

360 防火墙针对“永恒之蓝”勒索蠕虫的防护方案

1 漏洞描述

近期国内多处高校网络出现 ONION/Wncry 勒索软件感染情况，磁盘文件会被病毒加密为.onion 后缀，只有支付高额赎金才能解密恢复文件，对重要数据造成严重损失。

根据网络安全机构通报，这是不法分子利用 NSA 黑客武器库泄漏的“永恒之蓝”发起的蠕虫病毒攻击事件。恶意代码会扫描开放 445 文件共享端口的 Windows 机器，无需用户任何操作，只要开机上网，不法分子就能在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币挖矿机等恶意程序。

由于以前国内多次爆发利用 445 端口传播的蠕虫，部分运营商在主干网络上封禁了 445 端口，但是教育网并没有此限制，仍然存在大量暴露 445 端口且存在漏洞的电脑，导致目前此蠕虫在教育网内大量传播，大概量级是每天 5000 个用户中招。

360 新一代智慧防火墙（NSG3000/5000/7000/9000 系列）和下一代极速防火墙（NSG3500/5500/7500/9500 系列）产品系列，通过更新 IPS 特征库、应用识别特征库已经完成了蠕虫变种的防护，建议用户尽快将 IPS 特征库升级至“20170513”版本，应用识别特征库升级至“20170513”版本。此外，由于该攻击已开始在教育网内泛滥，不排除高校部分开放 445 端口的主机已被攻击，360 新一代智慧防火墙基于“智慧发现”、“智慧调查”特性可高效检测、统计产生此类攻击的终端 IP，协助用户快速定位已失陷主机以便于及时在终端系统进行处置操作。

特别提醒：WanaCry!勒索软件除了通过 ms17-010 的 SMBv1 传播,还可能通过曾经被安装过 NSA DoublePulsar 后门的渠道进行传播，曾被 EternalBlue 攻击并成功安装过 DoublePulsar 后门的系统，即便已安装 ms17-010 补丁仍有可能被该勒索软件感染。

2 处置建议

1. 立即封堵不必要的 SMB 协议（TCP 445 端口）；
2. 针对必须启用 SMB 协议的网络进行深度的 IPS 检测，及时阻断攻击；
3. 诱导方式，通过防火墙的静态 dns 功能进行诱导；
4. 在网络内部安全域间部署防火墙设备，通过隔离安全域降低攻击的影响范围；

3 配置指引

3.1 封堵 SMB 协议

3.1.1 新一代智慧防火墙配置方法

可通过配置 “一键处置” 或 “安全策略” 功能实现阻断（二者任选其一即可）。

方式 1: 通过 “一键处置” 阻断

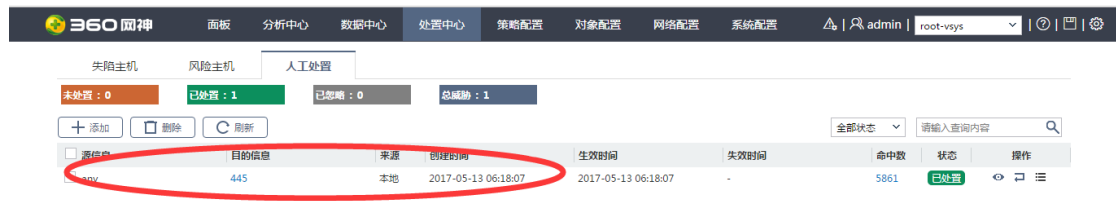
1. 登录防火墙管理界面，进入 “处置中心->人工处置”，点击 “+添加”，新建一条处置策略；



2. 按照下图参数设定，配置处置策略，“目的端口” 填写 “445”，“处置动作” 选择 “阻断”，点击 “确定” 完成新建；

The screenshot shows the '添加处置' (Add Disposal) form. The form has the following fields: '处置类型' (Disposal Type) set to '网络连接' (Network Connection), '地址类型' (Address Type) with 'IPv4' selected and 'IPv6' unselected, '源地址' (Source Address) set to 'any', '源端口' (Source Port) set to 'any' (with a range of 1-65535), '目的地址' (Destination Address) set to 'any', '目的端口' (Destination Port) set to '445' (with a range of 1-65535, highlighted with a red circle), '协议' (Protocol) set to 'any', '处置动作' (Disposal Action) set to '阻断' (Block), and '处置时间' (Disposal Time) set to '永久' (Permanent). At the bottom right, there are '确定' (Confirm) and '取消' (Cancel) buttons, with the '确定' button highlighted by a red circle and an arrow pointing to it from the '目的端口' field.

