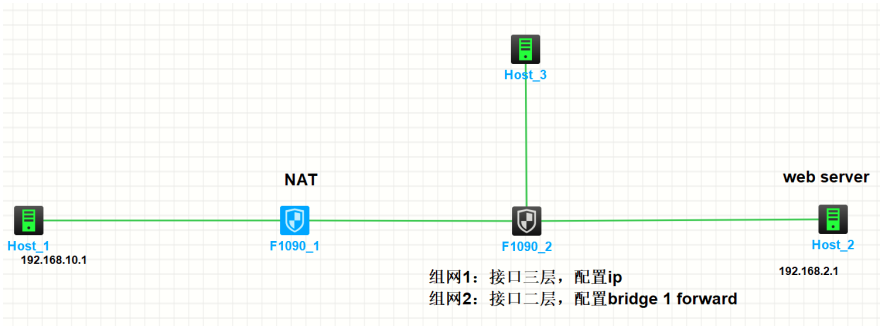
防火墙IPS重定向功能实现

IPS防攻击 **戴航** 2022-06-13 发表

组网及说明

防火墙墙二层或三层部署在网络中，安全策略中引用IPS策略，需要对特定或所有IPS攻击进行重定向。



告警信息

不涉及

问题描述

DPI重定向功能说明：

1、DPI的IPS/AV/url过滤/waf 等模块均支持重定向；

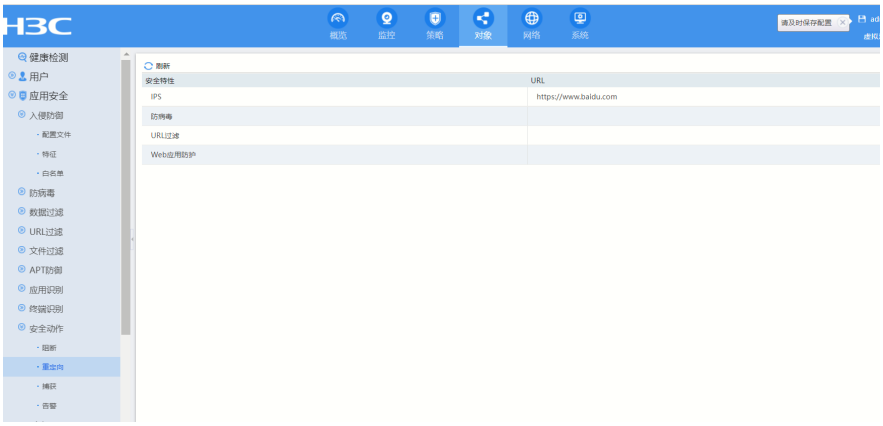
2、仅支持http的重定向；对于https，需结合https解密功能才能重定向；

3、当命中规则后，防火墙通伪造200 OK 报文回复给客户端，在html body中构造from标签，指定终端向特定的url提交表单，实现重定向的效果。

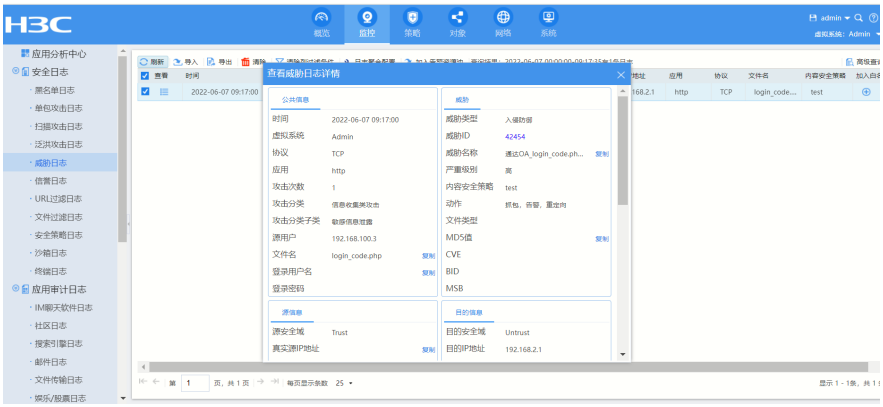
4、防火墙二层、三层组网下均支持重定向功能，特别的：bridge inline模式组网下，加入bridge桥中的接口模式必须是bridge模式，如果是route模式重定向报文无法发出。

