

360 防火墙针对“永恒之蓝”蠕虫病毒攻击的防护方案

1 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，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。

WanaCry!勒索软件除了通过 ms17-010 的 SMBv1 传播,还会通过曾经被安装过 NSA DoublePulsar 后门的渠道进行传播,这样,即使打了 ms17-010 补丁,但是在打补丁前曾经被 EternalBlue 攻击并成功安装过 DoublePulsar 后门的机器,也可能被该勒索软件感染.

2 南北侧防护

2.1 通过 IPS 特征阻断

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。

2.2 通过应用识别特征阻断

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，通过更新应用识别特征库已经完成了蠕虫变种的识别，建议用户尽快将应用识别特征库升级至“20170513”版本。

2.3 禁用 445 服务

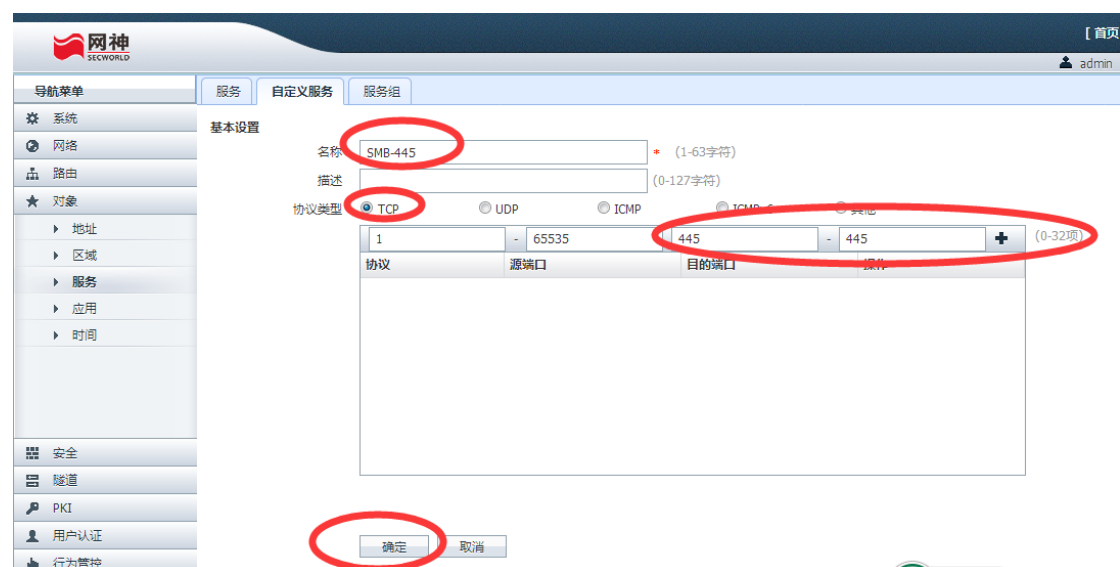
2.3.1 极速防火墙方案

2.3.1.1 安全策略

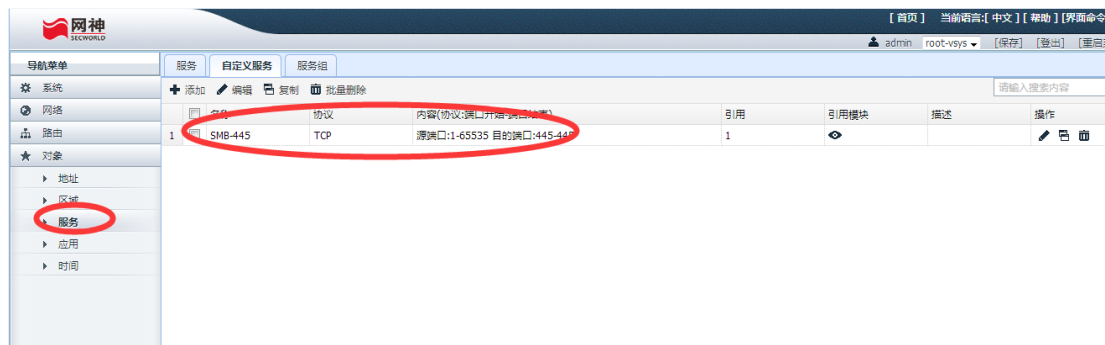
1. 登录防火墙管理界面，进入对象配置->服务->自定义服务，点击添加。



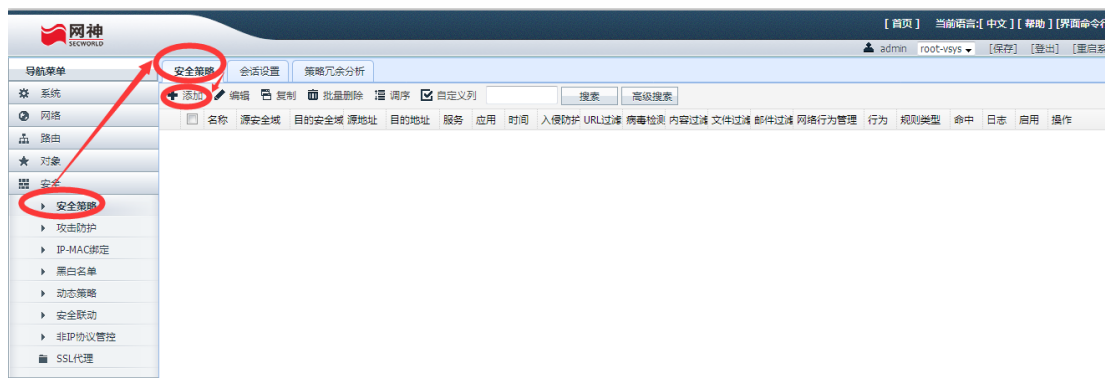
2. 添加自定义服务



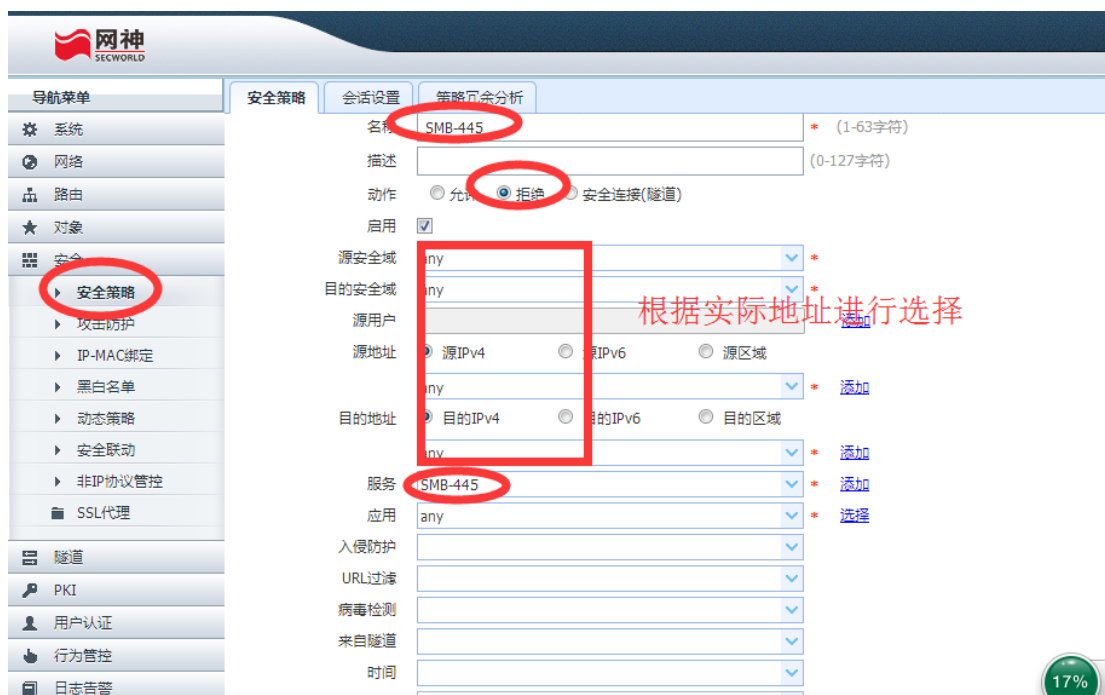
3. 确认自定义服务



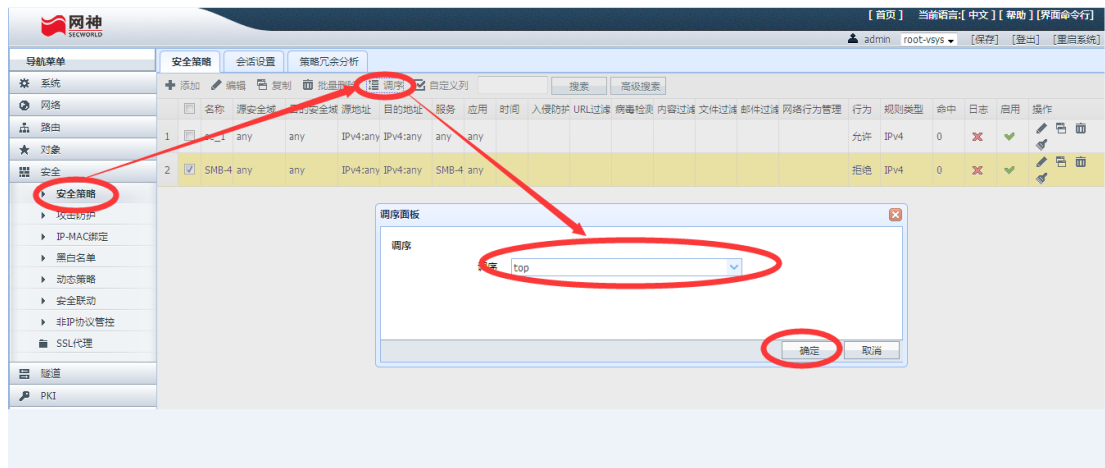
4. 点击策略管理->安全策略，点击添加。



5. 安全策略添加



6. 安全策略调序



7. 确认安全策略添加成功，并且添加的记录已经调序到**第一个**。



2.3.2 智慧防火墙方案 (NSG3000/5000/7000/9000 系列产品)

2.3.2.1 一键处置

