H3C V7平台 防火墙 URL 过滤用户自定义字段配置案例

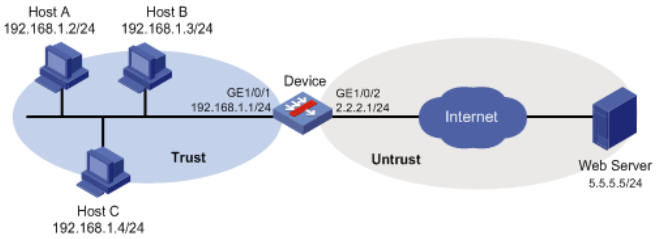
URL过滤 丁犁 2019-07-01 发表

组网及说明

如下图所示，Device分别通过Trust安全域和Untrust安全域与局域网和Internet相连。现有组网需求如下：

- 配置URL过滤功能，不允许Trust安全域的主机访问Untrust安全域的Web Server上包含“/_asyn/”字段的URL及，不允许访问www.xxx.com/_asyn/abc 或 www.xxx.com/yyy/_asyn/123 等。

- 配置URL过滤策略的缺省动作为允许和生成日志。



配置步骤

(1) 配置各接口的IP地址（略）

(2) 创建安全域并将接口加入安全域

向安全域Trust中添加接口GigabitEthernet1/0/1。

system-view

[Device] security-zone name trust

[Device-security-zone-Trust] import interface gigabitethernet 1/0/1

[Device-security-zone-Trust] quit

向安全域Untrust中添加接口GigabitEthernet1/0/2。

[Device] security-zone name untrust

[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2

[Device-security-zone-Untrust] quit

(3) 配置对象组

创建名为urlfilter的IP地址对象组，并定义其子网地址为192.168.1.0/24。

[Device] object-group ip address urlfilter

[Device-obj-grp-ip-urlfilter] network subnet 192.168.1.0 24

[Device-obj-grp-ip-urlfilter] quit

(4) 配置URL过滤功能

 # 创建名为async的URL过滤分类，并进入URL过滤分类视图，设置该分类的严重级别为2000。

[Device] url-filter category async severity 2000

在URL过滤分类async中添加URL过滤规则，模糊匹配“/_asyn/”字段。

[Device-url-filter-category-async] rule 1 host regex www uri regex _async

[Device-url-filter-category-async] rule 2 host regex com uri regex _async

[Device-url-filter-category-async] rule 3 host regex edu uri regex _async // 由于regx 最少三个字符串，因此主机名 不能用cn 模糊匹配

[Device-url-filter-category-async] quit

创建名为urlnews的URL过滤策略，并进入URL过滤策略视图。

[Device] url-filter policy urlnews

 # 在URL过滤策略urlnews中，配置URL过滤分类 async 绑定的动作为丢弃和打印日志。

[Device-url-filter-policy-urlnews] category async action drop logging

在URL过滤策略urlnews中，配置策略的缺省动作为允许和打印日志。

[Device-url-filter-policy-urlnews] default-action permit logging

[Device-url-filter-policy-urlnews] quit

(5) 配置DPI应用profile

创建名为sec的DPI应用profile，并进入DPI应用profile视图。

[Device] app-profile sec

在DPI应用profile sec中应用URL过滤策略urlnews。
[Device-app-profile-sec] url-filter apply policy urlnews
[Device-app-profile-sec] quit
激活DPI各业务模块的策略和规则配置。
[Device] inspect activate
(6)　配置安全策略引用URL过滤业务
进入IPv4安全策略视图
[Device] security-policy ip
创建名为urlfilter的安全策略规则，过滤条件为：源安全域Trust、源IP地址对象组urlfilter、目的安全域Untrust。动作为允许，且引用的DPI应用profile为sec。
[Device-security-policy-ip] rule name urlfilter
[Device-security-policy-ip-13-urlfilter] source-zone trust
[Device-security-policy-ip-13-urlfilter] source-ip urlfilter
[Device-security-policy-ip-13-urlfilter] destination-zone untrust
[Device-security-policy-ip-13-urlfilter] action pass
[Device-security-policy-ip-13-urlfilter] profile sec
[Device-security-policy-ip-13-urlfilter] quit
激活安全策略配置。
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit

配置关键点

不涉及