# 异步路由相关的防火墙处理机制

## 功能介绍

⽹络上的主机在访问其他⽹络的主机或者服务器时，因为其请求和响应数据包遵循不同的路径并且没有穿过同⼀防⽕墙。这种⾏为称为⾮对称路由（即异步路由）。如果防⽕墙接收到**响应数据包**，⽽不是**请求数据包**，默认情况下它会将这些数据包视为⽆效。

所以，如果由于某些特定的原因，要求防⽕墙允许⾮对称路由，可以使⽤以下命令开启异步路由功能:

define system settings

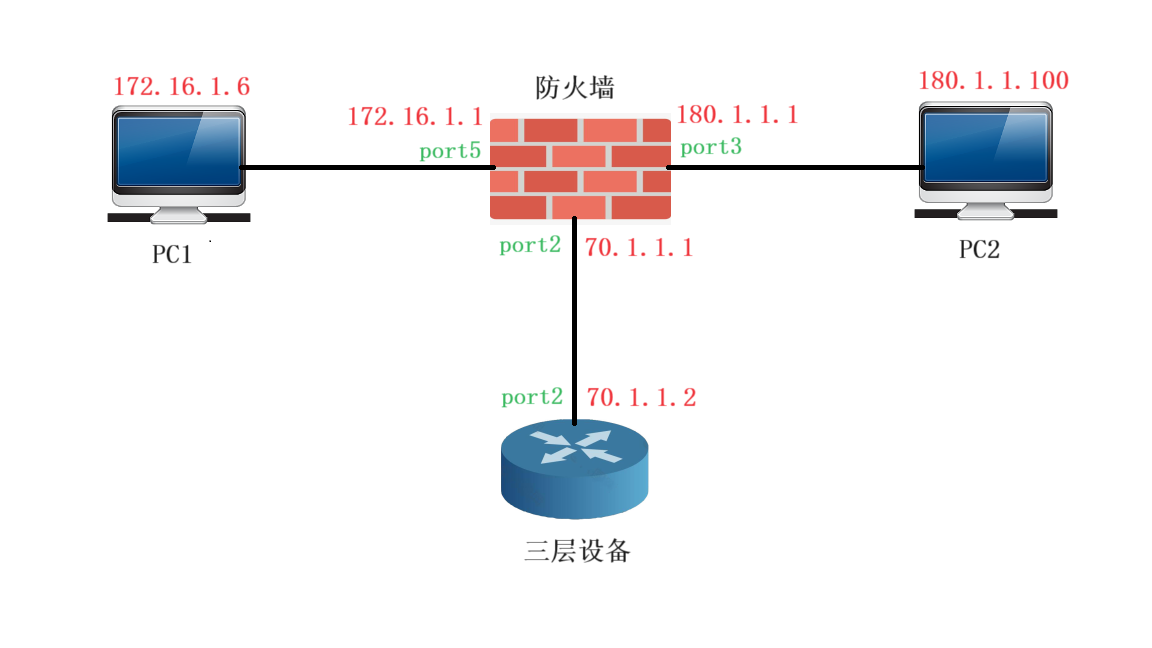
**set asymroute enable**

end

本文档的主要目的是，通过实验的方式，研究开启或关闭异步路由时，防火墙处理数据的机制，特别是处理**响应数据包**的机制。主要分四种情况进行探讨：

1. 响应数据包到达防火墙时，防火墙上**有对应的会话**，并且**关闭了异步路由**功能。
2. 响应数据包到达防火墙时，防火墙上**有对应的会话**，并且**开启了异步路由**功能。
3. 响应数据包到达防火墙时，防火墙上**没有对应的会话**，并且**关闭了异步路由**功能。
4. 响应数据包到达防火墙时，防火墙上**没有对应的会话**，并且**开启了异步路由**功能。