3. 确认处置策略添加成功。



方式 2: 通过“安全策略”阻断

1. 登录防火墙管理界面，进入“对象配置->服务->自定义服务”，点击“+添加”，新建一个服务对象；



2. 按照下图参数设定，配置服务对象，“源端口”填写“0~65535”，“目的端口”填写“445~445”，点击“确定”完成新建；

添加服务

名称: SMB_445 * (1-63字符)

描述: (0-127字符)

协议: + 添加 删除

协议: TCP

源端口: 1 - 65535 * (0-65535)

目标端口: 445 - 445 * (0-65535)

确定 取消

没有记录

(0-32项)

确定 取消

3. 确认服务对象添加成功；

360 网神 面板 分析中心 数据中心 处置中心 **策略配置** 对象配置 网络配置 系统配置

admin | root-vsys

地址 国家/地区 服务 服务组 应用 时间 关键字组 URL分类 自定义签名 安全配置文件 安全配置文件组

自定义服务 自定义服务

+ 添加 删除 刷新

名称	协议	内容	引用	操作
SMB_445	TCP	源端口:1-65535 目标端口:445-445	0	

4. 点击“策略管理->安全策略”，点击“+添加”新建一条安全策略；

360 网神 面板 分析中心 数据中心 处置中心 **策略配置** 对象配置 网络配置 系统配置

admin | root-vsys

安全策略 NAT策略 安全认证 SSL解密策略 IP-MAC绑定 QoS 黑白名单 会话限制 安全防护

安全策略 冗余策略

+ 添加 复制 删除 排序 清除命中数 刷新

名称	源安全域	目的安全域	源地址/地区	目的地址/地区	服务	应用	时间
test	any	any	any	any	any	any	
any	any	any	any	any	any	any	
y	any	any	any	any	any	京东商城	

5. 按照下图参数设定，配置策略条件，“动作”选择“拒绝”，点击“确定”完成新建；

添加安全策略

名称: 禁用SMB_445 * (1-63字符)

描述: (0-127字符)

启用: ☒

动作: ☐ 允许 ☒ 拒绝 ☐ 安全连接(隧道)

源安全域: any

目的安全域: any

源用户: 请选择源用户

源地址/地区: any

目的地址/地区: any

服务: |

应用: 全部

来自隧道: ☒ SMB_445 ☐ SMB_445

时间: |

VLAN: |

服务列表: any, AH, DHCP, DHCPv6, DNS, ESP, FTP, GRE, L2TP

确定 取消

页共 1 页 | 第 1 页

根据实际业务进行选择

6. 在策略列表中选择步骤 5 新建的策略，点击“调序”，并将该策略调整至第一位；

360 网神 面板 分析中心 数据中心 处置中心 策略配置 对象配置 网络配置 系统配置

安全策略

策略配置

策略列表:

名称	源安全域	目的安全域	源地址/地区	目的地址/地区	服务	应用	时间
test	any	any	any	any	any	any	
any	any	any	any	any	any	any	
y	any	any	any	any	any	京东商城	
<input checked="" type="checkbox"/> 禁用SMB_445	any	any	any	any	SMB_445	any	

