V7 防火墙使用SSL解密配合完成HTTPS网站过滤

域间策略/安全域 SSL URL过滤 薛佳宇 2022-08-25 发表

组网及说明

缺省情况下，设备仅对HTTP流量进行URL过滤，如果需要对HTTPS流量进行URL过滤，则可以选择如下方式：

①：使用SSL解密功能：先对HTTPS流量进行解密，然后再进行URL过滤。有关SSL解密功能的详细介绍，请参见“DPI深度安全配置指导”中的“代理策略”。
②：开启HTTPS流量过滤功能：不对HTTPS流量进行解密，直接对客户端发送的HTTPS的Client HELLO报文中的SNI（Sever Name Indication extension）字段进行检测，从中获取用户访问的服务器域名，使用获取到的域名与URL过滤策略进行匹配。

由于SSL解密功能涉及大量的加解密操作，会对设备的转发性能会产生较大的影响，建议在仅需要对HTTPS流量进行URL过滤业务处理的场景下开启HTTPS流量过滤功能。

本案例介绍使用SSL解密方式，测试PC在trust域，运营商出口在untrust域

配置步骤

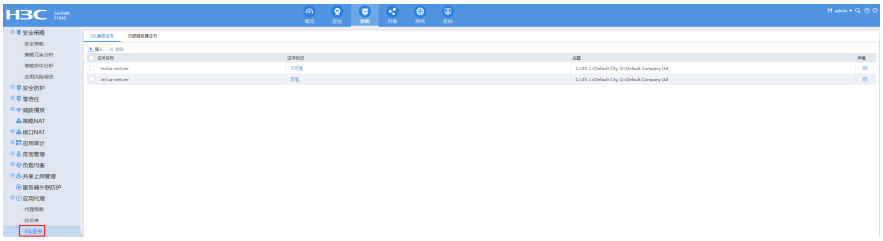
一、生成CA证书

具体可以参考我的另一个案例：https://zhiliao.h3c.com/theme/details/140116

需要注意的是，导入到防火墙的CA证书需要包含密钥对，且要配置密码

二、防火墙导入SSL解密证书

策略---应用代理---SSL证书---SSL解密证书



三、配置代理策略

策略---应用代理---代理策略

四、配置URL过滤配置文件

对象---应用安全---URL过滤---配置文件

五、安全策略调用URL过滤配置文件

策略---安全策略

配置关键点P配置

对象->应用安全->高级配置->配置激活

1、导入到防火墙的CA证书需要包含密钥对，且要配置密码

2、SSL解密功能涉及大量的加解密操作，会对设备的转发性能会产生较大的影响，建议在仅需要对HTTPS流量进行URL过滤业务处理的场景下开启HTTPS流量过滤功能

七、PC安装前面的可信证书到“信任的根证书颁发机构”

八、验证