ZStack 技术白皮书精选

安全组和云防火墙的区别

扫一扫二维码，获取更多技术干货吧

安全组和云防火墙的区别

前言

熟悉云平台的朋友可能都会注意到这样一个事情：无论公有云还是私有云，创建虚拟机的时候都需要选择安全组，来对虚拟机进行安全防护；有的云平台在 VPC 里，还能选择防火墙，ZStack 在 3.6 版本也发布了 VPC 防火墙功能。可能有的朋友会有疑惑，防火墙和安全组到底有什么区别？有了安全组，是否可以不需要防火墙了？他们是相互替代关系吗？本文将会给大家做一个详细介绍，剖析防火墙和安全组的异同以及各自的应用场景。

1．安全组

安全组在网络服务中，在管理界面上选择网络服务->安全组，到安全组的配置界面进行安全组配置。

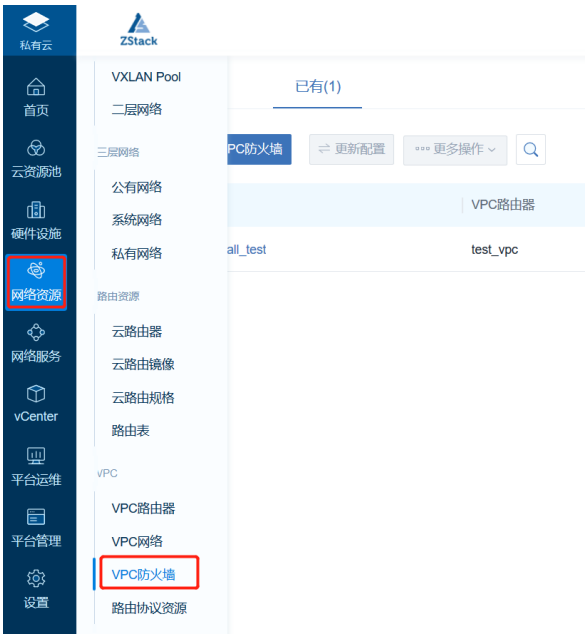
输入安全组名称，然后选择网络、配置规则、加载虚拟机网卡。

安全组作用于虚拟机的虚拟网卡上，给虚拟机提供三层网络的访问控制，支持入方向、出方向的过滤；控制 TCP/UDP/ICMP 等协议进行有效过滤；也可以直接匹配所有协议；可以根据数据包的源 IP 进行过滤。安全组实际上可以看成是一个分布式的访问控制，扁平网络和 VPC 网络均支持安全组。如果需要将更多的虚拟机加入安全组，则可以动态在安全组中添加虚拟机网卡，每次规则的更新，也会动态的添加/删除安全组规则，安全组中的所有虚拟机同步更新规则。

安全组中包含了一系列的访问控制规则，属于白名单机制，只有在白名单中的数据才允许通过。安全组可以加载一个或多个三层网络，虚拟机挂载到三层网络的网卡可以加入这些安全组。一个虚拟机的网卡可以加入多个安全组，安全组的规则会合并在一起并应用到该网卡上；也就是说，作用到虚拟机网卡上的规则是所有安全组的并集。

2 防火墙

防火墙在网络资源中，在管理界面上选择网络资源->VPC 防火墙，到防火墙的配置界面进行防火墙配置



输入防火墙名称，然后选择 VPC 路由器，这样就将 VPC 路由器变成了一台防火墙。

为 VPC 路由器配置防火墙以后，会自动创建入方向的规则集，规则允许 new、related、established 状态的报文以及 ICMP 报文通过，默认动作为拒绝。

防火墙中有如下几个概念：

规则集：是访问控制规则的集合，包含了一系列的规则，具体作用到 VPC 路由器的每个网卡的出入方向，包含对数据包处理的默认行为接受、拒绝或者丢弃。

规则：访问控制策略，支持 3-4 层的过滤；支持配置优先级，优先级越大，生效越早。

防火墙作用在 VPC 路由器上，属于集中式的 VPC 边缘设备，为整个 VPC 提供访问控制。防火墙的配置也是动态生效的，即时的配置会马上作用到 VPC 路由器接口；接口每个方向只能应用一个规则集。因此，接口每个方向上的策略是规则集中的所有规则，每个规则可以自定义行为，设置接受、拒绝或者丢弃。数据包进入防火墙时，根据规则集的规则优先级进行逐条匹配，如果匹配上了，则执行规则的行为；如果没有匹配上，则执行规则集的默认行为。

防火墙可以针对不同报文状态来进行过滤，如 new、established、invalid、related；也可以针对常见的协议，如 TCP、UDP、VRRP、ICMP 等。同时，如果协议是 TCP 或者 ICMP，防火墙提供了更加细粒度的过滤规则，能够针对 ICMP 的类型、TCP 的 flag 进行匹配，进一步细化策略，满足更多的使用场景。