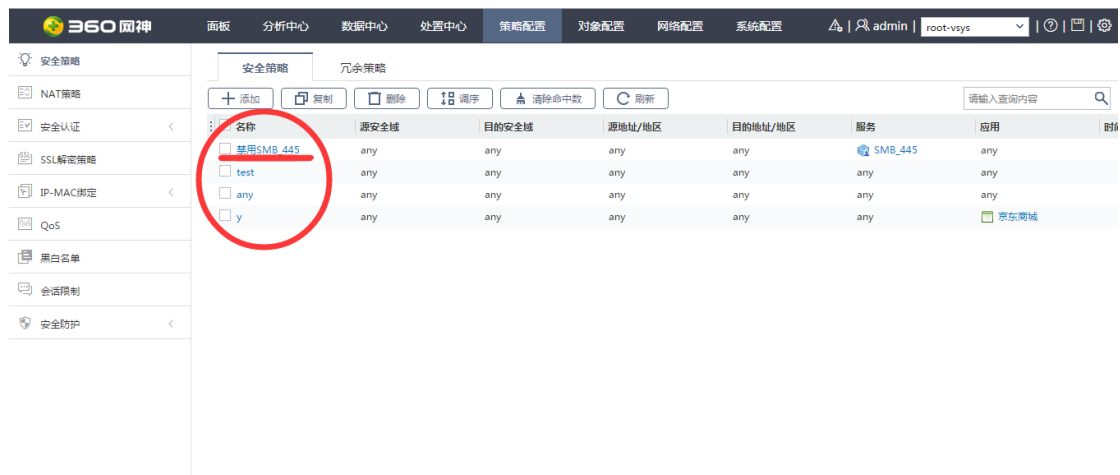
调序

调序对话框:

排序: top

确定 取消

7. 确认该策略排位已至第一。

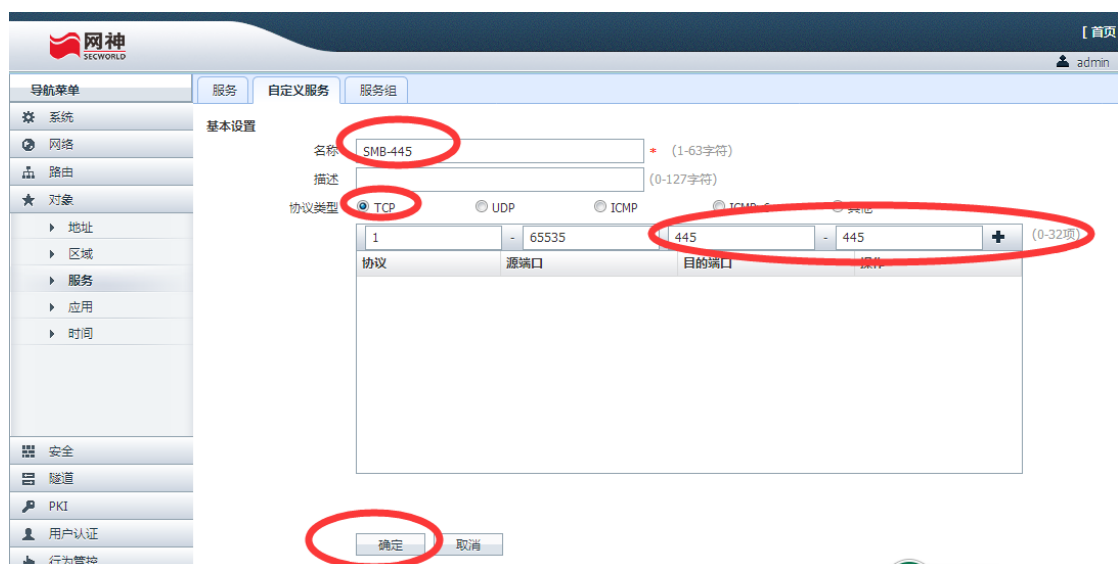


3.1.2 下一代极速防火墙配置方法

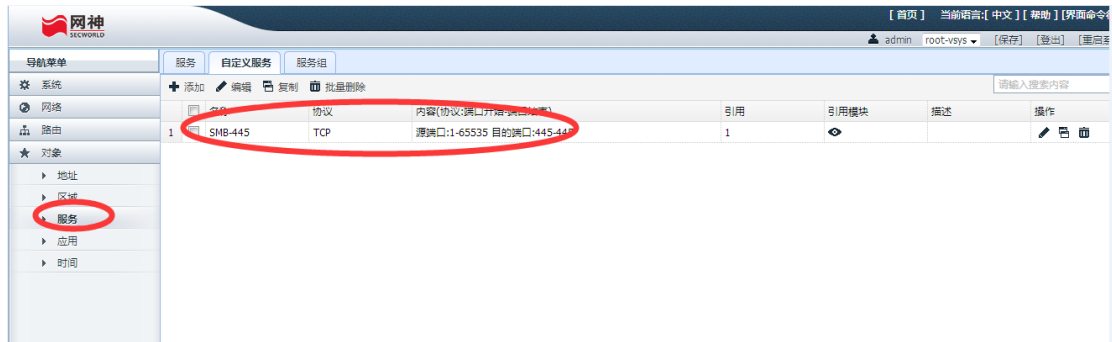
1. 登录防火墙管理界面，进入“对象配置->服务->自定义服务”，点击“+添加”。



