comwareV7防火墙1 安全策略基于应用/应用组的白名单典型配置

域间策略/安全域　孔德飞　2021-12-23 发表

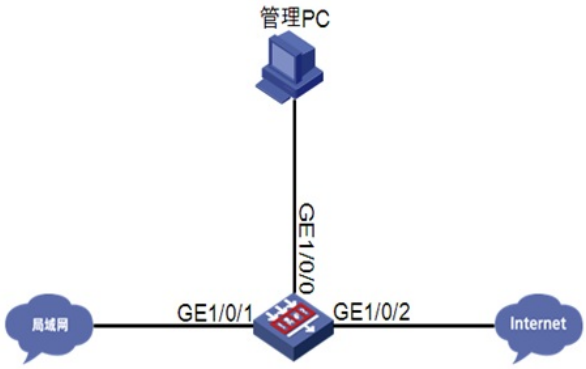
组网及说明

1　安全策略基于应用/应用组的白名单典型配置

1.1　组网需求

如下图所示，园区通过局域网连接到防火墙访问internet，要求能通过设备能访问web

图20 典型组网



配置步骤

1.1 配置思路

· 使管理PC能够通过Web登录设备进行管理

· 配置内外网接口地址并加入安全域，添加路由保证网络可达

· 安全策略下放行应用或应用组（本次放行淘宝以及它的基础协议，本次以安全策略下引用应用组为例）

1.2 使用版本

本举例是在最新软件版本上进行配置和验证的。

1.3 配置注意事项

在配置之前确保内外网路由可达

（注意：该典型配置只能保证访问淘宝，淘宝进行淘宝支付时可能涉及其他应用如支付宝等，如果需要进行淘宝支付可以根据需求再应用组里面加入相关应用即可）

1.4 配置步骤

说明
配置该功能前请确保内网主机与外网已路由可达。 配置思路中使PC能登陆Web以及配置内外网接口操作

1.4.1 配置放行应用组

Web页面配置：

点击Web上方标识和面板区的“对象”按钮，然后点击导航栏“应用安全”-“应用识别”-“应用组”页面

点击新建按钮，新建应用组，名称为permti，里面添加淘宝，http,https,dns，general-tcp,阿里云

（说明：http,https,dns，general-tcp为淘宝的基础协议；淘宝访问需要阿里云里面包含的阿里系应用的公共资源特征，所以也放行阿里云）

1.1.1 配置放行应用组的安全策略

点击Web上方标识和面板区的“策略”按钮，然后点击导航栏“安全策略”-“安全策略”页面

安全策略页面如下：

再点击“新建”按钮，进入 新建安全策略：

配置一条安全策略：动作为允许的安全策略

这一条安全策略：选好源安全域和目的安全域，动作选为“允许”，应用/应用组选择要放行的应用/应用组，点击“确定”按钮即可

页面如下：

原因是，报文先必须经过三次握手之后才能被识别为具体的应用

创建三条安全策略：

第一条放通基础协议

第二条放通淘宝

第三条全拒绝