云防火墙

用户指南

用户指南

添加或导入资产

云防火墙的智能分组功能将自动将您所登录账号中的ECS资产根据业务进行分区分组。关于智能分组的详细说明，参考**智能分组**。

您也可以通过手动添加或导入的方式，将智能分组未分配的ECS资产添加至云防火墙拓补图中进行管理。

操作步骤

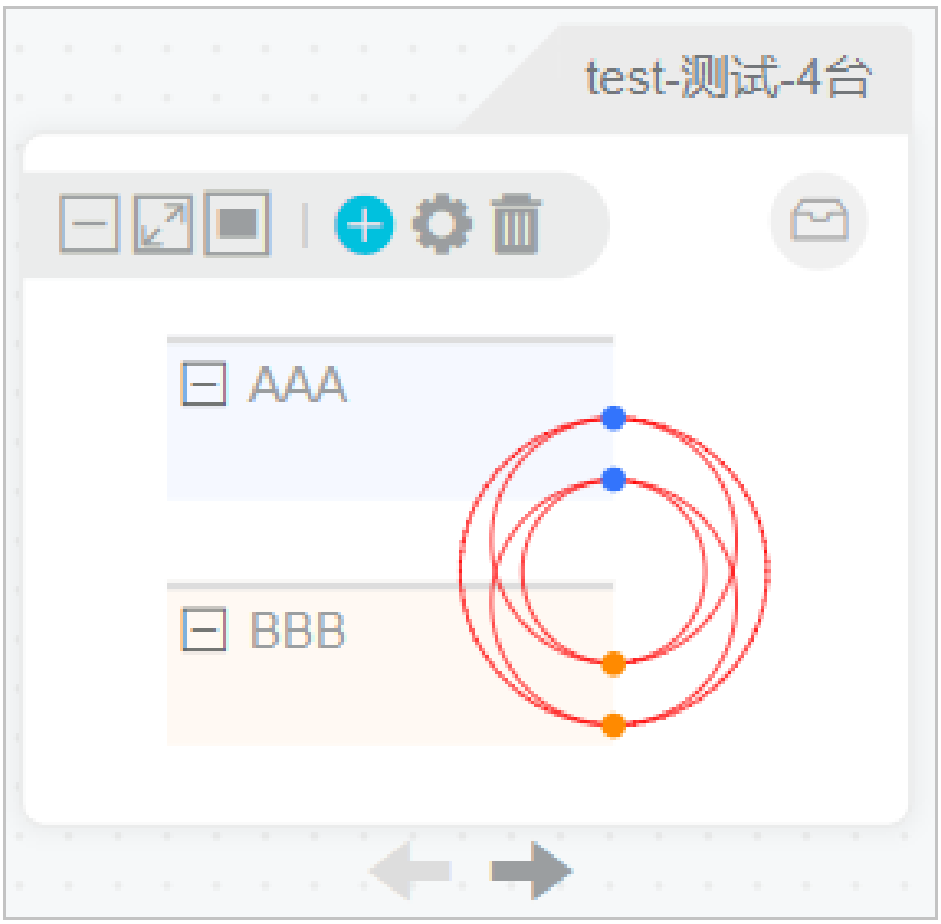
登录**云盾云防火墙管理控制台**。

选择**地域**，选择**网络**。

添加ECS资产。

手动添加

将鼠标移至需要添加资产的业务区，单击左上角的添加资产按钮。



在**添加资产**页面中，勾选尚未被分配的ECS资产，单击**立即添加**。

所选择的ECS资产即被添加至该业务的默认角色组中，需要变更角色组或转移服务器请参考**角色分组**。

导入资产

单击云防火墙拓扑图上方的**导入**。

在**导入**对话框中，单击**下载模板**将ECS资产导入模板下载至本地。在模板中填写导入到的业务区、角色组名称、被导入的ECS实例ID等信息，并保存。

说明： 在资产导入模板的**action**栏中，填写**add**。

	A	B	C	D	E
1	bizName(业务区名称)(必需参数)	roleName(角色组名称)(必需参数)	instanceId(Ecs实例id)(必需参数)	action(add新增/move移动)(必需参数)	tag(当有重名业务区，用tag区分，tag分为测试(test),预发(pre)，线上(online))
2	test2	AAA	i-bp16dy0dvsdzy76m8ejv	add	

