M9K系列IPS防护策略配置举例

IPS防攻击　zhiliao_5ilsv　2019-09-03 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

本案例适用于如M9006、M9010、M9014等M9K系列的防火墙。

1.2 使用限制

防火墙IPS功能需要安装License才能使用。License过期后，IPS功能可以采用设备中已有的IPS特征库正常工作，但无法升级特征库。

配置前请在防火墙界面“系统”>”License”>”授权信息”中确认IPS特性为激活状态。

位置	特性名称	是否授权	类型	状态	有效期	安装时间
Slot2	6					2018-09-26 19:00:51
	AV	Y	Trial (date restricted)	In use	2018-09-26至2018-12-2	
	SSL VPN	Y	Trial (date restricted)	In use	2018-09-26至2018-12-2	
	ACG	Y	Trial (date restricted)	In use	2018-09-26至2018-12-2	
	IPS	Y	Trial (date restricted)	In use	2018-09-26至2018-12-2	
	SLB	N	-	-	-	

1.3 功能介绍及配置需求

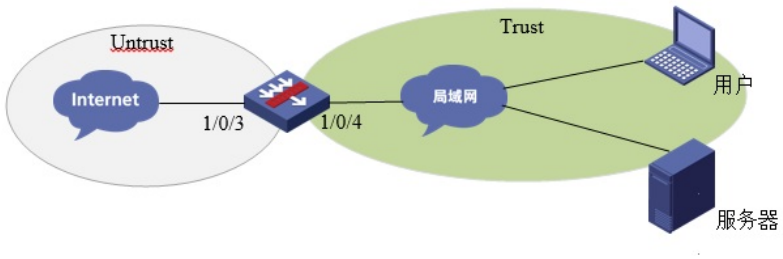
IPS（Intrusion Prevention System，入侵防御系统）是一种可以对应用层攻击进行检测并防御的安全防御技术。IPS通过分析流经设备的网络流量来实时检测入侵行为，并通过一定的响应动作来阻断入侵行为，实现保护企业信息系统和网络免遭攻击的目的。

配置需求：

1）为应对目前肆虐的**WannaCry**变种病毒，需要在公司外网进行IPS防护。2）对Microsoft Windows系统等漏洞进行防范。

配置步骤

2 组网图



3 配置步骤

3.1 基础组网配置

略

3.2 升级特征库至官网最新版本

在防火墙界面“系统”>”升级中心”>”特征库升级”中对特征库进行升级

升级中心列表

刷新　配置代理服务器

特征库	当前版本	版本发布日期	开启定时升级	定时升...	操作
入侵防御特征库	1.0.35	2017-05-17	☐	-	立即升级 | 本地升级 | 版本回退
防病毒特征库	1.0.36	2017-05-13	☐	-	立即升级 | 本地升级 | 版本回退
应用识别特征库	1.0.0	1999-12-31	☐	-	立即升级 | 本地升级 | 版本回退
URL特征库	1.0.0	1999-12-31	☐	-	立即升级 | 本地升级 | 版本回退

3.2.1 自动升级操作过程

1. 设备开启DNS代理并配置DNS服务器地址

在防火墙界面“网络”>”DNS”>”高级设置”开启防火墙DNS代理功能。

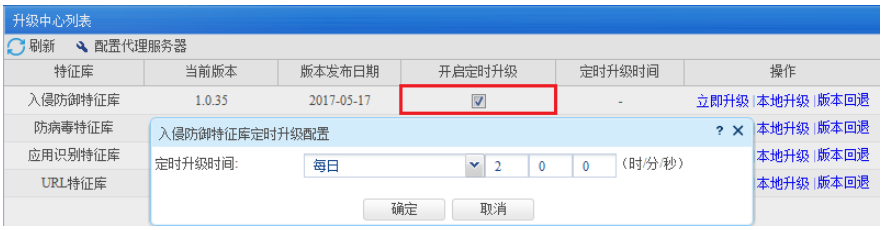
在防火墙界面“网络”>”DNS”>”DNS客户端”中添加DNS服务器地址。

2. 设备必须可以连接互联网

在防火墙界面“网络”>”探测工具”>”Ping”中测试域名是否可以正常解析?

