云防火墙

快速入门

快速入门

智能分组

目标：根据智能分组的结果，逐步优化

开通云防火墙产品后，云防火墙的智能分组将自动帮助您将业务进行分区分组。

智能分组功能基于阿里云大数据平台的机器学习算法，首创性地采用属性的传播聚类算法和加权分割算法，将您所登录账号中的ECS自动进行分区分组。通过机器学习，根据ECS实例访问关系的聚类生成业务区，根据进程的相似度生成角色组。

说明：智能分组功能仅支持对单个网络中拥有30台以上ECS实例的情况进行自动分区分组。如果该网络中的ECS实例小于30台，请根据您的实际业务情况手动完成分区分组。

操作步骤

登录云盾云防火墙管理控制台。

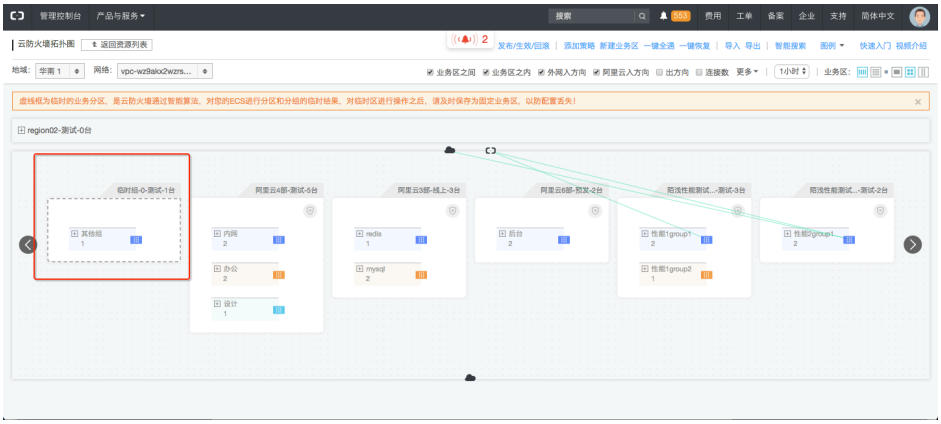
选择**地域**，选择**网络**。

说明：如果所选择的网络中的ECS实例数量小于30台，云防火墙无法为您进行自动分区分组。您需要单击**新建业务区**手动创建业务区，并将ECS实例添加至相应业务区中，完成分区分组。关于如何添加ECS实例，请查看添加或导入资产。

在云防火墙拓扑图中，查看智能分组结果。

智能分组自动对所有地域中各个专有网络 / 经典网络的所有ECS实例进行基于属性的自动学习，生成临时业务区和临时的角色组。

说明： 临时业务区是智能分组功能根据相关属性自主机器学习的结果，无法手动创建。在云防火墙拓扑图中，临时业务区将以“临时组”命名，并以虚线框表示。



同时，智能分组功能也会将您在配置云防火墙业务区后新创建的ECS实例自动进行分区分组，并以临时业务区的形式在云防火墙拓扑图中展示。关于云防火墙拓扑图的详细说明，参考**云防火墙拓扑图**。

根据实际业务情况对临时业务分区分组进行调整。

说明：对临时业务区所执行的所有操作不会被保存，也无法为相关的流量线进行策略配置。

单击临时业务区左上角的角色管理按钮，在**角色管理**页面，勾选ECS服务器，单击**更换角色组**或**转移服务器**，将临时角色组中的服务器转移至其他角色组或其他业务区的角色组中。关于角色分组详情，参考**角色分组**。