1. 登录防火墙管理界面，进入处理中心->人工处置，点击添加。



2. 添加处置策略

添加处置

处置类型

网络连接

地址类型

☒ IPv4 ☐ IPv6

源地址

any

源端口

any

(1-65535)

目的地址

any

目的端口

445

(1-65535)

协议

any

处置动作

阻断

处置时间

永久

确定

取消

3. 确认处置策略添加成功

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-vsyz

失陷主机 风险主机 人工处置

未处置: 0 已处置: 1 已忽略: 0 总威胁: 1

+ 添加

删除

刷新

全部状态

请输入查询内容

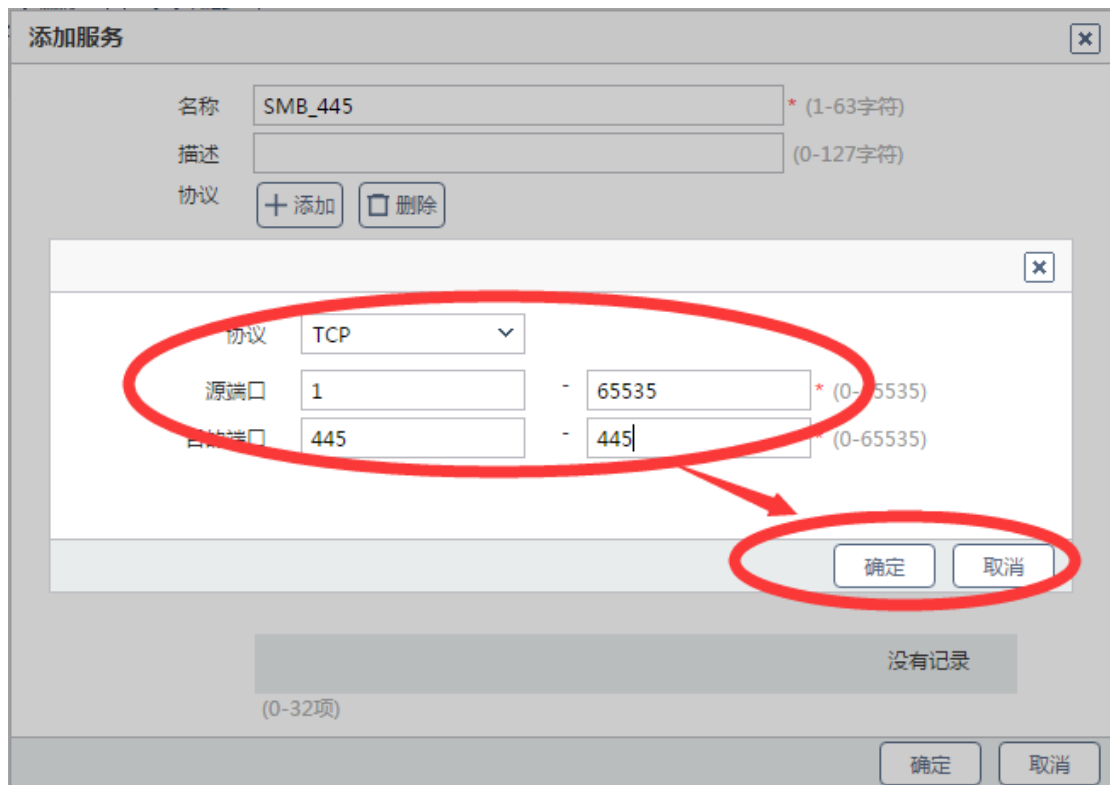
源信息	目的信息	来源	创建时间	生效时间	失效时间	命中数	状态	操作
any	445	本地	2017-05-13 06:18:07	2017-05-13 06:18:07	-	5861	已处置	<div>眼 方 三</div>

