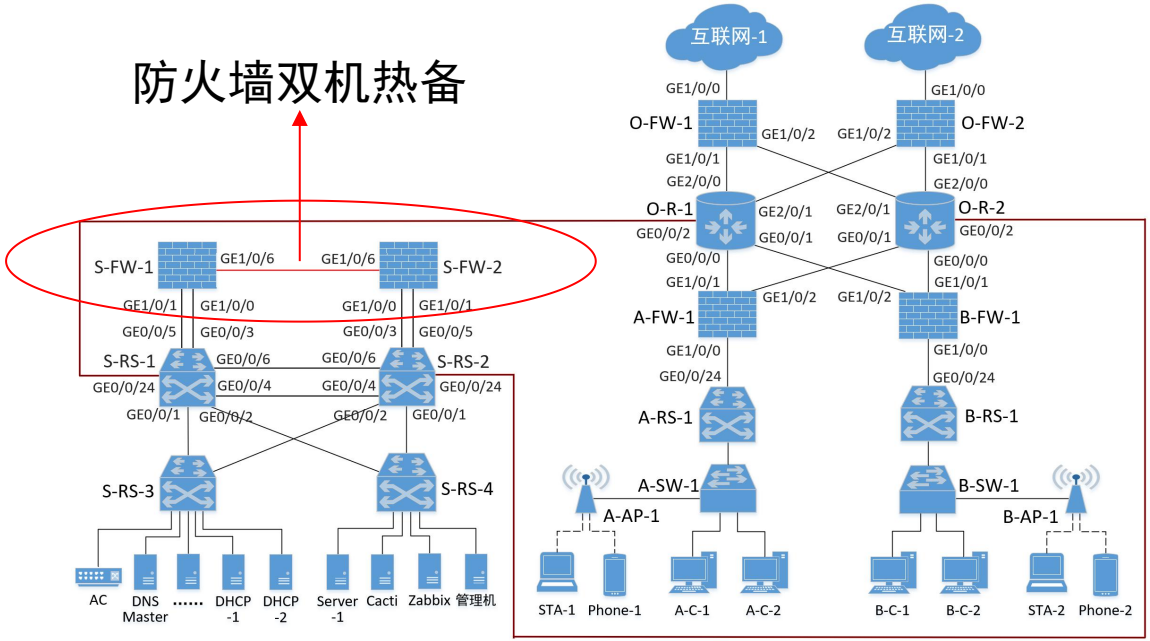
- S-RS-1和S-RS-2配置了VRF
- 数据中心的边界区域增加两台防火墙，旁挂部署，进出数据中心网络的流量必须先引流到防火墙，经过防火墙安全策略过滤后，再进一步转发。



防火墙部署 —— 双机热备

数据中心网络

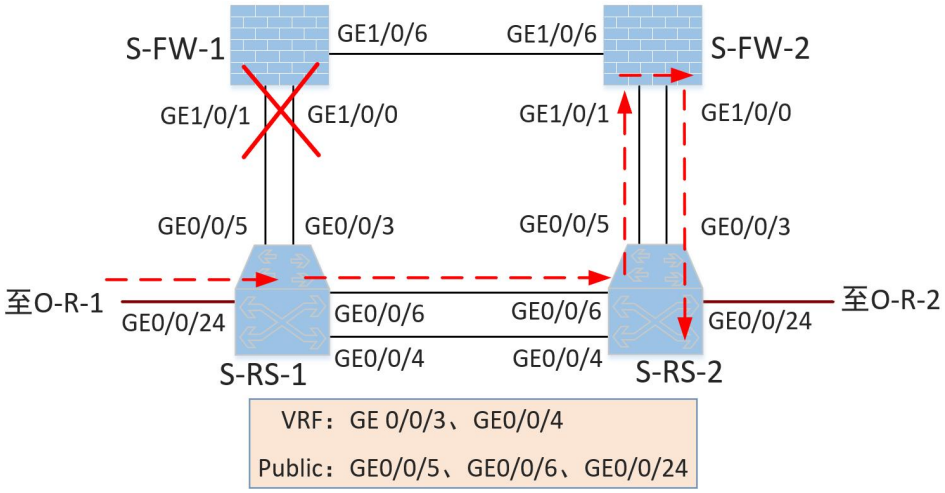
- 为了实现数据中心防火墙的设备灾备，将两台防火墙设置为双机热备，当一台出现故障时，可通过另一台进行工作。
- 此外，两台防火墙的工作方式为负载分担，即正常情况两台防火墙分担通信流量，若一台出现故障，则另一台承担全部流量。