## 二、响应数据包到达防火墙时，防火墙上有对应的会话，并且关闭了异步路由功能



首先，实验一下**响应数据包**到达防火墙时，防火墙上**有对应的会话**，并且**关闭了异步路由**功能，看看防火墙会如何处理。测试拓扑图如上。

防火墙默认就是关闭异步路由的，这里保持默认配置，也就是关闭了异步路由功能。

对照拓扑图，这里计划验证从PC2访问PC1（**从右到左**）。

**第1步：**防火墙上配置策略，允许PC2到PC1的流量：



**第2步：**配置一条策略路由，这个路由是针对从PC1回复的响应报文的，引导它走到下面那个三层设备。

这里之所以配置策略路由，是因为**策略路由**比**直连路由**180.1.0.0/16更优先，目的是为了做个对比，看看响应报文从**port5**进来之后，它是使用策略路由转发，还是使用直连路由转发。策略路由的出口指向**port2**，直连路由的出口指向**port3**。



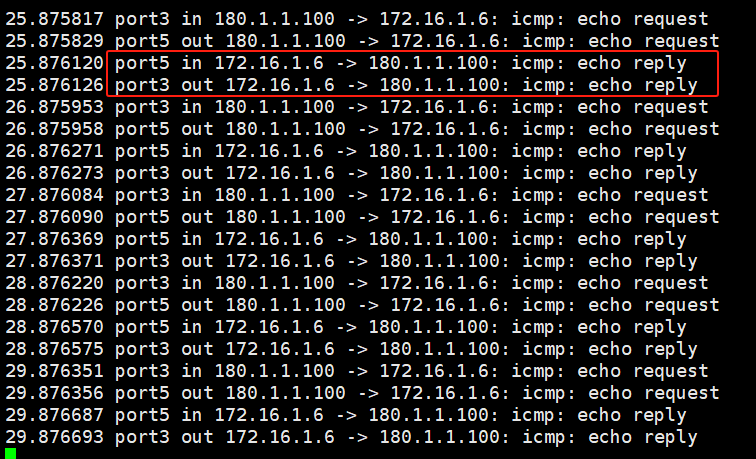
**第3步：**从PC2上ping机器PC1，**能ping通**。

**第4步：**可以看到防火墙上是产生了会话的，这应该是请求报文产生的会话。

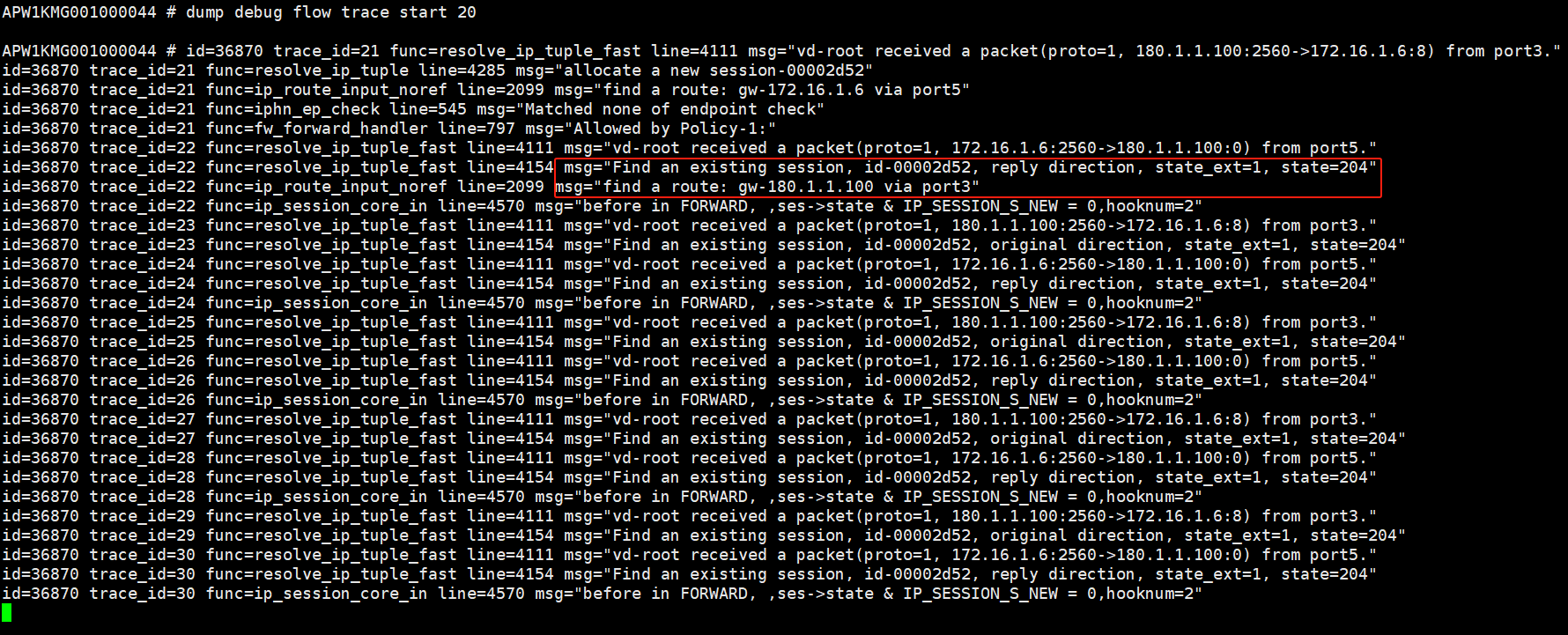


**第5步：**用抓包命令在防火墙上抓包，可以看到响应报文从**port5**进来，然后从**port3**转发了出去。

这说明，防火墙转发响应报文时，使用的是**直连路由**，而不是第2步配置的**策略路由，**即使策略路由的优先级更高。因为策略路由的出口指向**port2**，直连路由的出口指向**port3。**



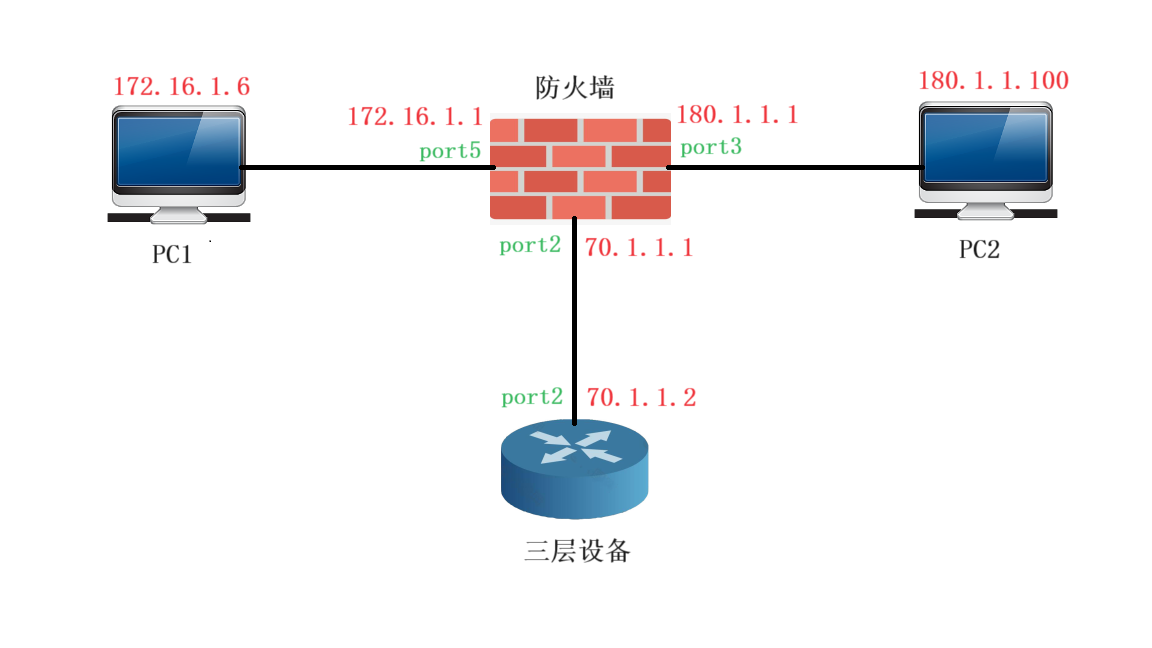
**第6步：**用dump debug flow继续进行分析，可以看到，响应报文从**port5**进来后，匹配了已有的会话，并且是从port3转发出去的。