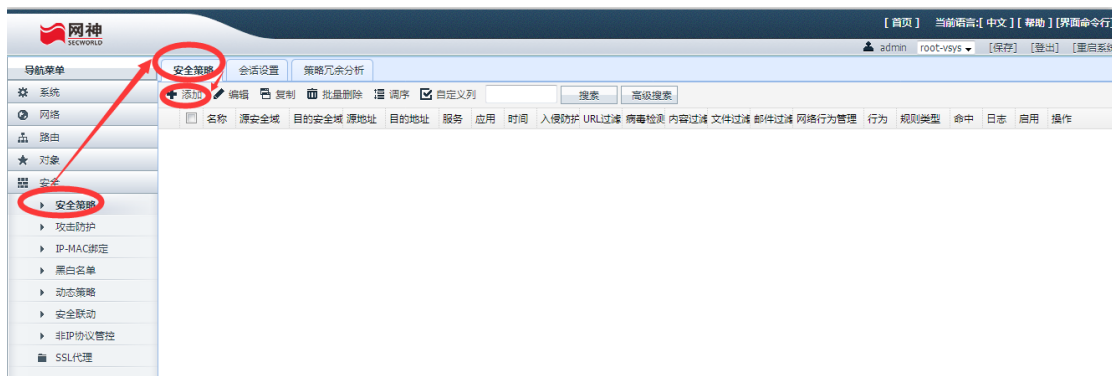
2. 按照下图参数设定，配置服务对象，“源端口”填写“0~65535”，“目的端口”填写“445~445”，点击“确定”完成新建；