防火墙部署 —— 双机热备

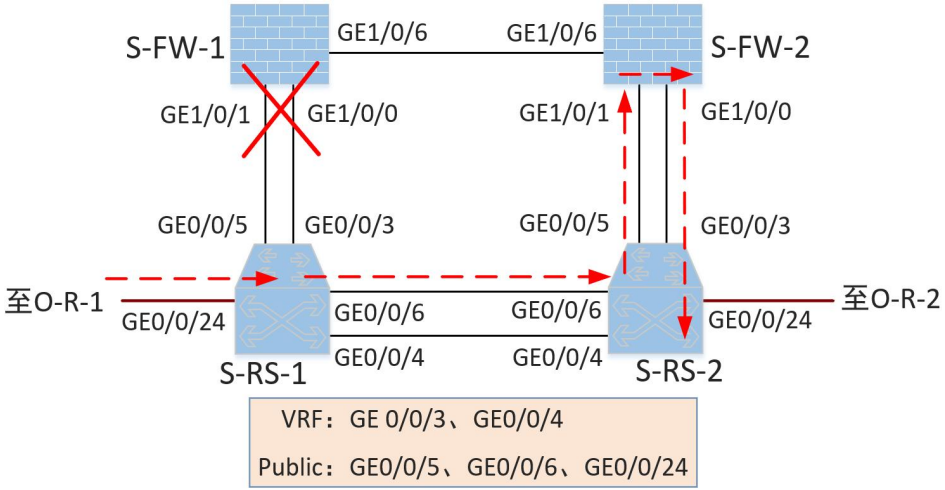
防火墙双机热备规划设计

- 当S-FW-1故障时，从外部网络发往服务器的报文，到达S-RS-1后，不再发往S-FW-1，而是通过GE0/0/6接口（属于Public）到达S-RS-2（GE0/0/6），然后再通过S-RS-2的Public的GE0/0/5接口发至S-FW-2，完成报文过滤后，再发回至S-RS-2的VRF，并进一步转发至目的地服务器。从而实现当一台防火墙故障时，报文可以通过另一台防火墙进行过滤、通信。



防火墙部署 —— 双机热备

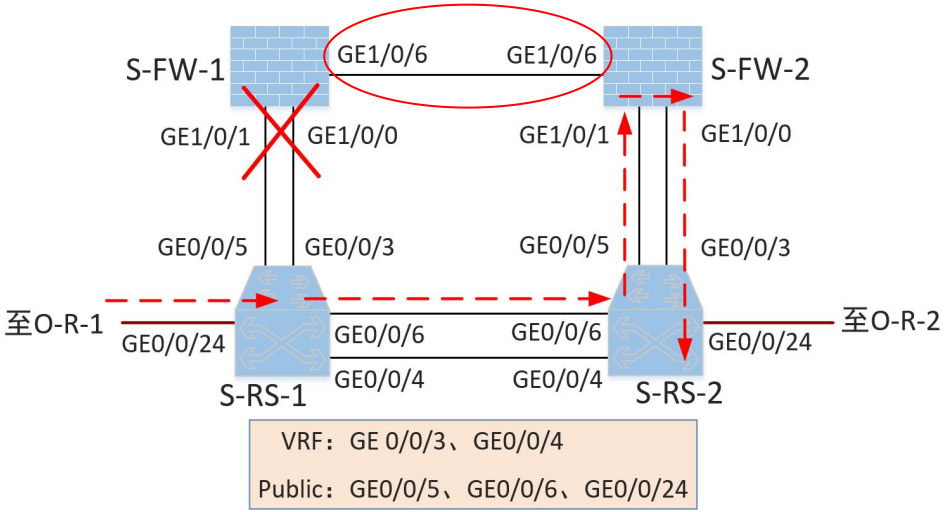
- 分析1：两台防火墙之间，会话表的相互同步问题
  - 报文通过S-FW-1时，会根据安全策略形成会话表。当S-FW-1故障，报文转而从S-FW-2通过时，若S-FW-2上没有之前流量的会话表，之前传输会话的的返回流量将无法通过S-FW-2，而会话的后续流量需要重新经过安全策略的检查，并生成会话。这就意味着之前所有的通信流量都将中断，除非重新建立连接。