**总结：**

**响应数据包**到达防火墙时，防火墙上**有对应的会话**，并且**关闭了异步路由**功能，那么防火墙转发**响应数据包**时，会先去匹配会话表，然后根据会话的入接口（port3），看看和入接口有关的路由有哪个，然后依据此路由转发出去。这样的话，“响应报文”回去的路径和“请求报文”来时的路径一样。

## 三、响应数据包到达防火墙时，防火墙上有对应的会话，并且开启了异步路由功能



接下来，测试一下**响应数据包**到达防火墙时，防火墙上**有对应的会话**，并且**开启了异步路由**功能，看看防火墙会如何处理。测试拓扑图如上。

首先，使用如下命令，开启防火墙的异步路由功能：

define system settings

**set asymroute enable**

End

然后对照拓扑图，这里计划验证从PC2访问PC1（**从右到左**）。

**第1步：**防火墙上配置策略，允许PC2到PC1的流量：



**第2步：**配置一条策略路由，这个路由是针对从PC1回复的响应报文的，引导它走到下面那个三层设备。

这里之所以配置策略路由，是因为**策略路由**比**直连路由**180.1.0.0/16更优先，目的是为了做个对比，看看响应报文从**port5**进来之后，它是使用策略路由转发，还是使用直连路由转发。策略路由的出口指向**port2**，直连路由的出口指向**port3**。