2.3.2.2 安全策略

8. 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。



9. 添加自定义服务



10. 确认自定义服务



11. 点击策略管理->安全策略，点击添加。



12. 安全策略添加

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

确定 取消

根据实际业务进行选择

13. 安全策略调序

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-vsyz

安全策略

安全策略 冗余策略

+ 添加 复制 删除 调序 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

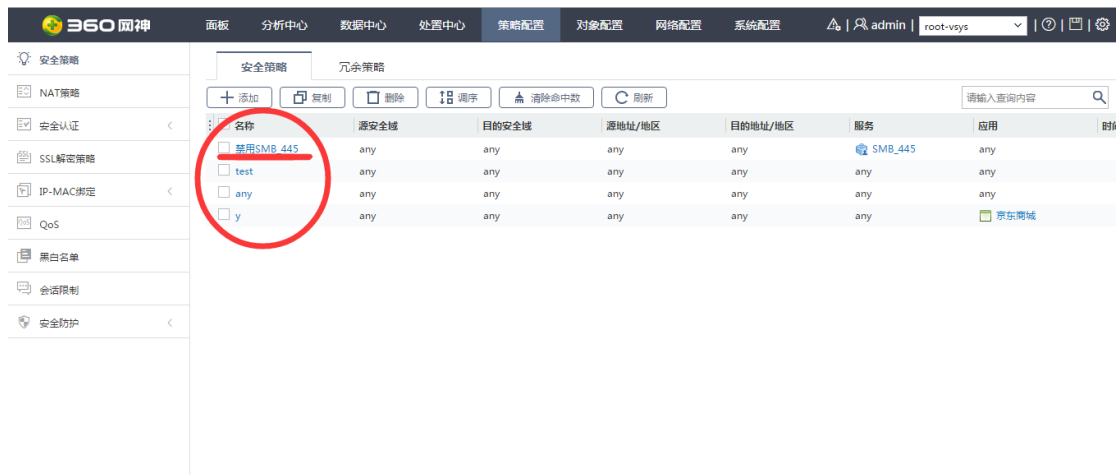
<input type="checkbox"/> test	any	any	any	any	any	any	
<input type="checkbox"/> any	any	any	any	any	any	any	
<input type="checkbox"/> y	any	any	any	any	any	京东商城	
<input checked="" type="checkbox"/> 禁用SMB_445	any	any	any	any	SMB_445	any	

调序

策略 top

确定 取消

14. 确认安全策略添加成功，并且添加的记录已经调序到**第一个**。



3 东西侧防护

针对东西侧已经部署防火墙的网络，可以通过 IPS、应用识别以及禁用 445 服务的手段进行处理，详细处理方案参见南北侧防护方案。

4 已感染设备处理

如果已经有感染的设备，为了防止内部扩散，可以通过智慧防火墙进行快速网络隔离，把已感染设备从网络中隔离开。操作截图如下。

1. 登录防火墙管理界面，进入处理中心->人工处置，点击添加。



2. 添加处置策略

添加处置

处置类型

网络连接

地址类型

☒ IPv4

☐ IPv6

源地址

192.168.1.10

源端口

any

目的地址

any

目的端口

any

(1-65535)

协议

any

处置动作

阻断

处置时间

永久

确定

取消

源地址请根据实际地址进行配置

3. 确认设备已经隔离成功

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-vsyz

失陷主机

风险主机

人工处置

未处置：0

已处置：1

已忽略：0

总威胁：1

+ 添加

删除

刷新

全部状态

请输入查询内容

<input type="checkbox"/> 源信息	目的信息	来源	创建时间	生效时间	失效时间	命中数	状态	操作
<div>192.168.1.10</div>	any	本地	2017-05-13 07:12:16	2017-05-13 07:12:16	-	0	已处置	<div><div></div><div></div><div></div></div>