防火墙部署 —— 双机热备

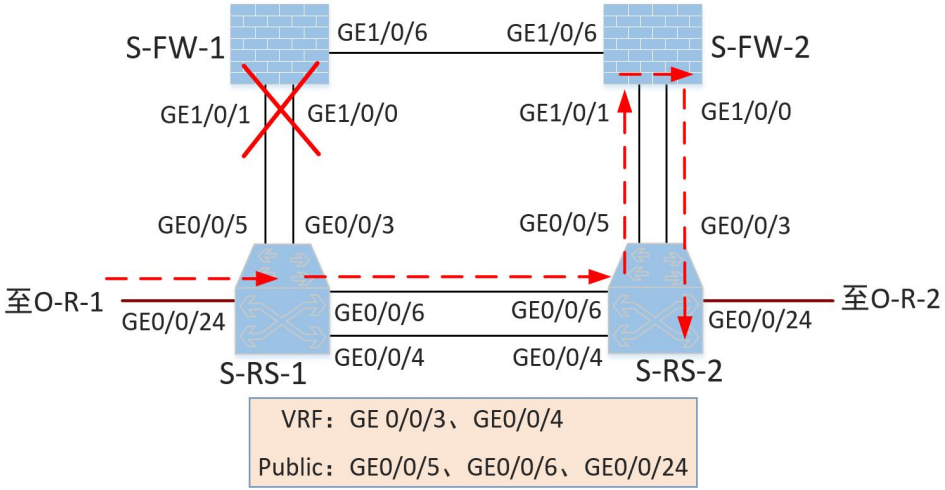
分析1：两台防火墙之间，会话表的相互同步问题

- 华为防火墙通过提供一条备份链路（心跳线，如图中的GE1/0/6接口链路），协商防火墙之间的主备状态及备份会话表、Server-map表等操作。根据防火墙的配置分别选举出主用设备及备用设备，当主用设备正常工作时，备用设备不提供数据包的转发，但是备用设备会实时从主用设备下载当前的会话表等。从而保证，当主用设备故障时，即使切换到备用设备，备用设备依然存在当前流量的会话表及Server-map表，从而保证业务流量不中断



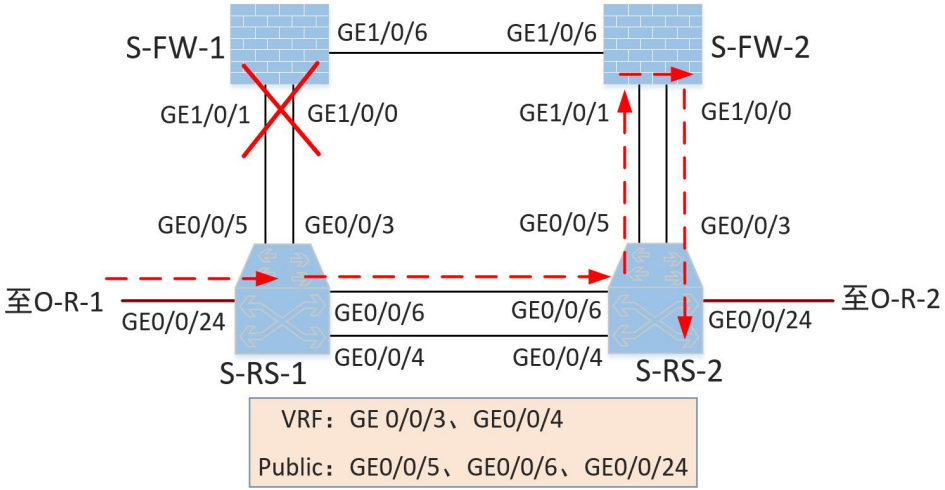
防火墙部署 —— 双机热备

- 分析1：两台防火墙之间，会话表的相互同步问题
  - 华为防火墙的双机热备包含以下两种模式：主备备份模式和负载分担模式
    - 主备备份模式：同一时间只用一台防火墙转发数据包，其他防火墙不转发数据包，但是会通过心跳线同步会话表及Server-map表；
    - 负载分担模式：同一时间，多台防火墙同时转发数据，每个防火墙即是主用设备也是备用设备，防火墙之间同步会话表及Server-map表。
    - 本任务中，两台旁挂防火墙采用负载分担模式工作。