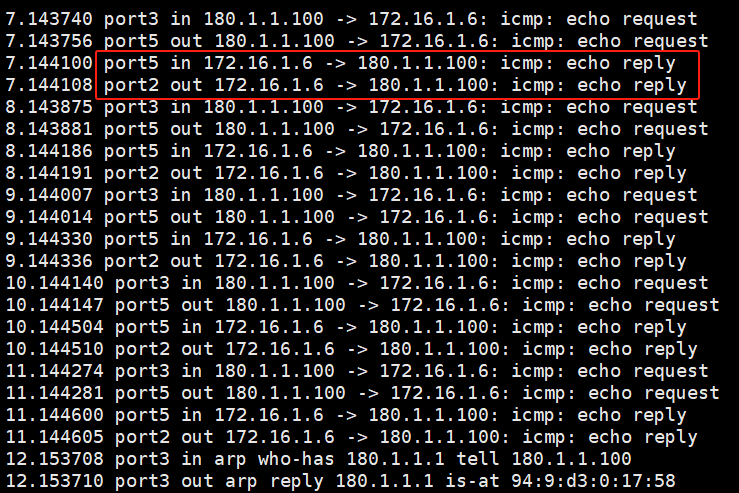


**第3步：**从PC2上ping机器PC1，**ping不通**。

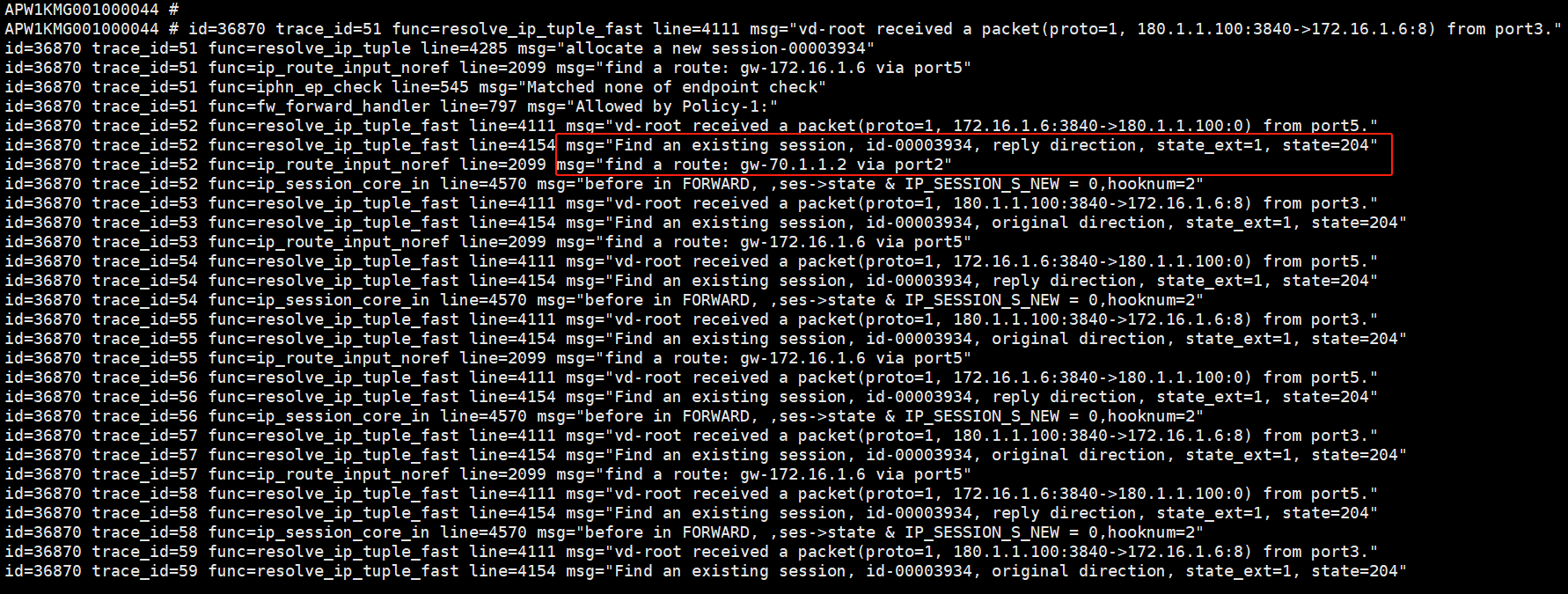
**第4步：**可以看到防火墙上是产生了会话的，这应该是请求报文产生的会话



**第5步：**用抓包命令在防火墙上抓包，可以看到，响应报文从**port5**进来，然后从**port2**转发了出去。这说明，防火墙转发响应报文时，使用的是第2步配置的**策略路由**，而不是**直连路由**。因为策略路由的出口指向**port2**，直连路由的出口指向**port3。**



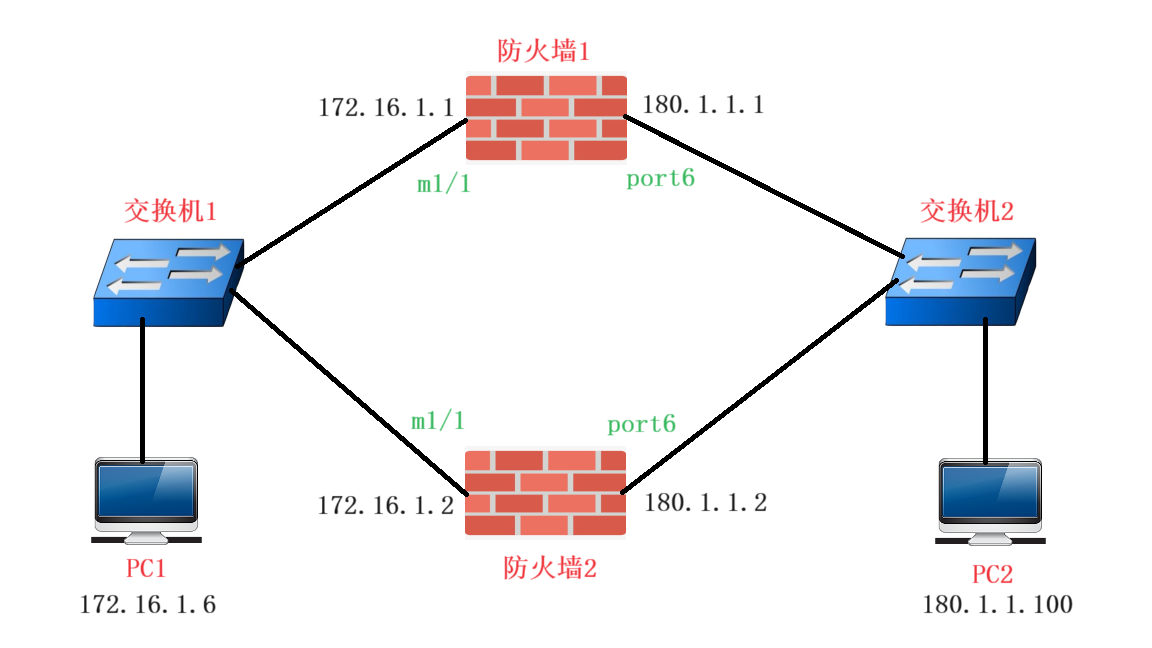
**第6步：**用dump debug flow继续进行分析，可以看到，响应报文从**port5**进来后，虽然匹配了已有的会话，但是，它没有从会话的入接口**port3**转发出去，而是查找策略路由转发了出去，出口是**port2**。



