F10X0/F50X0系列防火墙防病毒策略配置举例

AV防病毒 张旭 2019-04-08 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F1080、F1070、F5040、F5020等F10X0、F50X0系列的防火墙。

1.2 使用限制

防火墙防病毒功能需要安装License才能使用。License过期后，防病毒功能可以采用设备中已有的防病毒特征库正常工作，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”中确认防病毒（AV）特性为激活状态。

License授权信息

刷新

位置	特性名称	是否授权	状态
Slot1	ACG	N	-
Slot1	AV	Y	In use
Slot1	IPS	N	-
Slot1	SLB	N	-
Slot1	SSLVPN	N	-
Slot1	UFLT	N	-

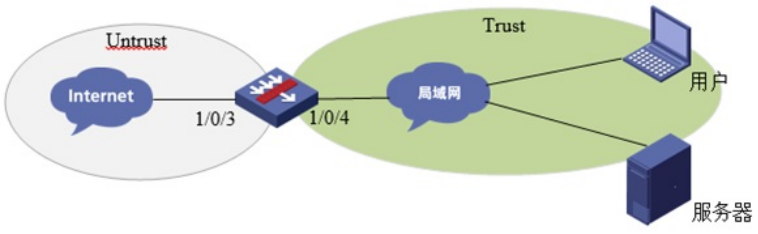
1.3 功能介绍及配置需求

防病毒（AV）功能是一种通过对报文应用层信息进行检测来识别和处理病毒报文的安全机制。防病毒功能凭借庞大且不断更新的病毒特征库可有效保护网络安全，防止病毒在网络中的传播。将具有防病毒功能的设备部署在企业网入口，可以将病毒隔离在企业网之外，为企业内网的数据安全提供坚固的防御。目前，该功能支持对基于FTP、HTTP、IMAP、POP3和SMTP的协议传输的报文进行防病毒检测。

配置需求：

1）为防御通过HTTP网页传播的电脑病毒，需要在公司防火墙部署病毒防护策略。

2 组网图



配置步骤

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。

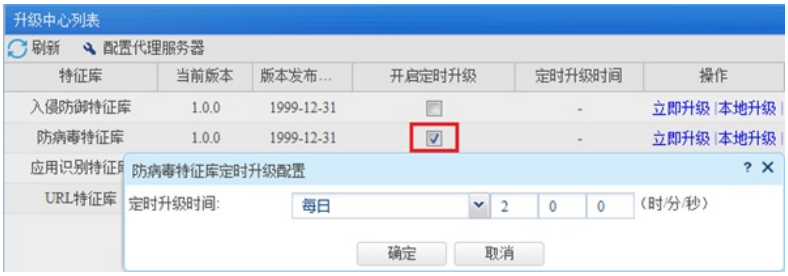
在防火墙界面“网络”>”DNS”>”DNS客户端”中添加DNS服务器地址。

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。

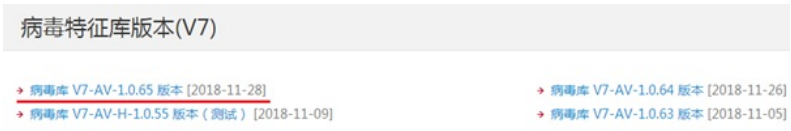


3.2.2 手动升级操作过程

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。

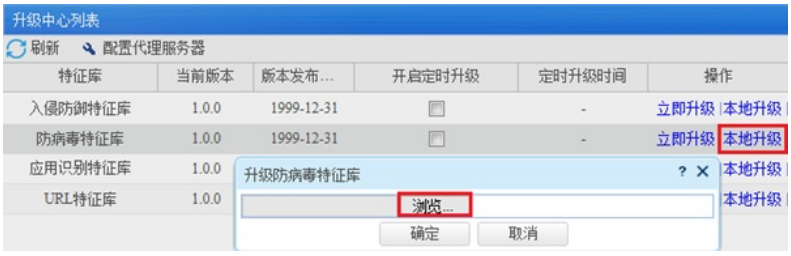
1. 在华三官网下载防火墙最新特征库文件

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



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 配置对外网的防病毒策略

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，在内容安全中将防病毒的”default”策略调用。

说明：防病毒特征有默认的过滤策略，缺省情况下已经默认设置完成，直接调用default策略即可，如需要自行定制过滤策略请在防火墙界面“对象”>”应用安全”>“防病毒”>”配置文件”中新建自定义的防病毒规则。

配置关键点

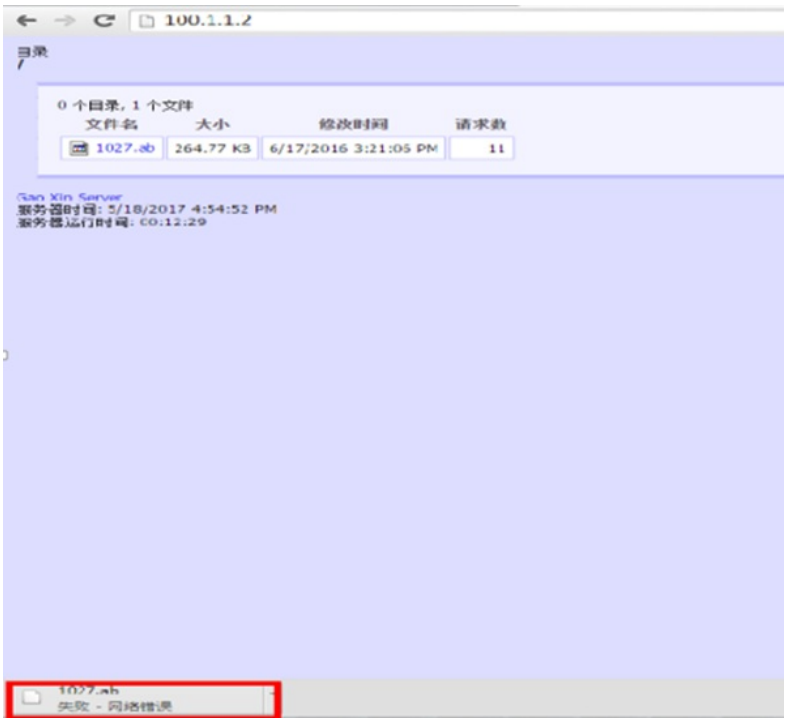
3.4 测试结果

3.4.1 对HTTP病毒防御测试

1. 在服务器存放病毒文件1027.ab

2. WEB Client登录server后，获取该病毒文件；

客户端界面显示获取病毒文件失败。



设备系统日志中显示已经将该病毒文件重置。

```
<H3C>%May 19 10:21:19:626 2017 H3C ANTI-VIR/4/ANTIVIRUS_IPV4_INTERZONE: -Context
=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPAddr(1003)=184.38.0.117; Sr
cPort(1004)=55517; DstIPAddr(1007)=100.1.1.2; DstPort(1008)=80; RcvVPNInstance(1
042)=--; SrcZoneName(1025)=Trust; DstZoneName(1035)=Untrust; PolicyName(1079)=b;
 VirusName(1085)=Trojan.Win32.Agent.roml; VirusID(1086)=1027; Severity(1087)=LOW
; Action(1053)=Reset & Logging; HitDirection(1115)=reply; 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。