防火墙通过安全策略实现过滤HTTPS网站配置方法(WEB界面)

目录

1 配置需求或说明

1.1 适用的产品系列

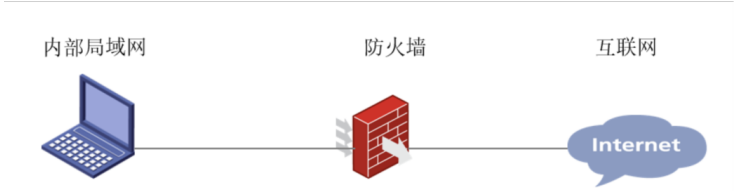
本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-WiNet、F1000-AK、F10X0等

注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

1.2 配置需求及实现的效果

防火墙部署在互联网出口，需要实现通过安全策略限制访问www.baidu.com的目的。

2 组网图



3 配置步骤

3.1 防火墙连接互联网配置

上网配置略，请参考《轻轻松松配安全》2.1章节防火墙连接互联网上网配置方法案例。

3.2 开启本地DNS代理

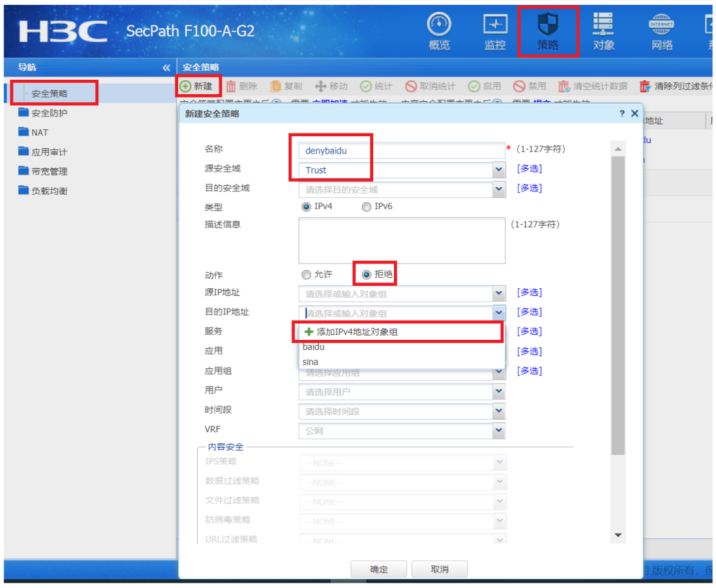
#开启设备本地DNS代理功能，用于解析域名。【注意：终端的DNS要设置为防火墙的IP，不能再是运营商的DNS或者114，不然不生效】

#在DNS-高级设置中，勾选开启dns代理

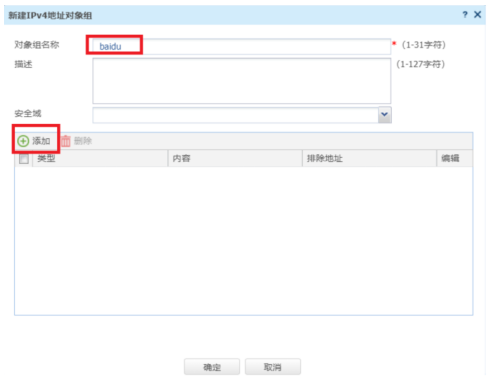
3.3 配置安全策略

#在“策略”>“安全策略”中点击新建，创建名称为“denybaidu”

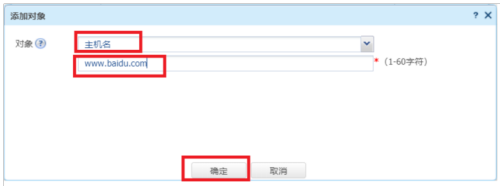
的安全策略，源安全域为“trust”，动作选择拒绝，目的地址位置点击下拉菜单后点击“添加IPV4地址对象组”。



#新建对象组名为“baidu”的对象组，点击添加按钮。



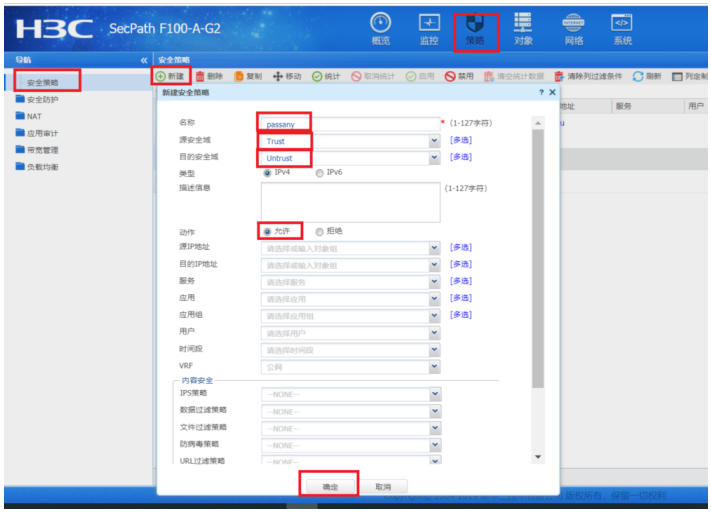
#对象选择主机名，输入www.baidu.com点击确定完成配置。



1111111 注

#检查配置无误后点击确认按钮完成配置；

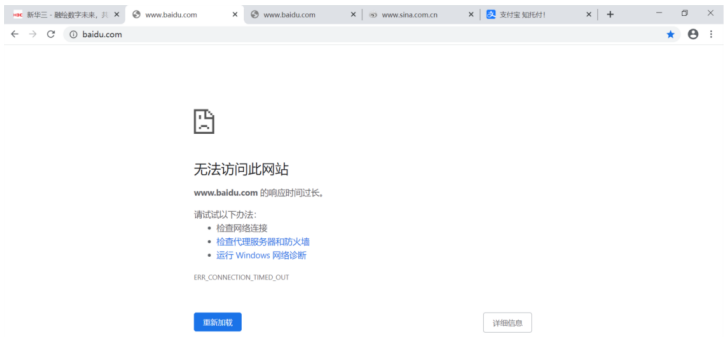
#在“策略”>“安全策略”中继续新建名称为“passany”的安全策略，源安全域为“trust”、目的安全域为“untrust”、动作选择允许。



3.4 保存配置

3.5 测试结果

使用浏览器打开www.baidu.com,不能正常访问：



使用浏览器打开www.alipay.com,可以正常访问：

查看pc针对百度解析的地址为39.156.66.18：

查看设备的安全策略日志，可以看到针对改目的ip已成功拒绝（第三条）：