**总结：**

响应数据包到达防火墙时，防火墙上**有对应的会话**，并且**开启了异步路由**功能。那么防火墙转发响应数据包时，会匹配会话表，但是，系统不会根据会话的入接口(port3)进行转发，而是单纯的只查找路由表，根据目的地址找一条优先级最高的路由进行转发，注意，这个时候路由表中找到的路由的出接口(port2)，有可能和会话的入接口(port3)不同。所以，这可能导致一个现象，那就是，“响应报文”回去的路径和“请求报文”来时的路径不一样。

## 四、响应数据包到达防火墙时，防火墙上没有对应的会话，并且关闭了异步路由功能



这一节，测试一下响应数据包到达防火墙时，防火墙上**没有对应的会话**，并且**关闭了异步路由**功能，看看防火墙会如何处理。测试拓扑图如上。

防火墙默认就是关闭异步路由的，这里保持默认配置，也就是关闭了异步路由功能。

对照拓扑图，计划让PC1访问PC2，数据流的具体走向是：

a、PC1发送请求报文，目的地址是PC2。由于PC1上配置的默认网关是172.16.1.2，所以，请求报文离开PC1后，会到达**防火墙2**上。

b、**防火墙2**会把请求报文转发给PC2（依据的是直连路由）

c、PC2收到PC1的请求报文后，会给出响应，响应报文会转发到**防火墙1**上（因为PC2上配置的默认网关是180.1.1.1）。

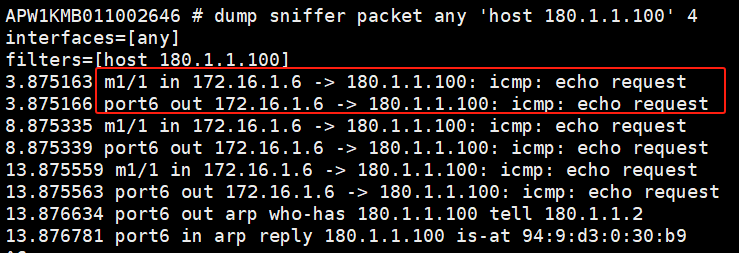
总之，**请求报文**走的是下面的路径（经过**防火墙2**），**响应报文**走的是上面的路径（经过**防火墙1**），而且当响应报文到达**防火墙1**时，**防火墙1**上还没有建立会话。