单击**上传文件**，选择已填写完成的ECS资产导入列表，单击**打开**。

导入成功后，刷新云防火墙拓扑图页面即可看到已导入的ECS资产及业务区。

说明： 您也可以通过导入资产功能实现ECS资产的批量转移服务器或变更角色组。只需在资产导入列表中，填写变更后的业务区、角色组名称、需要变更的ECS实例ID，并在**action**栏中填写**move**后完成导入即可。

智能搜索

智能搜索是帮助您简化云防火墙拓扑图中流量线信息的一种方法。通过智能搜索，您可以在拓扑图中快速找出您感兴趣的流量线。

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**智能搜索**。

单击**添加规则**，设置智能搜索规则。

说明： 智能搜索提供了强大的搜索规则功能，来实现过滤不相关流量信息的显示效果。智能搜索规则可以组合执行，采用自上而下的匹配顺序；每条规则都可单独设定是否显示符合规则条件的流量线。

最多可以定义10条搜索规则，并且系统默认有一条缺省规则。

搜索规则可以通过左侧的勾选框区决定是否生效（缺省规则是无法取消勾选）。

智能搜索的规则应用举例：

例如，通过设置以下智能搜索规则即可只显示特定业务区特定角色组中提供80端口的流量和服务器。

勾选需要使用的智能搜索规则，单击**保存并执行**。

云防火墙拓扑图将根据所设定的智能搜索规则显示流量线和服务器信息。

角色分组

根据实际业务需要，您可以将云防火墙所管理的ECS资产进行分组，帮助您更好地甄别各服务器之间流量的合法性。

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**。

将鼠标移至业务区，单击业务区左上方的角色管理按钮，打开**角色管理**页面。

说明： 单击源角色组旁的加号可添加角色组。

根据访问源的信息，为ECS资产选择相应的角色组。

对于尚未明确角色组的ECS资产，您可以通过以下功能进一步查看服务器的信息。

说明： 您也可以参考**简化拓扑**中的方法，在云防火墙拓扑图中隐藏部分无关的流量线，帮助明确ECS资产的角色。

在云防火墙拓扑图中，将鼠标悬停在服务器上，查看该ECS资产的服务器信息。

在云防火墙拓扑图中，单击服务器，打开**服务器信息**页面，查看该ECS资产与其他服务器的访问关联信息。

您也可以在**角色管理**页面中，通过查看本业务区所有ECS资产的服务器信息、及ECS资产与其他服务器的访问关系，判断该ECS资产的应属角色组。

一键全通

业务的中断，往往是因为存在错误的防火墙策略配置导致的。然而，传统的人肉排查过程通常无效、冗长。

云防火墙提供一键全通功能，帮助您在特殊情况下为当前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。

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**一键全通**。

在**一键全通**对话框中，勾选需要被临时放行的业务区，单击**确定**。

说明： 单击勾选所有业务区可以对选中所有业务区。

一键全通生效后，在该业务区上所配置的访问控制策略将暂时失效。出入该业务区的全部流量都将被临时放行，可恢复您被中断的业务，您应在此期间尽快完成排查工作。

修正错误的访问控制策略配置后，单击云防火墙拓扑图上方的**一键恢复**，勾选需要恢复的业务区，单击**确定**即可自动删除由一键全通功能所增加的临时放行策略，恢复到业务区原有的访问策略配置。

外部流量管理

在云防火墙拓扑图中，将来自公网（互联网）、阿里云内部产品、阿里云其他账户下的资源、其他地域和网络的流量统称为外部流量。

在云防火墙拓扑图的顶部和底部，使用以下图标对外部流量进行区分：

外网流量

外部流量即为公网流量，分为外部入流量与外部出流量。

说明： 对于外部入流量，您可以通过单击流量线条直接进行策略定义。但是，对于外部出流量无法通过流量线定义配置策略。如果您需要对外部出方向流量进行策略管控，您可以在云防火墙的**策略管理**页面手工定义策略。

