# V7防火墙域间策略配置举例

关萌 2016-06-29 发表

**安全域简介**

**安全域（Security Zone），是一个逻辑概念，用于管理防火墙设备上安全需求相同的多个接口。管理员将安全需求相同的接口进行分类，并划分到不同的安全域，能够实现安全策略的统一管理。**

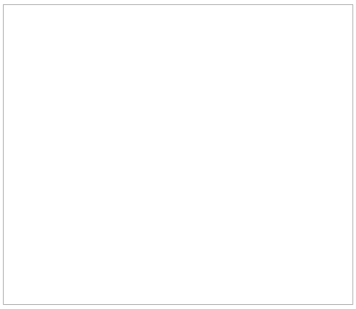
**传统防火墙的安全策略配置通常是基于报文入接口、出接口的，进入和离开接口的流量基于接口上指定方向的策略规则进行过滤。这种基于接口的策略配置方式需要为每一个接口配置安全策略，给网络管理员带来配置和维护上的负担。随着防火墙技术的发展，防火墙已经逐渐摆脱了只连接外网和内网的角色，出现了内网/外网/DMZ（Demilitarized Zone，非军事区）的模式，并且向着提供高端口密度服务的方向发展。基于安全域来配置安全策略的方式可以解决上述问题。**

**说明**

**DMZ这一术语起源于军方，指的是介于严格的军事管制区和松散的公共区域之间的一种有着部分管制的区域。安全域中引用这一术语，指代一个逻辑上和物理上都与内部网络和外部网络分离的区域。通常部署网络时，将那些需要被公共访问的设备（如Web server、FTP server等）放置于此。**

**一个安全域中，可以包含多个成员。例如，可以将公司防火墙设备上连接到研发部门不同网段的四个接口作为成员加入安全域Zone_RND，连接服务器区的两个接口作为成员加入安全域Zone_DMZ，这样管理员只需要部署这两个域之间的安全策略即可，此处的安全策略包括包过滤策略、ASPF策略、对象策略等。如果后续网络环境发生了变化，则只需要调整相关域内的接口，而域间安全策略不需要修改。包过滤策略的相关配置请参考“ACL和QoS配置指导”中的“ACL”。ASPF策略的相关配置请参考“安全配置指导”中的“ASPF”。对象策略的相关配置请参考“安全配置指导”中的“对象策略”。**

**图 安全域划分示意图**



创建安全域后，设备上各接口的报文转发遵循以下规则：

· 一个安全域中的接口与一个不属于任何安全域的接口之间的报文，会被丢弃。

· 属于同一个安全域的各接口之间的报文缺省会被丢弃。

· 安全域之间的报文由域间策略进行安全检查，并根据检查结果放行或丢弃。若域间策略不存在或不生效，则报文会被丢弃。

· 非安全域的接口之间的报文被丢弃。

· 目的地址或源地址为本机的报文，缺省会被丢弃，若该报文与域间策略匹配，则由域间策略进行安全检查，并根据检查结果放行或丢弃。

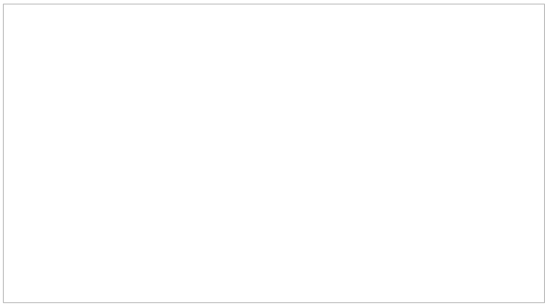
· 当存在Any到Any域间实例时，仅当报文未匹配对应域间实例时，才会匹配Any到Any域间实例。如未配置Any到Any域间实例且报文未匹配对应域间实例时，则直接丢弃报文。

某公司以Device作为网络边界防火墙，连接公司内部网络和Internet。公司需要对外提供Web服务和FTP服务。现需要在防火墙上部署安全域，并基于以下安全需求进行域间安全策略的配置。

· 与接口GigabitEthernet1/0/1相连的公司内部网络属于可信任网络，部署在Trust域，可以自由访问服务器和外部网络。

· 与接口GigabitEthernet1/0/3相连的外部网络属于不可信任网络，部署在Untrust域，访问公司内部网络和服务器时，需要受到严格的域间安全策略的限制。

· 与接口GigabitEthernet1/0/2相连的Web server、FTP server部署在DMZ域，可以自由访问处于Untrust域的外部网络，但在访问处于Trust域的公司内部网络时，需要受到严格的域间安全策略的限制。



# 向安全域Trust中添加接口GigabitEthernet1/0/1。
<Device> system-view
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
# 向安全域DMZ中添加接口GigabitEthernet1/0/2。
[Device] security-zone name dmz
[Device-security-zone-DMZ] import interface gigabitethernet 1/0/2
[Device-security-zone-DMZ] quit
# 向安全域Untrust中添加接口GigabitEthernet1/0/3。
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/3
[Device-security-zone-Untrust] quit
# 配置ACL 3500，定义规则：允许IP流量。
[Device] acl advanced 3500
[Device-acl-ipv4-adv-3500] rule permit ip
[Device-acl-ipv4-adv-3500] quit
# 创建ASPF策略1，配置检测应用层协议FTP（FTP仅为示例，若要检测其它应用协议，可根据需要配置）。
[Device] aspf policy 1
[Device-aspf-policy-1] detect ftp
[Device-aspf-policy-1] quit
# 创建源安全域Trust到目的安全域Untrust的安全域间实例，并在该域间实例上应用ASPF策略和包过滤策略，可以拒绝Untrust域用户对Trust的访问，但Trust域用户访问Untrust域以及返回的报文可以通过。
[Device] zone-pair security source trust destination untrust
[Device-zone-pair-security-Trust-Untrust] aspf apply policy 1
[Device-zone-pair-security-Trust-Untrust] packet-filter 3500
[Device-zone-pair-security-Trust-Untrust] quit
# 创建源安全域Trust到目的安全域DMZ的安全域间实例，并在该域间实例上开启ASPF检测功能，可以拒绝DMZ域用户对Trust的访问，但Trust域用户访问DMZ域以及返回的报文可以通过。
[Device] zone-pair security source trust destination dmz
[Device-zone-pair-security-Trust-DMZ] aspf apply policy 1
[Device-zone-pair-security-Trust-DMZ] packet-filter 3500
[Device-zone-pair-security-Trust-DMZ] quit
未配置安全域或域间策略时所有网络都是不通的，接口想要互通必需加安全域，同时配置对应的域间策略，包括相同安全域之前的互通。
any到any域的域间策略不包括相同安全域之间的互访。