**第1步：**给防火墙1和防火墙2都配置一条全通策略。



**第2步：**在PC1上ping机器PC2，**结果ping不通**。

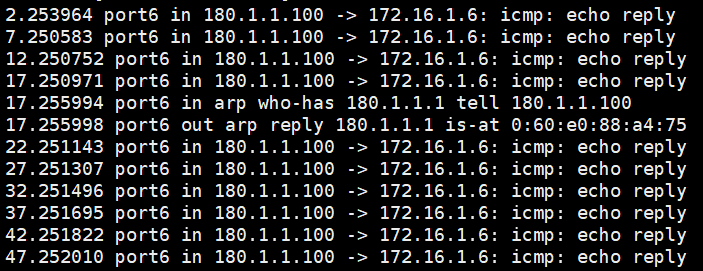
**第3步：**在**防火墙2**上抓包，可以看到，**防火墙2**的m1/1网口收到了**请求报文**，而且**防火墙2**把请求报文从port6转发了出去。



**第4步：**查看**防火墙2**上有会话，这是请求报文产生的会话。



**第5步：**在**防火墙1**上抓包进行查看，**防火墙1**的port6网口收到了响应报文，但是**防火墙1**没有转发响应报文。



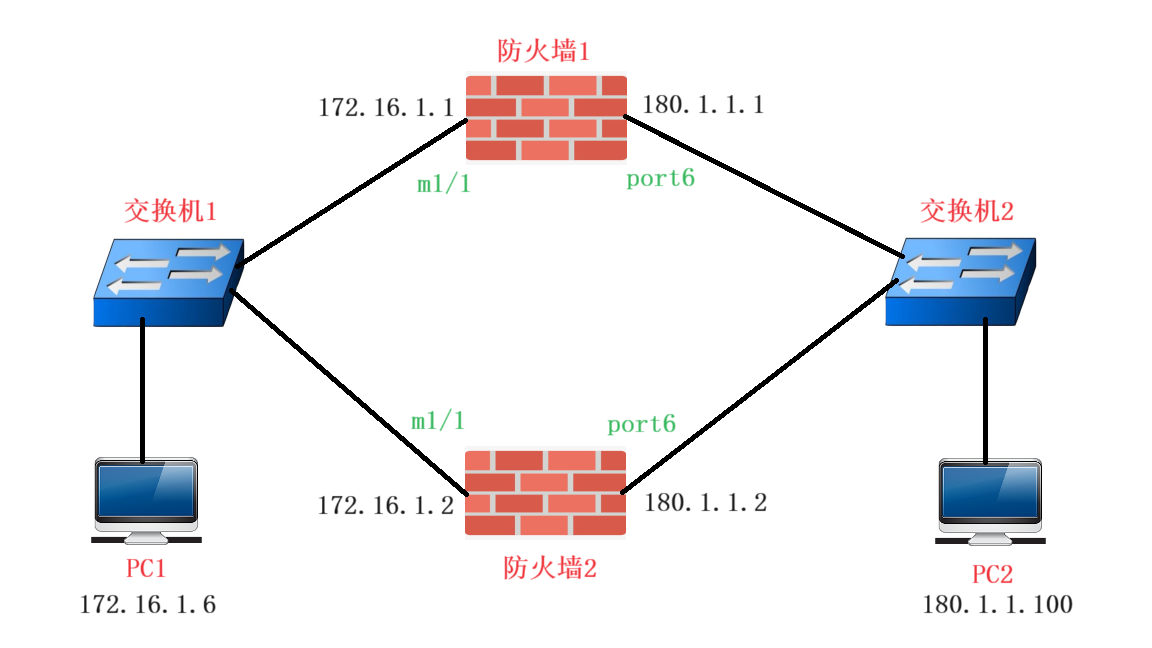
**第6步：**在防火墙1上查看会话，没有ICMP会话



**总结：**

响应数据包到达防火墙时，防火墙上**没有对应的会话**，并且**关闭了异步路由**功能，那么防火墙会把收到的响应数据包丢弃掉。

## 五、响应数据包到达防火墙时，防火墙上没有对应的会话，并且开启了异步路由功能



这一节，测试一下响应数据包到达防火墙时，防火墙上**没有对应的会话**，并且**开启了异步路由**功能，看看防火墙会如何处理。测试拓扑图如上。

首先，使用如下命令，开启防火墙的异步路由功能：

define system settings

**set asymroute enable**

end

对照拓扑图，计划让PC1访问PC2，数据流的具体走向是：

a、PC1发送请求报文，目的地址是PC2。由于PC1上配置的默认网关是172.16.1.2，所以，请求报文离开PC1后，会到达**防火墙2**上。

