

Q: Comware V5平台防火墙不同虚拟防火墙之间的安全域如何通信?

A: 不同虚拟设备之间可以通过共享域进行通信。

假设有虚拟设备Vd1和Vd2, 虚拟设备Vd1中有安全域vd1-z1, Vd2中有安全域vd2-z1。为实现vd1-z1区域中的主机能够访问vd2-z1, 则可以将会话目的区域vd2-z1设置为共享域。这样, 从vd1-z1区域中的主机主动发起会话的报文, 可以向vd2-z1转发, 而从vd2-z1区域返回的匹配会话的报文, 也可以转发回vd1-z1。如果vd2-z1区域中的主机主动发起会话, 访问vd1-z1区域, 由于vd1-z1没有被设置为共享区域, 报文会被防火墙拒绝, 不能转发。

当某一虚拟设备安全区域被设备为共享域后, 其他虚拟设备安全区域至该共享域之间可以配置域间策略以实现网络策略控制。