防火墙部署 —— 双机热备

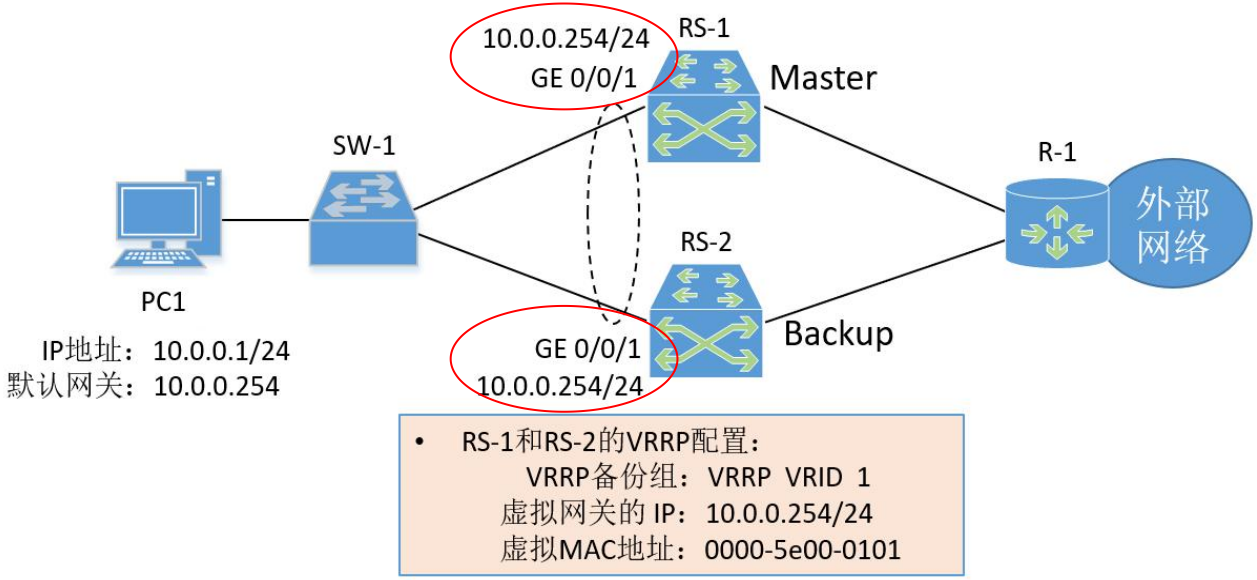
- 分析2：下一跳（网关）的自动切换问题（1）
  - 当S-FW-1故障时，从S-RS-1的GE0/0/5发出，发往S-FW-1的GE1/0/1的流量，如何自动切换，发往S-FW-2的GE1/0/1？
    - 提醒：S-RS-1和S-FW-1之间是静态路由！
    - 所以，要保证双机热备可以正常工作，还需解决客户机网关自动切换的问题，这就要用到VRRP技术。



防火墙部署 —— 双机热备

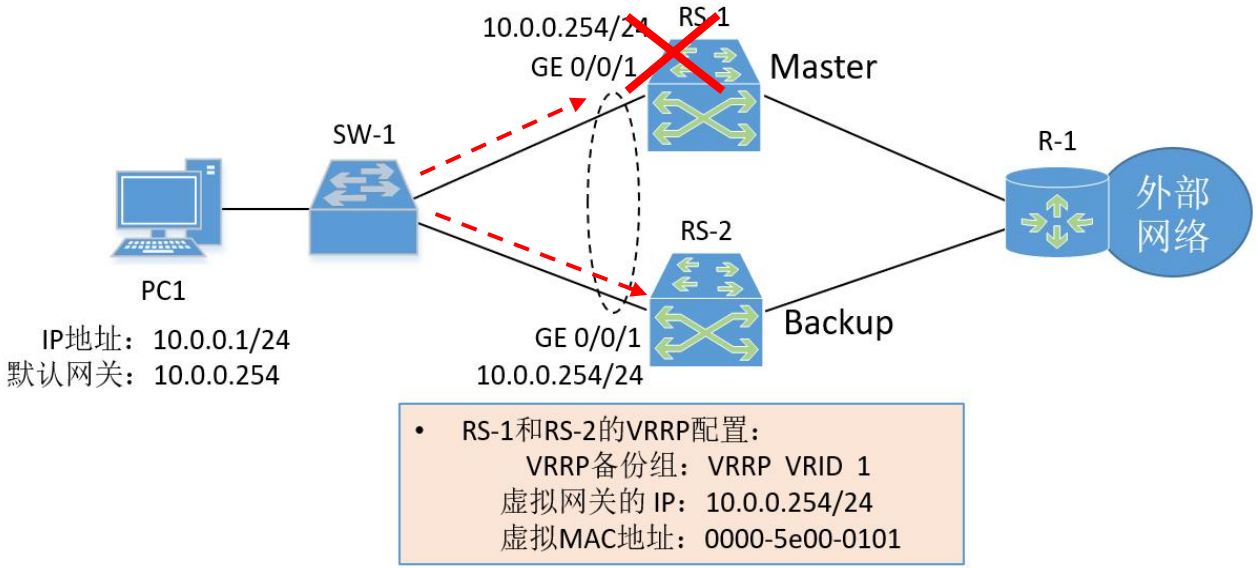
分析2：下一跳（网关）的自动切换问题（2）

- 虚拟路由冗余协议 VRRP（Virtual Router Redundancy Protocol），通过把几台路由设备上的网关接口联合组成一个虚拟网关，将该虚拟网关的 IP 地址作为用户的默认网关实现与外部网络通信。



