F1000-X-G2/F100-X-G2系列防护WannaCry勒索病毒配置举例

AV防病毒 zhiliao_5ilsv 2019-11-28 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F1000-A-G2、F1000-S-G2、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙。

1.2 使用限制

防火墙IPS（入侵防御）功能需要安装License才能使用。License过期后，IPS（入侵防御）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”中确认应用（ACG）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	N	-
Slot1	IPS	Y	In use
Slot1	SLB	N	-
Slot1	SSLVPN	N	-
Slot1	UFLT	N	-

1.3 功能介绍及配置需求

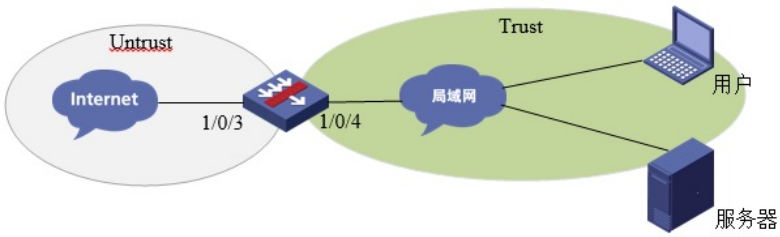
勒索病毒利用电脑系统中445端口（用于共享文件或共享打印机）和139端口为主要通道，悄悄共享被攻击者电脑的硬盘使网络黑客有机可乘，然后黑客在被攻击者电脑里上传网络病毒。该病毒会将电脑硬盘中的照片、文档、压缩包、音频、视频、可执行文件等进行加密，加密后文件后缀名统一修改为“.WNCRY”，并且在电脑屏幕上显示勒索信息，被攻击者只要支付一定费用便可以获取解密方法。

该病毒之所以能传播如此迅速是因为利用了微软基于455端口传播的SMB漏洞MS17-010，2017年3月份微软已经发布过该漏洞的系统补丁。所以此次病毒影响主要波及以下操作系统：Windows 2000、Windows 2003、Windows XP、Windows Vista、Windows 7、Windows 8、Windows 10、Windows 2008、Windows 2012。

配置需求：

某公司为保证内网电脑不受勒索病毒影响，希望在防火墙上能阻断勒索病毒。

2 组网图



配置步骤

3 常用防护手段

3.1 终端侧勒索病毒预防方法

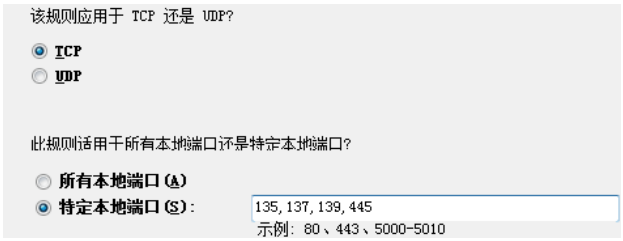
1、及时安装更新补丁，确认电脑上已经安装了MS17-010补丁。

2、出口路由器自带NAT功能，默认外网是不能向内网电脑发起连接的，对病毒也是如此。但是电脑如果主动向病毒服务器发起数据连接那么就会突破这层屏障。所以请不要打开不明链接、应用以避免中毒。

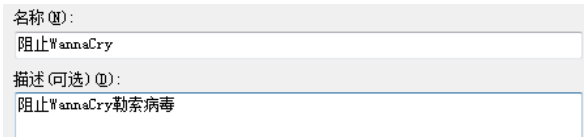
3、如果暂时难于完成补丁安装，您可以使用windows自带防火墙禁止445端口。

打开“控制面板”，单击“防火墙”，然后单击“高级设置”。进入新建规则设置界面。

规则类型选择“端口”点击下一步，输入“135、137、139、445”端口点击下一步。



选择“阻止端口”后为新建策略命名。



最后请在“打开或关闭Windows防火墙”中开启Windows防火墙。

3.2 防火墙防护勒索病毒方法

H3C防火墙防御此病毒的方法有两种：

1、通过域间策略禁止445、135等端口。

2、通过IPS策略检测利用MS17-010相关漏洞的病毒并重置。

3.2.1 通过封禁端口的方式防御勒索病毒

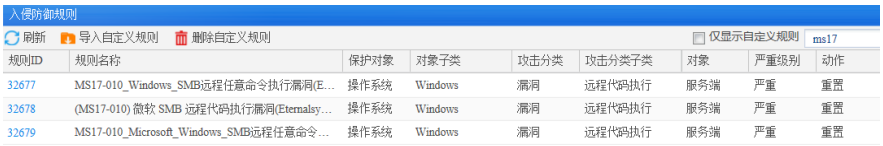
例如：利用防火墙过滤445端口的数据（其他病毒端口设置方法一致）。

在“对象组”中选择“服务对象组”添加名称为“WannaCry”的对象组并编辑445端口的对象。

点击“策略”>“安全策略”配置源域为“untrust”目的域为“trust”禁止目的地端口为445的端口。

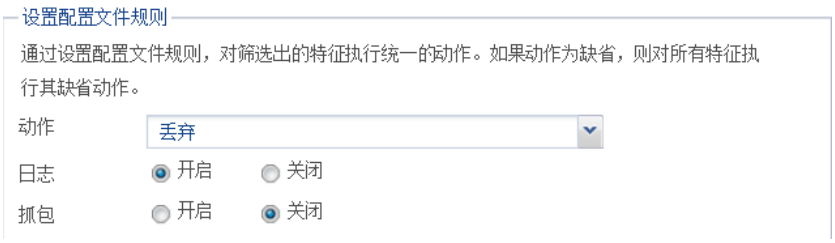
3.2.2 通过IPS功能防御勒索病毒

目前我司防火墙IPS特征库已经完全可以防护MS17-010漏洞造成的攻击。



在“应用安全”中点击“入侵防御”》“配置文件”点击新建。新建“防御Wannacry”筛选对象为“操作系统”筛选攻击分类为“漏洞”。对象为“服务端”，缺省动作为重置，级别为“严重”和“高”。

缺省动作选择丢弃并记录日志



在安全策略中选择“新建”源安全域现则“untrust”目的区域为“trust”区域并调用“防御Wannacry”策略。

3.3 配置注意事项

随着时间的推移病毒端口、特征等也在变化，如果想要及时防护病毒需要做到以下几点：

1、及时更新电脑操作系统，避免漏洞出现被黑客利用。

2、防火墙及时更新IPS特征库，即使病毒变异也能进行防御。

3、验证良好的上网习惯，不打开不明链接或者安装不安全应用。

配置关键点