b、**防火墙2**会把请求报文转发给PC2（依据的是直连路由）

c、PC2收到PC1的请求报文后，会给出响应，响应报文会转发到**防火墙1**上（因为PC2上配置的默认网关是180.1.1.1）。

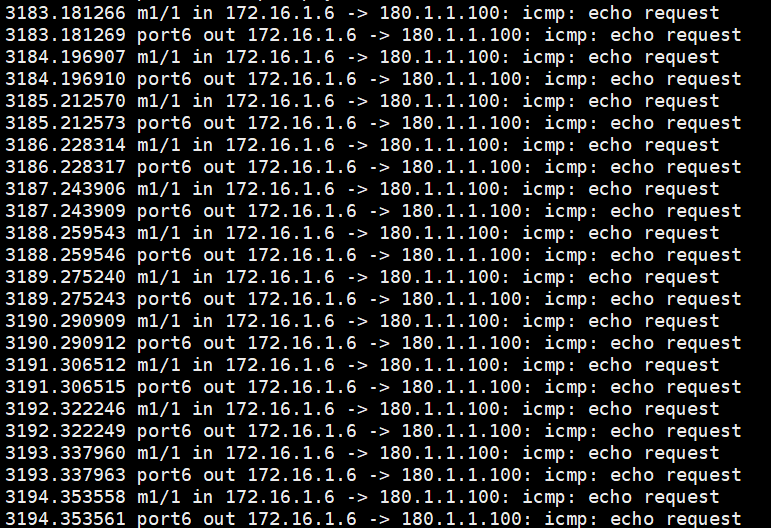
总之，**请求报文**走的是下面的路径（经过**防火墙2**），**响应报文**走的是上面的路径（经过**防火墙1**），而且当响应报文到达**防火墙1**时，**防火墙1**上还没有建立会话。

**第1步：**给防火墙1和防火墙2都配置一条全通策略。



**第2步：**在PC1上ping机器PC2，**能ping通**。

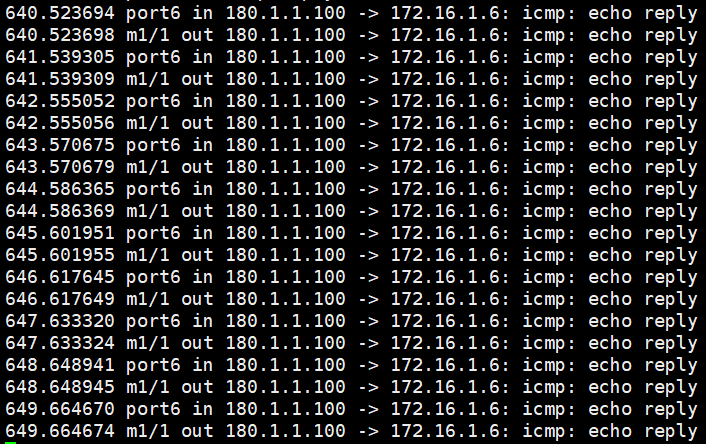
**第3步：**在**防火墙2**上抓包，可以看到，**防火墙2**的m1/1网口收到了**请求报文**，而且**防火墙2**把请求报文从port6转发了出去。



**第4步：**查看**防火墙2**上有会话，这是请求报文产生的会话。



**第5步：**在**防火墙1**上抓包进行查看，**防火墙1**的port6网口收到了响应报文，然后**防火墙1**把响应报文从m1/1网口转发了出去。



**第6步：**在防火墙1上查看会话，没有ICMP会话



**总结：**

响应数据包到达防火墙时，防火墙上**没有对应的会话**，并且**开启了异步路由**功能，那么响应数据包会被传递到CPU，防火墙不会查找匹配的防火墙策略。由于不需要匹配任何策略，所以报文只根据路由表进行转发，防火墙作为路由器只做路由决策，不进行安全检查。