## 不同转发域端口加入同一zone功能测试

1，拓扑图如下

* port1物理口下配置vlan100-out，vlan200-out；
* port2物理口下配置vlan100-in，vlan200-in；
* 不同vlan设置不同转发域；
* vlan100-out，vlan200-out加入outside区；vlan100-in，vlan200-in加入inside区；
* 针对区进行策略配置；



2，配置说明

1. 防火墙为透明模式，



1. 为不同的vlan端口设置不同的转发域



1. 命令行下确认如下命令

#define system setting

(setting)#set forward-domain-check disable

默认不进行转发域检查，设置成enable后，不同转发域将不能加入同一个zone。

1. 创建不同的zone，并将不同转发域端口加入同一zone



1. 配置放行策略，允许vlan通信



1. 测试结果，同一转发域vlan可以通过防火墙进行通信，PC1可以与PC3正常通信，同一zone内不同转发域的vlan不会接到对方信息。

## 基于策略的MTU配置



1. 如图所示，port2端口设置MTU值为1400
2. 配置Port2到Port1策略设置MTU值为1300

define firewall policy

edit 1

set pmtu-override

set pmtu 1300

end

1. 在PC2上使用1315的包ping192.168.200.5，抓包可发现ping包被分片。