防火墙部署 —— 双机热备

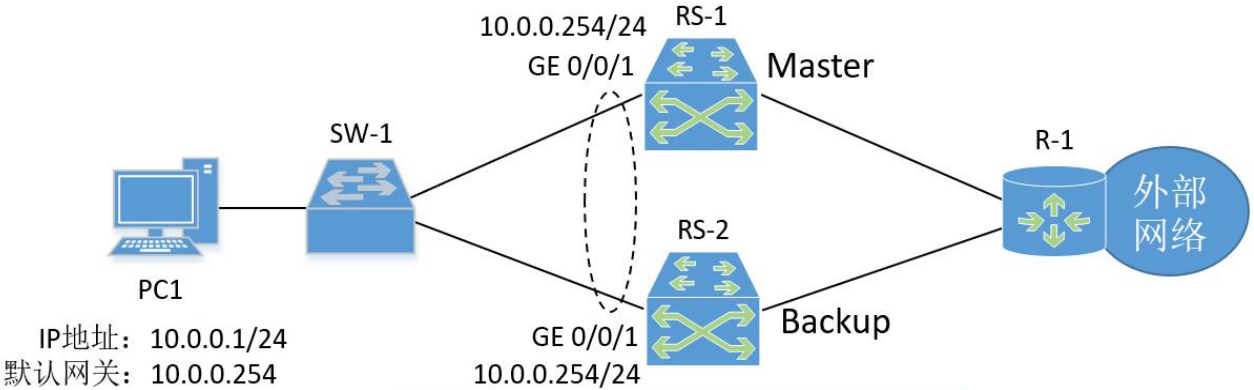
- 分析2：下一跳（网关）的自动切换问题（3）
  - 当一台网关设备发生故障时，VRRP 机制能够自动选举新的网关设备承担数据流量，无需修改主机及网关设备的配置信息便可有效避免单一链路发生故障后的网络中断问题



防火墙部署 —— 双机热备

分析2：下一跳（网关）的自动切换问题（4）—— 几个概念

- VRRP路由器：运行VRRP协议的路由器，也可以是路由交换机或防火墙；
- 虚拟路由器：由一个主用路由器和若干备用路由器组成的一个备份组，一个备份组对客户机提供一个虚拟网关；

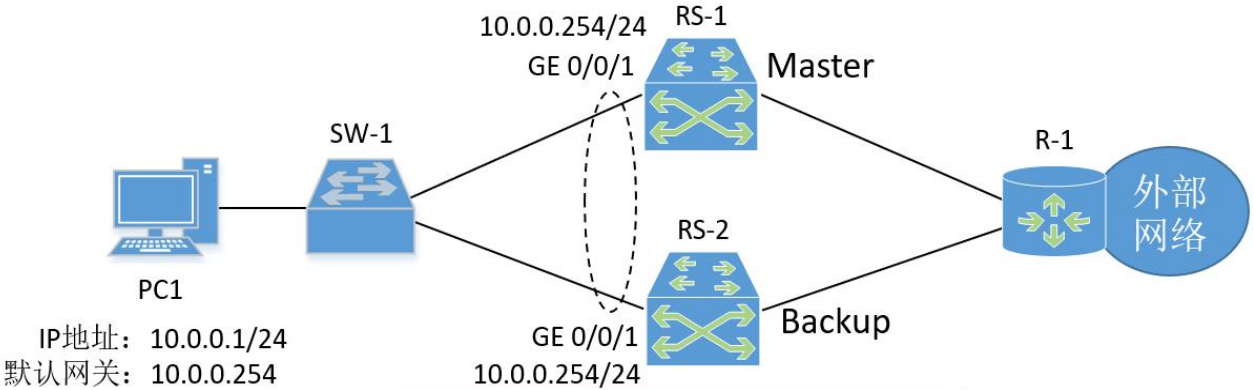


- RS-1和RS-2的VRRP配置：
  VRRP备份组：VRRP VRID 1
  虚拟网关的 IP：10.0.0.254/24
  虚拟MAC地址：0000-5e00-0101