单击临时业务区右上角的名称，在**业务区信息**页面，将鼠标移至名称与环境信息处单击**编辑**，将临时业务区根据业务需要重新命名。

单击临时业务区左上角的保存为固定业务区按钮，将临时业务区保存为固定业务区。

说明：保存为固定业务区后，该临时业务区内的ECS服务器将不再参与智能分组的机器学习计算。同时，对该业务区所执行的操作将会被保存下来。

被保存的固定业务区将会与临时业务区共存。但是，在您完成所有分区分组的调整工作后，理应不再存在临时业务区。

简化拓扑

目标：去掉无关的流量线，找到感兴趣的流量线

确定完业务分区分组后，需要在云防火墙拓扑图中找出您感兴趣的流量线，从而快速地进行服务器分区/分组的

调整，同时也能甄别出流量的合法性为后续的策略配置做准备。

操作步骤

登录云盾云防火墙管理控制台。

选择**地域**，选择**网络**。

在云防火墙拓扑图中，观察各业务分区中的流量线，去除无关的流量线。

说明：关于云防火墙拓扑图的详细说明，参考云防火墙拓扑图。

流量线范围筛选：根据实际业务情况在拓扑图上方仅勾选需要显示的流量线，从而简化拓扑图。例如，只显示业务区之间的流量、业务区之内的流量、外网入方向流量、阿里云入方向流量或出方向流量等。

您也可以单击**更多**，勾选是否显示特定类型的流量线，或者自定义不显示特定端口的流量线。

同时，您还可以单击时间维度选择所显示的流量线的时间范围。

智能搜索：单击拓扑图右上方的**智能搜索**，通过设定搜索规则显示或不显示某个业务区或某个角色组的特定流量线。关于智能搜索的详细说明，参考智能搜索。

说明： 为了让智能搜索结果更加准确，建议完整填写规则条件。其中，关键字字段可用于搜索服务器备注名、进程名称、操作系统类型等，但IP地址和端口需通过相应条件字段设置。