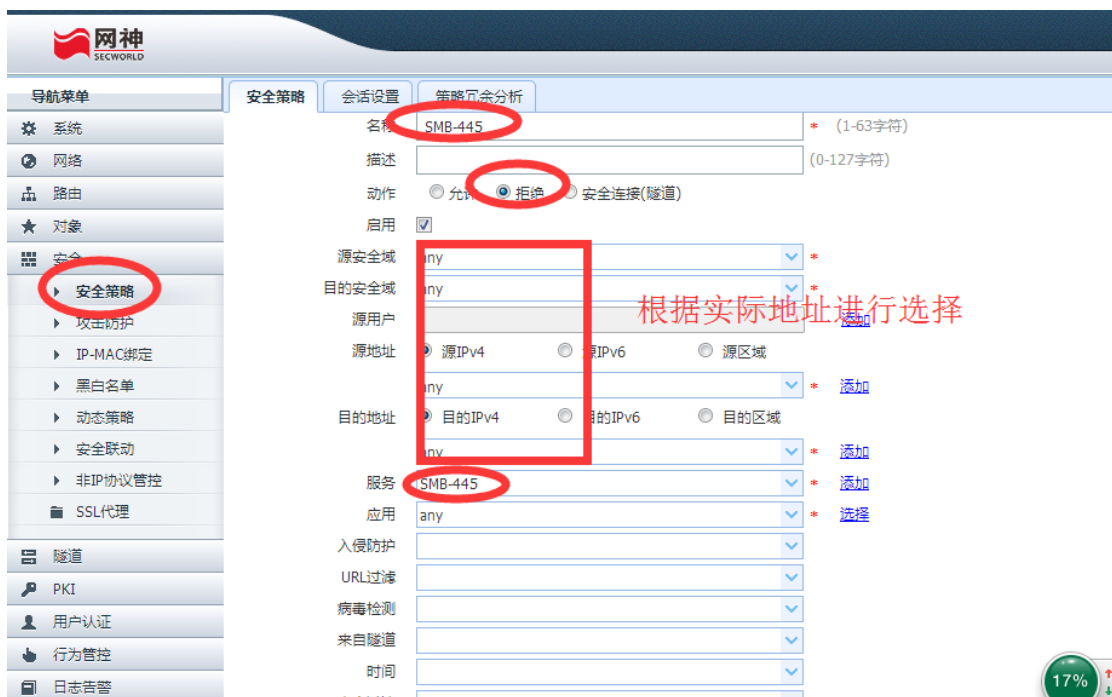
3. 确认服务对象添加成功；



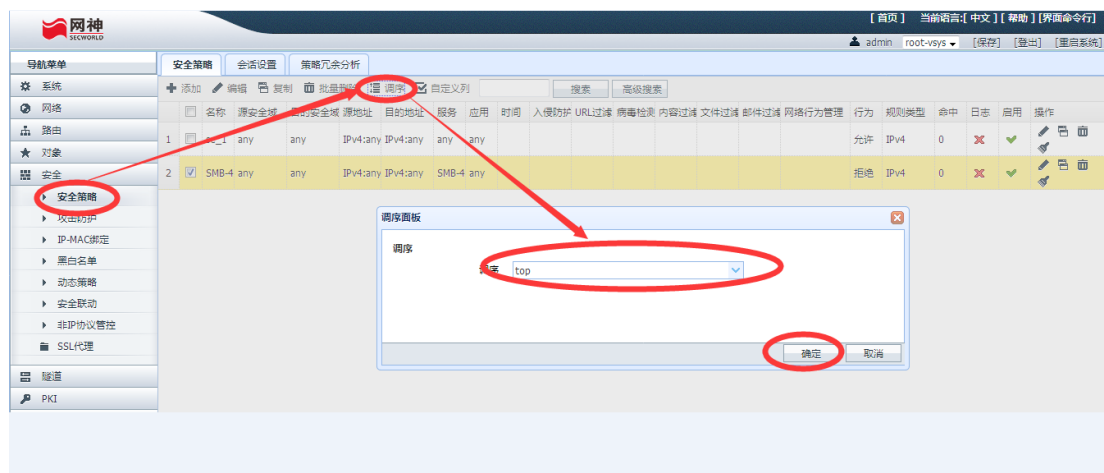
4. 点击“策略管理->安全策略”，点击“+添加”新建一条安全策略；



5. 按照下图参数设定，配置策略条件，“动作”选择“拒绝”，点击“确定”完成新建；



6. 在策略列表中选择步骤 5 新建的策略，点击“调序”，并将该策略调整至第一位



7. 确认该策略排位已至第一。

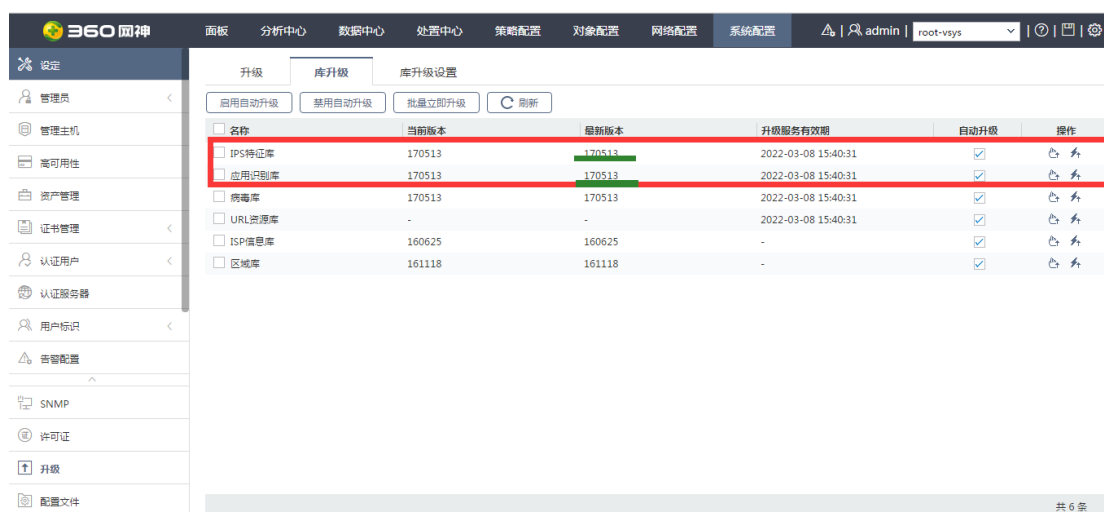


3.2 通过入侵防御、应用控制规则阻断攻击流量

新一代智慧防火墙和下一代极速防火墙均可通过配置入侵防御规则实现攻击阻断,同时可通过配置应用控制规则增强防护效果。

3.2.1 新一代智慧防火墙配置方法

1. 登录防火墙管理界面,进入“系统配置->升级->库升级”确认特征库版本,应确保 IPS 特征库需升级到 20170513,应用识别特征库升级到 20170513;