阿里云流量

阿里云流量包含阿里云内部产品的管理流量、来自其他阿里云账户的流量、以及其他地域和网络的流量。

说明：对于阿里云流量，您可以通过单击流量线条直接进行策略定义，也可以通过云防火墙的**策略管理**页面手工定义策略。

导出流量信息

在**云防火墙拓扑图**页面，您可以将某个业务区中的某个角色组的流量信息导出，便于您在本地对该角色组的流量进行进一步的分析和处理。

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**导出**。

在**导出**对话框中，选择业务区、角色组，选择流量时长范围，选择流量方向，单击**确定**。

导出到本地的文件中包含所选择业务区、角色组在指定时间范围内的出方向流量或入方向流量的详细信息。

资源列表

您也可以在云防火墙控制台的**资源列表**页面，对业务区、角色组及ECS资产等进行管理。

说明： 云防火墙拓扑图是云防火墙业务可视化的核心所在，建议您在云防火墙拓扑图中对业务区、角色组及ECS资产等直观地进行管理。

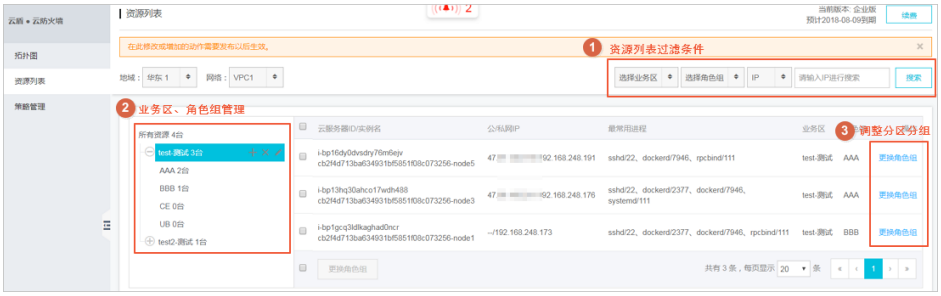
操作步骤

登录云盾云防火墙管理控制台。

在**云防火墙拓扑图**页面，单击左上角的**返回资源列表**。

在**资源列表**页面，选择**地域**，选择**网络**。

管理业务区、角色组及ECS资产。



您可以通过选择业务区、角色组，设定IP或端口号关键字，单击**搜索**，筛选资源列表中所显示的ECS资产。

您可以将鼠标移至业务区、角色组，单击添加、删除、修改按钮设置业务区和角色组。

说明： 将鼠标移至**所有资源**处，单击添加按钮可新建业务区。

选择ECS资产，单击**更换角色组**，在对话框中选择业务区、角色组，单击**确定**可变更该ECS资产的分区分组。

说明： 您也可以勾选多个ECS资产，单击列表下方的更换角色组进行批量变更。

策略管理

业务区发布后，您可以在云防火墙控制台中的**策略管理**页面，查看并管理已创建的访问控制策略。

说明： 云防火墙拓扑图是云防火墙业务可视化的核心所在，建议您在云防火墙拓扑图中对访问控制策略直观地进行管理。

操作步骤

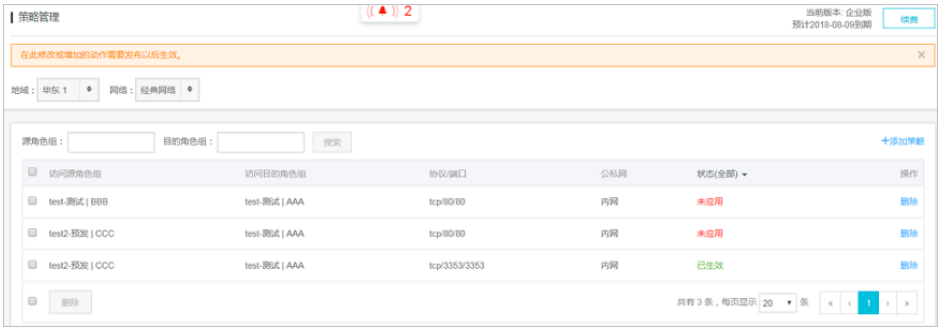
登录云盾云防火墙管理控制台。

在**云防火墙拓扑图**页面，单击左上角的**返回资源列表**。

在**策略管理**页面，选择**地域**，选择**网络**。

管理访问控制策略。

说明： 在**源角色组**或**目的角色组**中输入关键字，单击**搜索**，可查看包含该关键字的角色组的相关访问控制策略。



选择访问控制策略，单击**删除**，可删除该访问策略。

单击**添加策略**，可手动配置访问控制策略。

在**策略管理**页面所执行的增加、修改的操作，都需要在相关业务区被发布后才可生效。关于发布业务区的详细说明，请参考策略下发。