3 安全组和防火墙对比

从前面的介绍，咱们来对安全组和防火墙做一个对比小结，如下图

对比项	安全组	防火墙
作用范围	虚拟机网卡	VPC网络或者整个VPC
部署方式	分布式	集中式
部署位置	虚拟机所在宿主机	VPC路由器
配置策略	仅支持允许	自定义允许、拒绝或丢弃
优先级	按照配置顺序	自定义规则优先级
规则匹配	源IP，源端口，协议	源IP，源端口，目的IP，目的端口，协议，TCP flag，ICMP Type，报文状态

从作用范围来看，安全组作用于虚拟机网卡，而防火墙则是在 VPC 路由器上，保护整个 VPC；

安全组是分布式部署的，在每个计算节点上都会存在，而防火墙是集中式，把 VPC 路由器变成了防火墙；

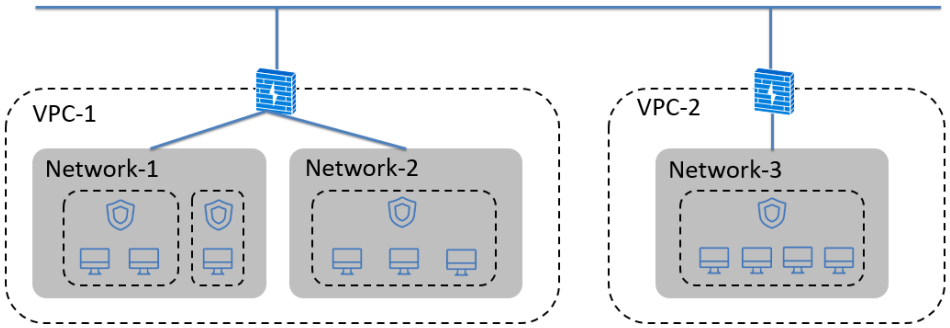
安全组是白名单机制，仅支持允许策略，防火墙可以自定义规则行为是允许还是拒绝；

安全组规则根据配置顺序来定优先级，防火墙则可以自定义优先级；

安全组规则的匹配内容包括源 IP、源端口、协议，防火墙则包括五元组以及 TCP flag、ICMP Type、报文状态。

从上面的分析可以看到，防火墙的功能是更为强大的，但可能有朋友要问了，这些都是属于包过滤的功能，安全组同样可以做，这和防火墙是否有功能上的重复？诚然，防火墙的功能主要是包过滤，但后续可以加入更多的功能。

从流量的角度再来看下，访问 VPC 内部虚拟机的流量到公有网络后，先经过 VPC 路由器，也就是防火墙，然后是 VPC 网络，再到虚拟机端口上，经过安全组过滤最后发给虚拟机。可以看到，防火墙是在安全组之前生效的。



打一个比方，把 VPC 看做是企业 IT 环境，虚拟机就是 PC 机或者服务器，安全组就好比 PC 机的软件防火墙，VPC 路由器就是企业出口设备。对于企业来说，出口肯定是需要硬件防火墙设备来做防护的，保证内部环境的安全，不可能只靠 PC 机的软件防火墙；对于 VPC 来说也是同样的道理，VPC 使用防火墙，在更靠近威胁源的地方，将流量阻断，保证了 VPC 内部通信的安全，同时也保证了 VPC 路由器的安全。如果 VPC 路由器没有防火墙功能，那危险流量过来后，VPC 路由器就直接被攻破，后端连接的所有 VPC 网络全部通信中断，安全组其实根本没能发挥出应有的作用。由此可以看到，VPC 路由器是 VPC 的入口，在入口部署防火墙进行统一的策略防护，是最好的安全手段。

从配置的角度来看，安全组是作用于虚拟机网卡的，如果虚拟机数量非常多，那么就需要再一个个将虚拟机选择出来加入安全组，过程复杂且繁琐；而用防火墙就方便的多，直接几条策略即可，防护整个网段。

当然，防火墙也有无法触及之处，防火墙作为 VPC 网络的网关，主要对南北向流量进行过滤，同一个 VPC 网络中的虚拟机通信没有办法做控制，这个时候就需要依靠安全组了。

4 总结

从上面的分析咱们可以看到，防火墙主要是做南北向的访问控制，作用范围是整个 VPC，安全组主要是做东西向的访问控制，作用范围是虚拟机网卡，和防火墙形成互补的关系。当然，安全组也是可以做南北向的访问控制的，从安全的角度来看，在离威胁源更近的地方进行防护是更好的方式，所以南北向交给防火墙来做，安全组作为防火墙的补充，是云主机安全的最后防线。

安全组和防火墙不是两者只取其一的关系，他们是相辅相成的，两者有机结合，才能够更好的做云主机的安全防护。