防火墙部署 —— 双机热备

分析2：下一跳（网关）的自动切换问题（5）—— 几个概念

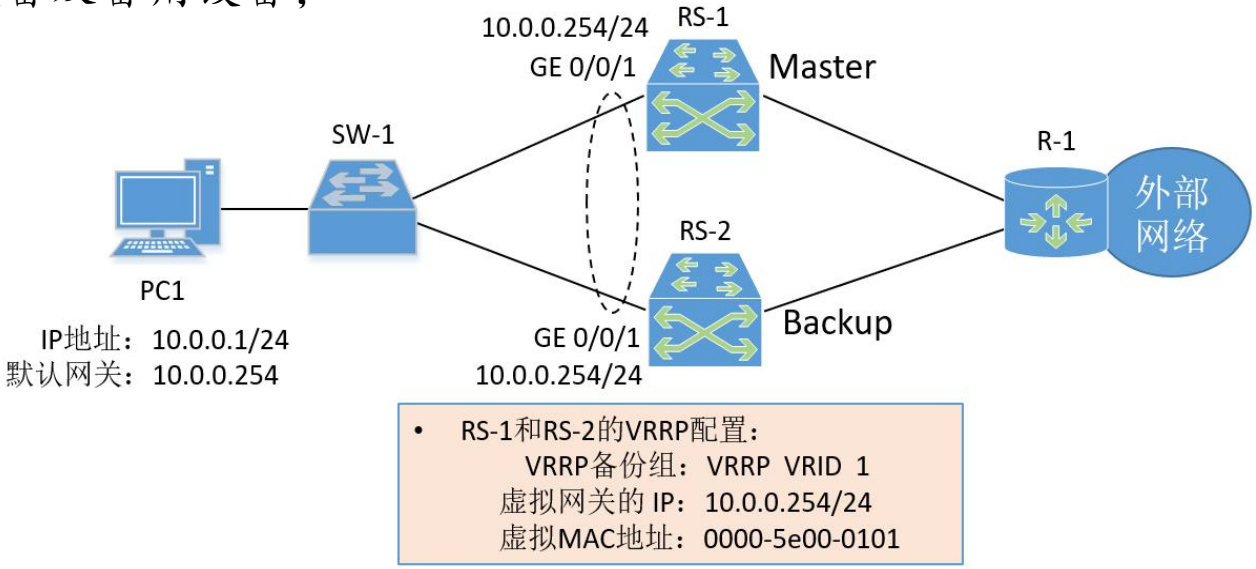
- VRID：Virtual Router ID，虚拟路由器标识，用来唯一的标识一个备份组；
- 虚拟IP地址：提供给客户端的网关IP地址，也是分配给虚拟路由器的IP地址，在所有的VRRP中配置，只有主用设备提供该IP地址的ARP响应；



防火墙部署 —— 双机热备

分析2：下一跳（网关）的自动切换问题（6）—— 几个概念

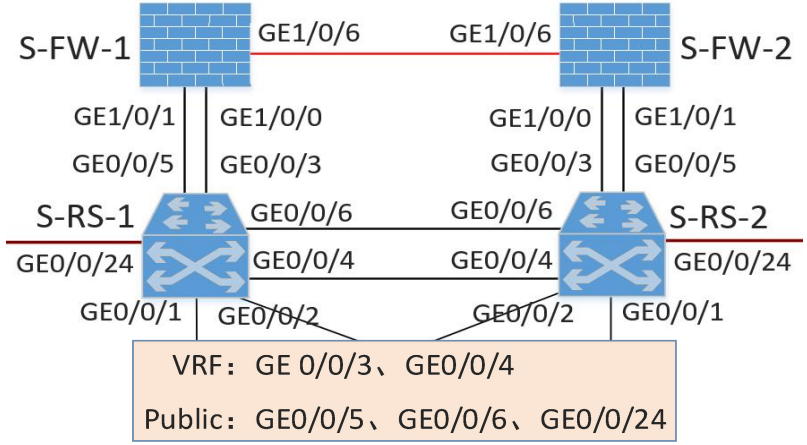
- 虚拟MAC地址：基于VRID生成的用于VRRP的MAC地址，在客户端通过ARP协议解析网关的MAC地址时，主用路由器提供该MAC地址；
- 优先级：用于表示VRRP路由器的优先级，并通过每个VRRP路由器的优先级选举主用设备及备用设备；



防火墙部署 —— 双机热备

分析3：本任务中，VRRP的配置（1）

- 本任务中，数据中心区域的核心交换机（S-RS-1和S-RS-2）配置了VRF（即分隔为VRF和Public虚拟交换机），并且与旁挂防火墙（S-FW-1和S-FW-2）之间通过静态路由实现防火墙旁挂引流。
- 为了实现双机热备，并且解决默认网关自动切换的问题，需要在防火墙（S-FW-1和S-FW-2）和路由交换机（S-RS-1和S-RS-2）上分别配置VRRP备份组，而静态路由中的下一跳地址就是对端设备中相应的VRRP备份组的虚拟IP地址。