2. 进入“对象配置->安全配置文件->漏洞防护”,添加一个漏洞防护配置实例;

添加漏洞防护

名称 漏洞防护 * (1-63字符)

描述 (0-127字符)

类型

启用	类别名称	动作
<input checked="" type="checkbox"/>	其它攻击	默认
<input checked="" type="checkbox"/>	缓冲区溢出	默认
<input checked="" type="checkbox"/>	跨站脚本	默认
<input checked="" type="checkbox"/>	拒绝服务	默认
<input checked="" type="checkbox"/>	恶意扫描	默认
<input checked="" type="checkbox"/>	SQL注入	默认
<input checked="" type="checkbox"/>	WEB攻击	默认
<input checked="" type="checkbox"/>	自定义签名	默认

共 8 条

高级

确定 取消

- 新建一条安全策略，在“漏洞防护”中选择步骤 2 中新建的漏洞防护实例，点击确定完成新建；

添加安全策略

应用 请选择应用或应用组

来自隧道 请选择隧道

时间 请选择时间

VLAN 请输入VLAN
(取值范围0-4094, 格式: 1,5,10,12)

流量日志 ☐ 会话开始 ☒ 会话结束

高级

配置文件类型 安全配置文件

漏洞防护 漏洞防护

防间谍软件

URL过滤

反病毒

内容过滤

文件过滤

邮件过滤

确定 取消

- 在策略列表中选择步骤 3 新建的策略，点击“调序”，并将该策略调整至第一位；
- 新建另外一条安全策略，在“应用”中选择“NSA_Eternalblue_17_010_SMB”，“动

作”选择“拒绝”；

6. 在策略列表中选择步骤 5 新建的策略，点击“调序”，并将该策略调整至第一位。

3.2.2 下一代极速防火墙配置方法

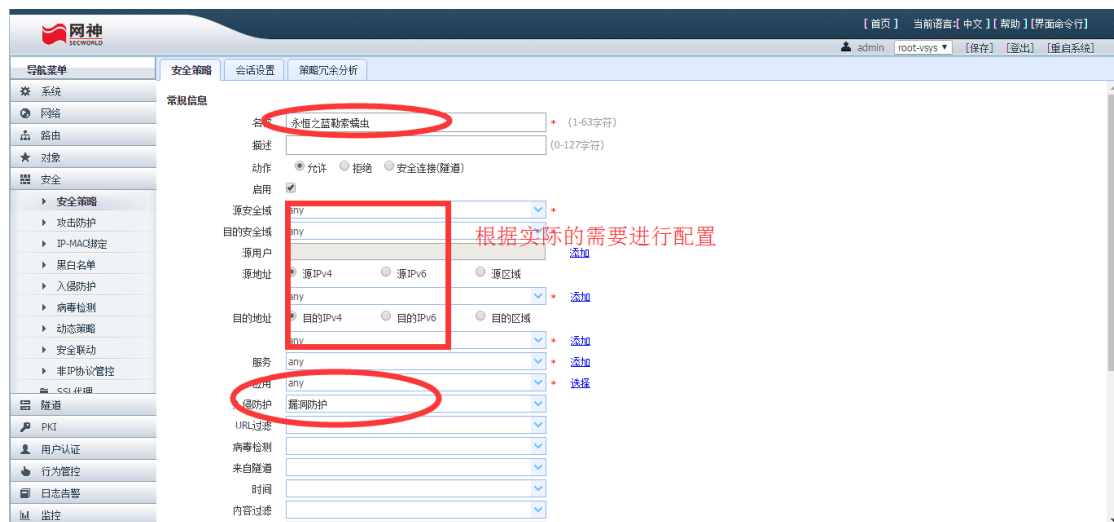
1. 登录防火墙管理界面，进入“系统配置->升级->库升级”确认特征库版本，应确保 IPS 特征库需升级到 20170513，应用识别特征库升级到 20170513；