单服务器查看：在拓扑图中，单击某台服务器，可以查看该服务器的相关信息及与该服务器相关的流量线，其它的流量线信息将不显示。

通过上述方法，定位到您需要查看的关键流量线信息，帮助您对服务器的分区/分组进行相应调整，同时帮助您甄别流量的合法性。

策略模拟

目标：逐一将流量或角色进行策略部署

定位到关键流量信息后，您就可以基于流量线、服务器或角色组配置访问控制策略。

注意： 只要业务区发布，您在该业务区上配置的所有策略并不会真实下发，更不会影响您的业务。

操作步骤

登录云盾云防火墙管理控制台。

选择**地域**，选择**网络**。

在云防火墙拓扑图中，对流量线、服务器或角色组配置访问控制策略。

说明： 基于流量线的配置方法最为直观，建议您尽可能通过操作具体流量线的方式定义访问控制策略。

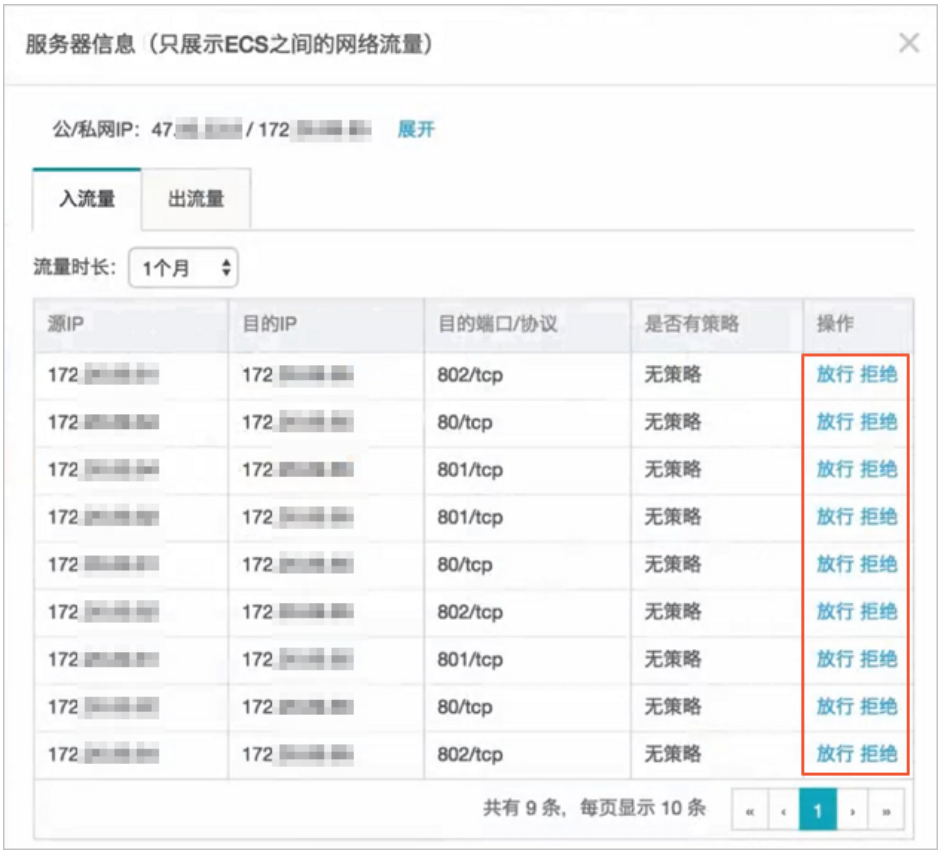
基于流量线配置策略

拓扑图中的红色流量线为待定义流量线，您需要逐条确认流量的合法性，而审核的过程就是定义相应的访问控制策略。

在拓扑图中，单击红色流量线，在**流量线**对话框中查看详细的访问记录，单击**放行**或**拒绝**即可为该类型的访问设置放行或拒绝的策略。已配置放行策略的流量线将显示为绿色。

基于服务器配置策略

在拓扑图中，单击服务器，在**服务器信息**对话框中选择**入流量**或**出流量**页签，查看与该服务器相关的出/入方向的访问流量记录，单击**放行**或**拒绝**即可为该类型的访问设置放行或拒绝的策略。



基于角色组配置策略

在拓扑图中，单击角色组，在**角色组信息**对话框中选择**入流量**或**出流量**页签，查看与该角色组相关的出/入方向的访问流量记录，单击**放行**或**拒绝**即可为该类型的访问设置放行或拒

绝的策略。

对于暂时还没有访问流量的情况，您可以通过单击业务区左上角的角色管理按钮，在**角色管理**页面直接添加访问控制策略。

说明：您也可以在拓扑图上方单击**添加策略**，手动添加访问控制策略。

策略下发

目标：发布业务区，下发真实的访问控制策略

在访问控制策略配置完成后，这些策略仍没有真实下发，您需要发布业务区将所配置的访问控制策略真实下发。

操作步骤

登录云盾云防火墙管理控制台。

选择**地域**，选择**网络**。

单击云防火墙拓扑图上方的**发布/生效/回滚**。

选择业务区发布模式，选择业务区，单击**发布**。

说明： 存在流量线关联的业务区必须一起发布，无法单独发布。

观察模式

如果您还不确定策略配置是否合理时，建议选择**发布观察模式**。在观察模式下，云防火墙不会对流量进行真实阻断。

业务区发布为观察模式后，您可以在一段时间后继续观察拓扑图中是否出现其它未被放行的正常业务流量线，并配置相应的访问控制策略。

拦截模式

选择**发布拦截模式**，云防火墙将根据业务区中所有基于流量线、服务器或角色组配置的访问控制策略自动生成安全组规则。拦截模式发布成功后，所有不在白名单策略定义的流量都会被拦截。

说明：为了避免ECS实例原先所属的安全组的规则影响云防火墙的访问控制规则的效果，在将所有业务区以拦截模式发布后，您需要将所有ECS实例从的原先的安全组中移出，在云防火墙中配置访问规则才能真正生效。您可以在**发布/生效/回滚**页面中选择**生效/回滚**页签，选择安全组单击**脱离**，即可将ECS实例从安全组中移出。

在业务区以拦截模式发布后，如果正常业务由于所配置的访问控制策略导致中断，您可以使用一键全通功能实现在特殊情况下为某个业务区提供临时性放行策略，从而为您争取更多的排查时间。关于一键全通功能的详细说明，参考**一键全通**。