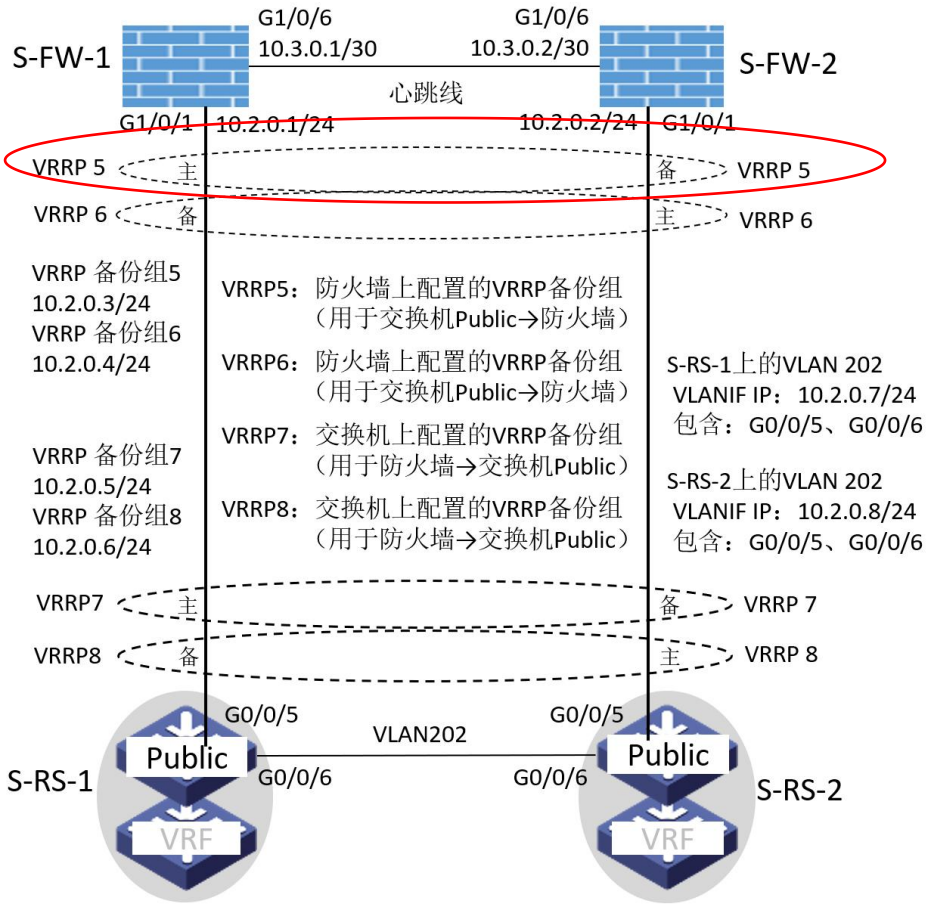


防火墙部署 —— 双机热备

- 分析3：本任务中，VRRP的配置（2

  - 将S-FW-1的GE1/0/1和S-FW-2的GE1/0/1接口都配置成VRRP备份组5。其中S-FW-1的GE1/0/1设置成“主状态”，S-FW-2的GE1/0/1同样设置VRRP备份组5，但设置成“备状态”。

  - 把备份组5理解为一个虚拟网关，当从外部网络发往服务器网段的报文到达S-RS-1或S-RS-2的Public时，根据相应的静态路由，下一跳要先转发至旁挂防火墙，此处的下一跳地址就是该虚拟网关地址