批量启用自动升级 批量禁用自动升级 批量立即升级						
	名称	当前版本	最新版本	升级服务有效期	自动升级	操作
1	IPS特征库	170513	170504	2017-05-21 16:16:43	✓	⚙️
2	应用识别库	170513	170428	2017-05-21 16:16:43	✓	⚙️
3	AV特征库	170420	170406	2017-05-21 16:16:43	✓	⚙️

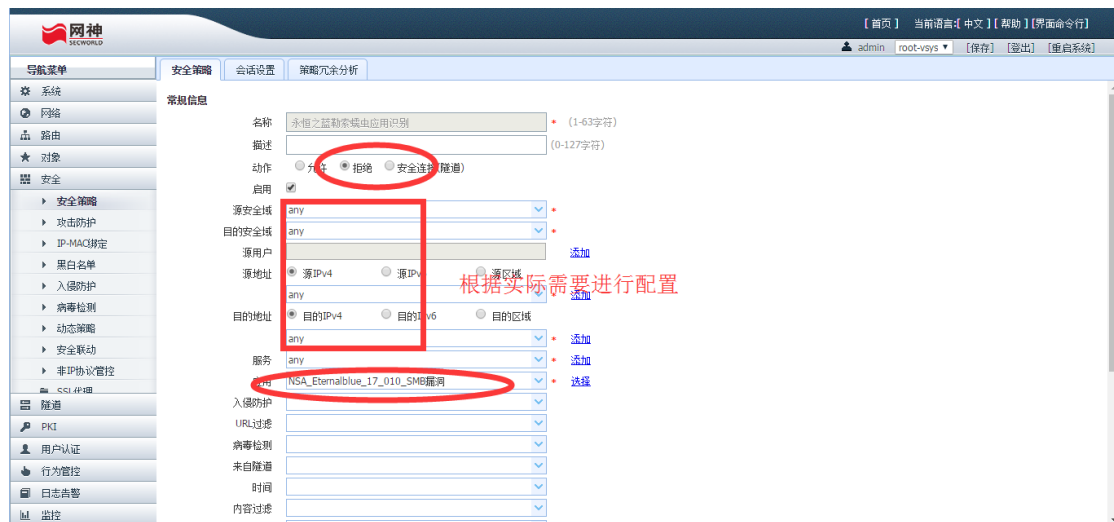
2. 进入“安全->入侵防护”，添加一个入侵防护配置实例；



3. 新建一条安全策略，在“漏洞防护”中选择步骤 2 中新建的漏洞防护实例，点击确定完成新建；



4. 在策略列表中选择步骤 3 新建的策略，点击“调序”，并将该策略调整至第一位；
5. 新建另外一条安全策略，在“应用”中选择“NSA_Eternalblue_17_010_SMB”，“动作”选择“拒绝”；



6. 在策略列表中选择步骤 5 新建的策略，点击“调序”，并将该策略调整至第一位。

3.3 通过诱导方式

通过域名欺骗方式，把恶意软件访问的域名 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com，欺骗到一个存活的 http 服务器后，该样本就不会进行文档加密，而是自动退出。