3. 开启设备定时升级功能

在防火墙界面“系统”>”升级中心”>”特征库升级”中 开启入侵防御特征库定时升级功能。



3.2.2 手动升级操作过程

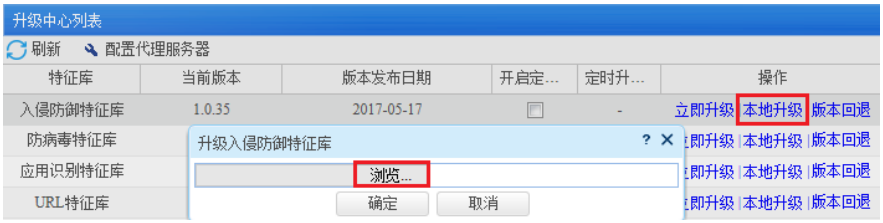
部分设备部署环境可能无法访问互联网，需要使用手动升级更新特征库。

1. 在华三官网下载防火墙最新特征库文件

登录“www.h3c.com” 华三官网，在“产品技术”>“大安全”>”特征库服务专区”中下载IPS特征库文件。

2. 升级特征库

在“浏览”中选择下载好的特征库文件，点击“确定”后完成升级。



3.3 配置对外网的IPS防护策略

3.3.1 新建安全策略

在防火墙界面“策略”>”安全策略”>新建源安全域为“Untrust”目的安全域为“Trust”的安全策略，在内容安全中将IPS的”default”策略调用。

说明：特征库对IPS特征有默认的过滤策略，直接调用default即可，如需要自行定制过滤策略请在防火墙界面“对象”>”应用安全”>“入侵防御”>”配置文件”中新建自定义的IPS规则。

3.4 测试结果

3.4.1 对Microsoft Windows系统漏洞攻击防护测试

执行python脚本构造攻击

1）将struts2-243.py脚本中服务器地址修改为web server地址

2）在kali下运行脚本

```
root@kali:~/Desktop/python_test# ./struts2-243.py
Traceback (most recent call last):
  File "./struts2-243.py", line 12, in <module>
    response = urllib2.urlopen(request, "class.classLoader.jarPath=%28%23context
['xwork.MethodAccessor.denyMethodExecution']%3d+new+java.lang.Boolean%28false%29
%2c+%23_memberAccess['allowStaticMethodAccess']%3dtrue%2c+%23a%3d%40java.lang.Ru
ntime%40getRuntime%28%29.exec%28%27uname -r%27%29.getInputStream%28%29%2c%23b%3d
new+java.io.InputStreamReader%28%23a%29%2c%23c%3dnew+java.io.BufferedReader%28%2
3b%29%2c%23d%3dnew+char[50000]%2c%23c.read%28%23d%29%2c%23k8team%3d%40org.apache
.struts2.ServletActionContext%40getResponse%28%29.getWriter%28%29%2c%23k8team.pr
intln%28%23d%29%2c%23k8team.close%28%29%29%28meh%29&z[%28class.classLoader.jarPa
th%29%28%27meh%27%29]")
  File "/usr/lib/python2.7/urllib2.py", line 127, in urlopen
    return _opener.open(url, data, timeout)
  File "/usr/lib/python2.7/urllib2.py", line 401, in open
    response = self._open(req, data)
```

设备检测到攻击后生成日志：

```
<H3C>%May 17 11:27:08:809 2017 H3C IPS/4/IPS_IPV4_INTERZONE: -Context=1; Protoco
l(1001)=TCP; Application(1002)=http; SrcIPAddr(1003)=184.37.0.124; SrcPort(1004)
=56163; DstIPAddr(1007)=184.37.0.152; DstPort(1008)=80; RcvVPNInstance(1042)=; S
rcZoneName(1025)=Trust; DstZoneName(1035)=Untrust; PolicyName(1079)=ips; AttackN
ame(1088)=CVE-2017-5638_Apache_Struts2_Remote_Commond_Execution_Vulnerability(S2
-046); AttackID(1089)=32374; Category(1090)=Vulnerability; Protection(1091)=WebS
erver; SubProtection(1092)=Apache; Severity(1087)=CRITICAL; Action(1053)=Reset &
 Logging; CVE(1075)=CVE-2017-5638; BID(1076)=BID-96729; MSB(1077)=--; HitDirecti
on(1115)=original; RealSrcIP(1100)=;
```

管理员可在设备管理界面“监控 > 安全日志 > 威胁日志”中，定期查看威胁日志信息。

配置关键点