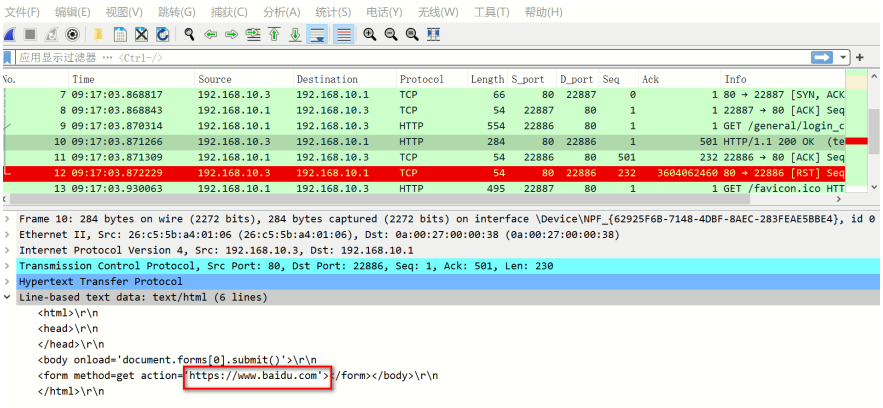
典型实例：针对某特定规则进行重定向

构造攻击：http://192.168.10.3/general/login_code.php?codeuid={8F034ED0-827A-3998-BACF-E4337F68E34B} （此攻击对应IPS 42454号规则）




https://www.baidu.com/?
新闻 hao123 地图 贴吧 视频 图片 网盘 更多
北京 21℃
Bai du 百度
百度一下
直击2022高考，为考生加油!
我的关注 推荐
+ 自定义
我的导航
显示分类 编辑


H3C
概览 监控 策略 对象 网络 系统
admin
虚拟系统：Admin
应用分析中心
安全日志
黑名单日志
单包攻击日志
扫描攻击日志
泛洪攻击日志
威胁日志
信誉日志
URL过滤日志
文件过滤日志
安全策略日志
沙箱日志
终端日志
应用审计日志
IM聊天软件日志
社区日志
搜索引擎日志
邮件日志
文件传输日志
娱乐/股票日志
查看威胁日志详情
公共信息
时间 2022-06-07 09:17:00
虚拟系统 Admin
协议 TCP
应用 http
攻击次数 1
攻击分类 信息收集类攻击
攻击分类子类 敏感信息泄露
源用户 192.168.100.3
文件名 login_code.php
登录用户名
登录密码
威胁
威胁类型 入侵防御
威胁ID 42454
威胁名称 通达OA_login_code.ph...
严重级别 高
内容安全策略 test
动作 抓包，告警，重定向
文件类型
MD5值
CVE
BID
MSB
源信息
源安全域 Trust
真实源IP地址
目的信息
目的安全域 Untrust
目的IP地址 192.168.2.1


文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 ... <Ctrl-/>
No. Time Source Destination Protocol Length S_port D_port Seq Ack Info
7 09:17:03.868817 192.168.10.3 192.168.10.1 TCP 66 80 22887 0 1 80 → 22887 [SYN, ACK
8 09:17:03.868843 192.168.10.1 192.168.10.3 TCP 54 22887 80 1 1 22887 → 80 [ACK] Seq
9 09:17:03.870314 192.168.10.1 192.168.10.3 HTTP 554 22886 80 1 1 GET /general/login_c
10 09:17:03.871266 192.168.10.3 192.168.10.1 HTTP 284 80 22886 1 501 HTTP/1.1 200 OK (te
11 09:17:03.871309 192.168.10.1 192.168.10.3 TCP 54 22886 80 501 232 22886 → 80 [ACK] Seq
12 09:17:03.872229 192.168.10.3 192.168.10.1 TCP 54 80 22886 232 3604062460 80 → 22886 [RST] Seq
13 09:17:03.930063 192.168.10.1 192.168.10.3 HTTP 495 22887 80 1 1 GET /favicon.ico HTT
Frame 10: 284 bytes on wire (2272 bits), 284 bytes captured (2272 bits) on interface \Device\NPF_{62925F6B-7148-4DBF-8AEC-283FEAE5BBE4}, id 0
Ethernet II, Src: 26:c5:5b:a4:01:06 (26:c5:5b:a4:01:06), Dst: 0a:00:27:00:00:38 (0a:00:27:00:00:38)
Internet Protocol Version 4, Src: 192.168.10.3, Dst: 192.168.10.1
Transmission Control Protocol, Src Port: 80, Dst Port: 22886, Seq: 1, Ack: 501, Len: 230
Hypertext Transfer Protocol
Line-based text data: text/html (6 lines)
<html>\r\n
<head>\r\n
</head>\r\n
<body onload='document.forms[0].submit()'>\r\n
<form method=get action='https://www.baidu.com'></form></body>\r\n
</html>\r\n

解决方法

不涉及