诱导方式防火墙配置

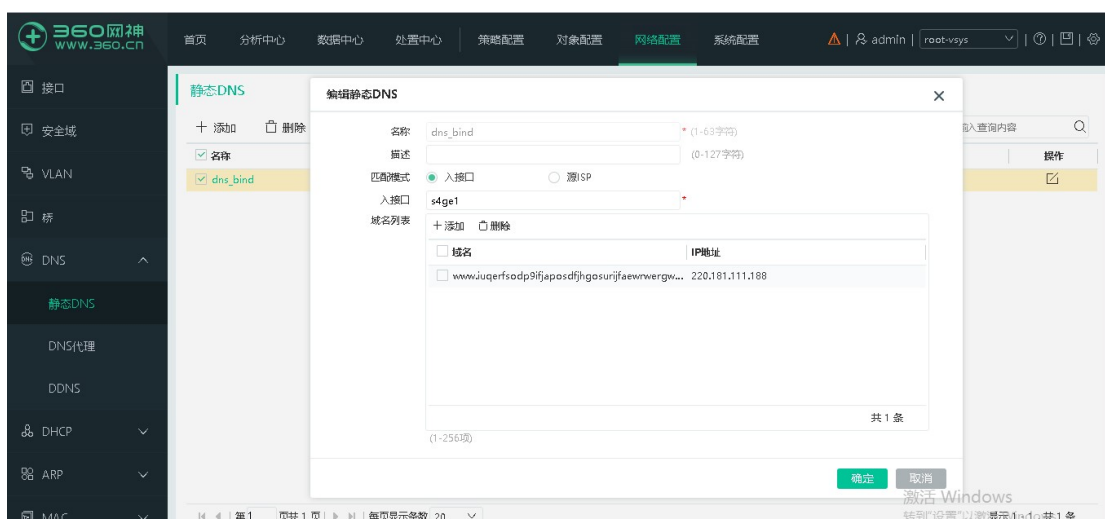
这种方式 360 智慧防火墙和极速防火墙的配置相同，该场景必须满足如下条件：

- 1、windows 主机的网络访问必须经过防火墙；
- 2、windows 主机的 dns 解析必须经过防火墙；
- 3、必须有一个存活的 http 服务器（可以是公网的 web 服务器）；

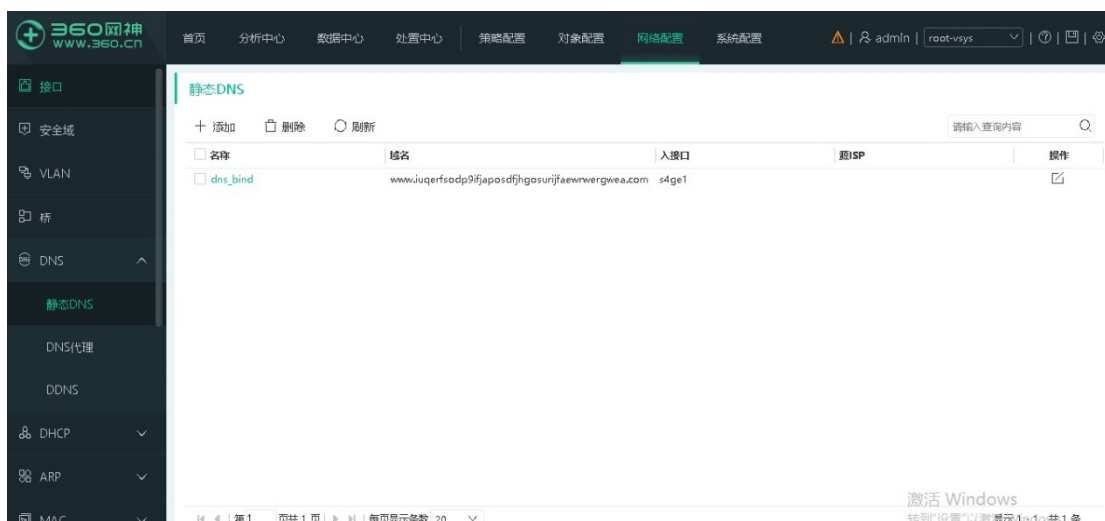
防火墙配置如下：

打开网络配置->DNS->静态 dns

- 1、把域名 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 添加进去，对应的 ip 地址选择一个存活的 http 服务器，同时如接口选择连接 windows 测的网络接口。



2、点击确定即可



通过这种域名欺骗的方式可以使勒索软件不再进行恶意加密，而是自动退出。

3.4 新一代智慧防火墙“处置中心”隔离中招主机配置方法

针对已中招主机，为防止内部扩散，可通过新一代智慧防火墙“处置中心”功能对其执行快速的网络隔离操作。

1. 登录防火墙管理界面，进入“处理中心->人工处置”，点击“+添加”；



- 按照下图设置,添加一条处置策略,“源地址” 填为已确定的中招主机 IP 地址,“动作” 选择“阻断”;

源地址请根据实际地址进行配置

- 确认处置策略下发成功。