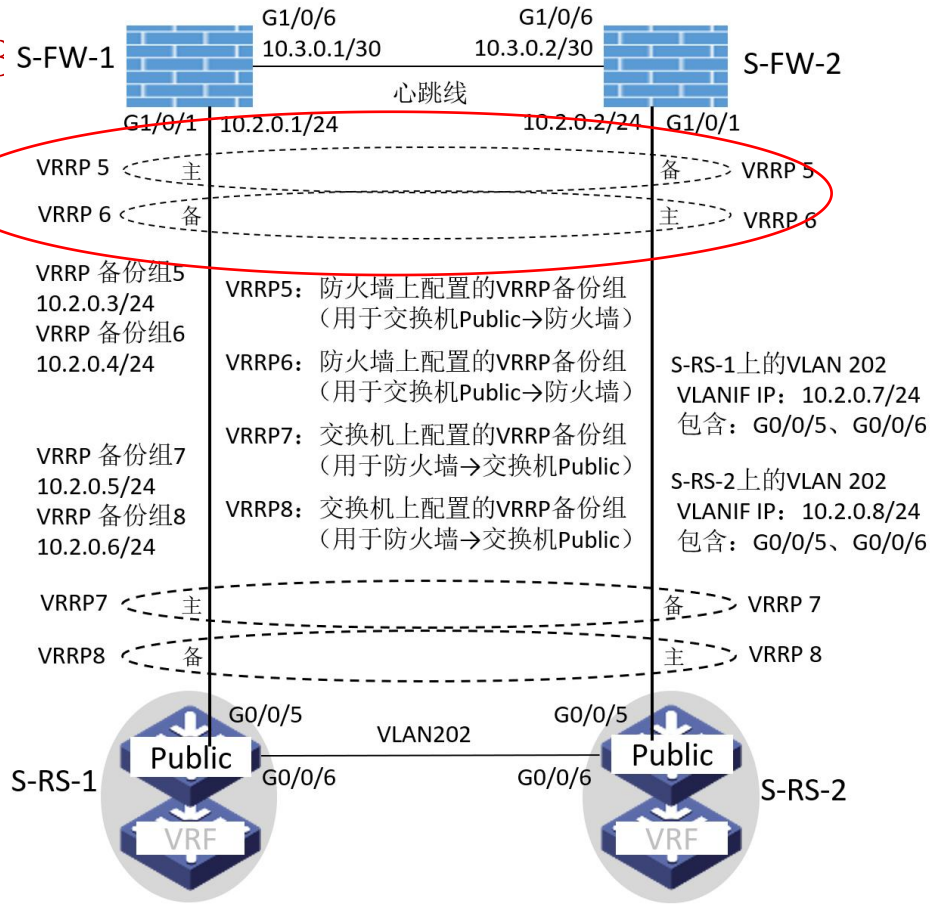


防火墙部署 —— 双机热备

- 分析3：本任务中，VRRP的配置（3

  - 同时，由于两台旁挂防火墙以负载分担方式工作，所以基于同一组接口配置VRRP备份组时，要在实现双机热备的两台设备上（例如S-FW-1和S-FW-2或者S-RS-1和S-RS-2），分别配置两个相同的VRRP备份组，并且主、备状态要交叉设置。

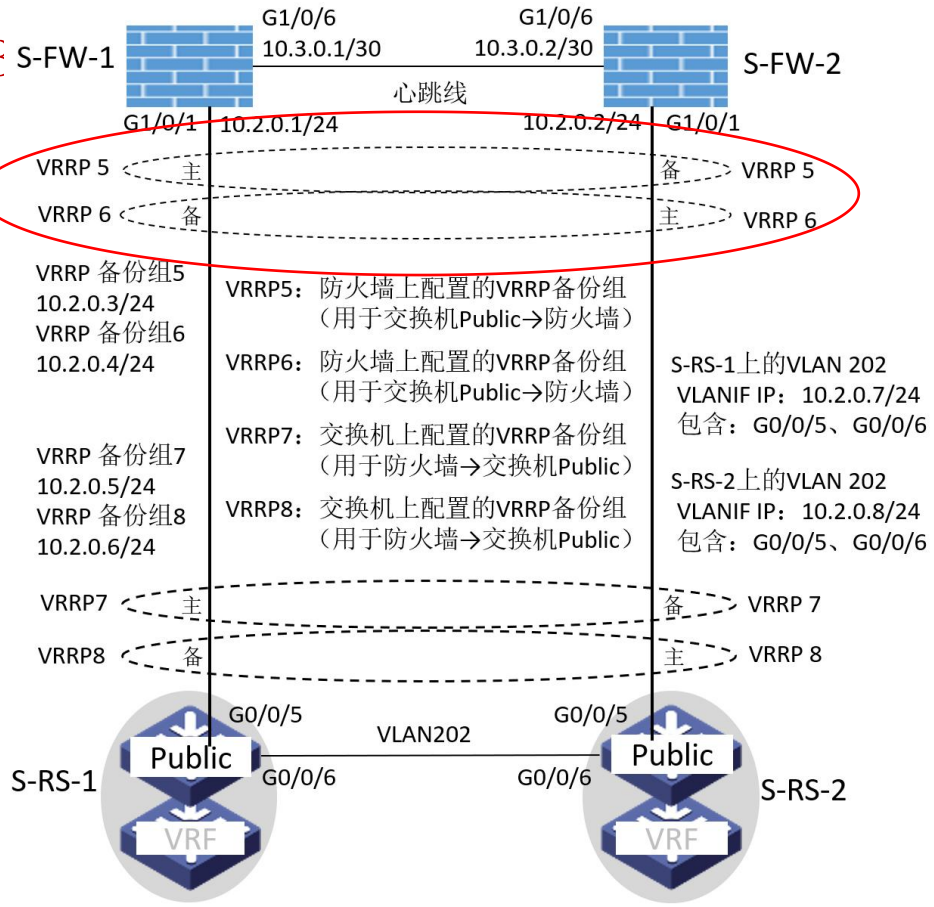
  - 例如,将S-FW-1的GE1/0/1和S-FW-2的GE1/0/1接口都配置成VRRP备份组6。其中S-FW-1的GE1/0/1设置成“备状态”,S-FW-2的GE1/0/1同样设置VRRP备份组6，但设置成“主状态”



防火墙部署 —— 双机热备

- 分析3：本任务中，VRRP的配置（3

  - 在防火墙对端交换机（S-RS-1或S-RS-2）的Public上，针对同一个目的网络（例如172.16.64.0/23）需要配置两条等价的静态路由，下一跳分别为旁挂防火墙上的VRRP备份组5和备份组6。



防火墙应用

完