防火墙通过安全策略实现过滤HTTPS网站配置方法（命令行）

URL过滤 **张新姿** 2020-11-08 发表

组网及说明

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：如F1080、F1070、F5040、F5020等F10X0、F50X0系列的防火墙。

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

配置步骤

1 配置步骤

1.1 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。

1.2 开启本地DNS代理

#开启设备本地DNS代理功能，用于解析域名。

system-view

System View: return to User View with Ctrl+Z.

[H3C]dns proxy enable

[H3C]dns server 114.114.114.114

1.3 修改DHCP服务器DNS为设备接口地址

#如果防火墙作为DNS服务器则需要保证下发给终端地址时，客户端DNS为防火墙接口地址；

[H3C]dhcp server ip-pool 2

[H3C-dhcp-pool-2]gateway-list 192.168.2.1

[H3C-dhcp-pool-2]network 192.168.2.0 mask 255.255.255.0

[H3C-dhcp-pool-2]dns-list 192.168.2.1

[H3C-dhcp-pool-2]quit

防火墙开启DNS代理后，如果终端将DNS请求发向防火墙则防火墙会替代向外网发起DNS解析请求，DNS回应报文返回防火墙后再由防火墙转发至终端，这样做的目的是保证终端和防火墙解析的地址相同。

1.4 配置安全策略

#创建地址对象组，地址对象组名称为baidu.使用基于主机的形式关联域名：www.baidu.com.

[H3C]object-group ip address baidu

[H3C-obj-grp-ip-baidu]0 network host name www.baidu.com

[H3C-obj-grp-ip-baidu]quit

#创建安全策略规则1名称为“baidu-deny”源安全域为“trust”、目的IP为名称为“baidu”的地址对象，安全策略默认策略为拒绝；创建安全策略规则2名称为“passany”源安全域为“trust”、目的安全域为“untrust”，动作配置为“pass”放通所有数据。

[H3C]security-policy ip

[H3C-security-policy-ip]rule 1 name baidu-deny

[H3C-security-policy-ip-1-denybaidu]source-zone trust

[H3C-security-policy-ip-1-denybaidu]destination-ip baidu

[H3C-security-policy-ip-1-denybaidu]quit

[H3C-security-policy-ip]rule 2 name passany

[H3C-security-policy-ip-2-passany]action pass

[H3C-security-policy-ip-2-passany]source-zone trust

[H3C-security-policy-ip-2-passany]destination-zone untrust

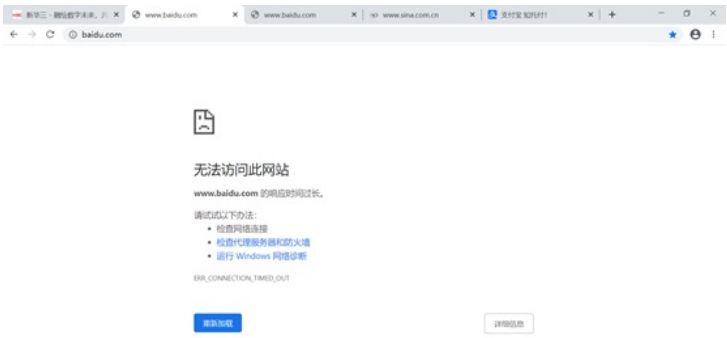
[H3C-security-policy-ip-2-passany]quit

1.5 保存配置

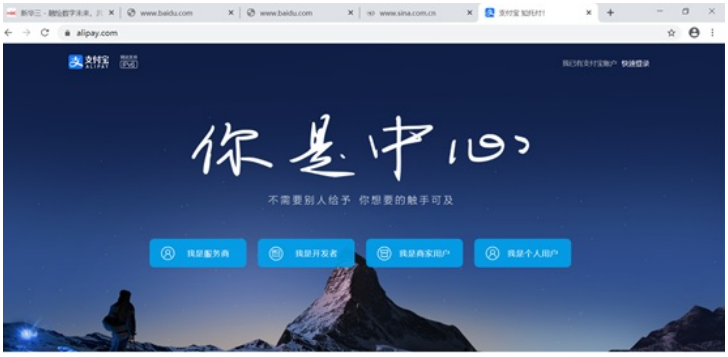
[H3C]save force

1.6 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）：

```
[H3C]*Aug 29 11:24:33:591 2020 H3C ASPF/7/PACKET: -Context=1; The first packet was dropped by packet filter or object-policy. Src-Zone=Trust, Dst-Zone=Untrust;If-In=GigabitEthernet2/0/6(71), If-Out=GigabitEthernet2/0/5(70); Packet Info:Src-IP=192.168.2.2, Dst-IP=39.156.66.14, VPN-Instance=none,Src-Port=53187, Dst-Port=443. Protocol=TCP(6). Flag=SYN. Seq=663489238.

*Aug 29 11:24:33:812 2020 H3C ASPF/7/PACKET: -Context=1; The first packet was dropped by packet filter or object-policy. Src-Zone=Trust, Dst-Zone=Untrust;If-In=GigabitEthernet2/0/6(71), If-Out=GigabitEthernet2/0/5(70); Packet Info:Src-IP=192.168.2.2, Dst-IP=39.156.66.14, VPN-Instance=none,Src-Port=53188, Dst-Port=443. Protocol=TCP(6). Flag=SYN. Seq=2319944221.

*Aug 29 11:24:34:043 2020 H3C ASPF/7/PACKET: -Context=1; The first packet was dropped by packet filter or object-policy. Src-Zone=Trust, Dst-Zone=Untrust;If-In=GigabitEthernet2/0/6(71), If-Out=GigabitEthernet2/0/5(70); Packet Info:Src-IP=192.168.2.2, Dst-IP=39.156.66.18, VPN-Instance=none,Src-Port=53219, Dst-Port=443. Protocol=TCP(6). Flag=SYN. Seq=1125947972.

*Aug 29 11:24:38:864 2020 H3C ASPF/7/PACKET: -Context=1; The first packet was dropped by packet filter or object-policy. Src-Zone=Trust, Dst-Zone=Untrust;If-In=GigabitEthernet2/0/6(71), If-Out=GigabitEthernet2/0/5(70); Packet Info:Src-IP=192.168.2.2, Dst-IP=39.156.66.14, VPN-Instance=none,Src-Port=53207, Dst-Port=443. Protocol=TCP(6). Flag=SYN. Seq=3788447735.
```

配置关键点

无