

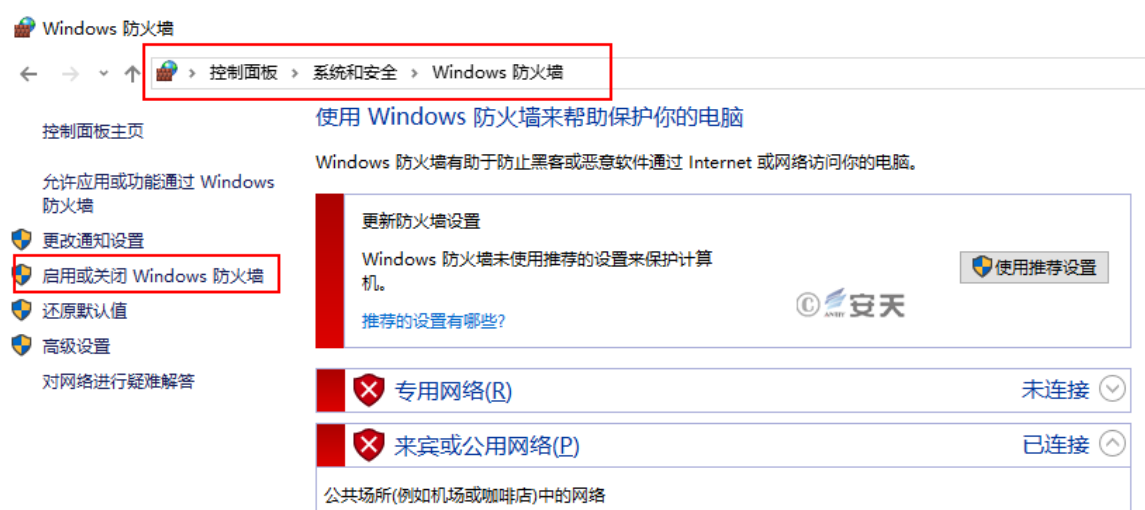
# 应对新型电脑勒索软件的临时解决方案

安天安全研究与应急处理中心

1. 开启系统防火墙
2. 利用系统防火墙高级设置阻止向 445 端口进行连接（该操作会影响使用 445 端口的服务）
3. 打开系统自动更新，并检测更新进行安装

## Win7、Win8、Win10 的处理流程

打开控制面板-系统与安全-Windows 防火墙，点击左侧启动或关闭 Windows 防火墙



选择启动防火墙，并点击确定

## 自定义各类网络的设置

你可以修改使用的每种类型的网络的防火墙设置。

### 专用网络设置

- 启用 Windows 防火墙
  - 阻止所有传入连接，包括位于允许应用列表中的应用
  - Windows 防火墙阻止新应用时通知我
- 关闭 Windows 防火墙(不推荐)

### 公用网络设置

- 启用 Windows 防火墙
  - 阻止所有传入连接，包括位于允许应用列表中的应用
  - Windows 防火墙阻止新应用时通知我
- 关闭 Windows 防火墙(不推荐)



确定

取消

## 点击高级设置

### Windows 防火墙

控制面板 > 系统和安全 > Windows 防火墙

控制面板主页

允许应用或功能通过 Windows 防火墙

更改通知设置

启用或关闭 Windows 防火墙

还原默认值

高级设置

对网络进行疑难解答

### 使用 Windows 防火墙来帮助保护你的电脑

Windows 防火墙有助于防止黑客或恶意软件通过 Internet 或网络访问你的电脑。

专用网络(R)

来宾或公用网络(P)

公共场所(例如机场或咖啡店)中的网络

Windows 防火墙状态: 启用  
传入连接: 阻止所有与未在允许应用  
活动的公用网络: 网络  
通知状态: Windows 防火墙阻止新

## 点击入站规则，新建规则

高级安全 Windows 防火墙

文件(F) 操作(A) 查看(V) 帮助(H)

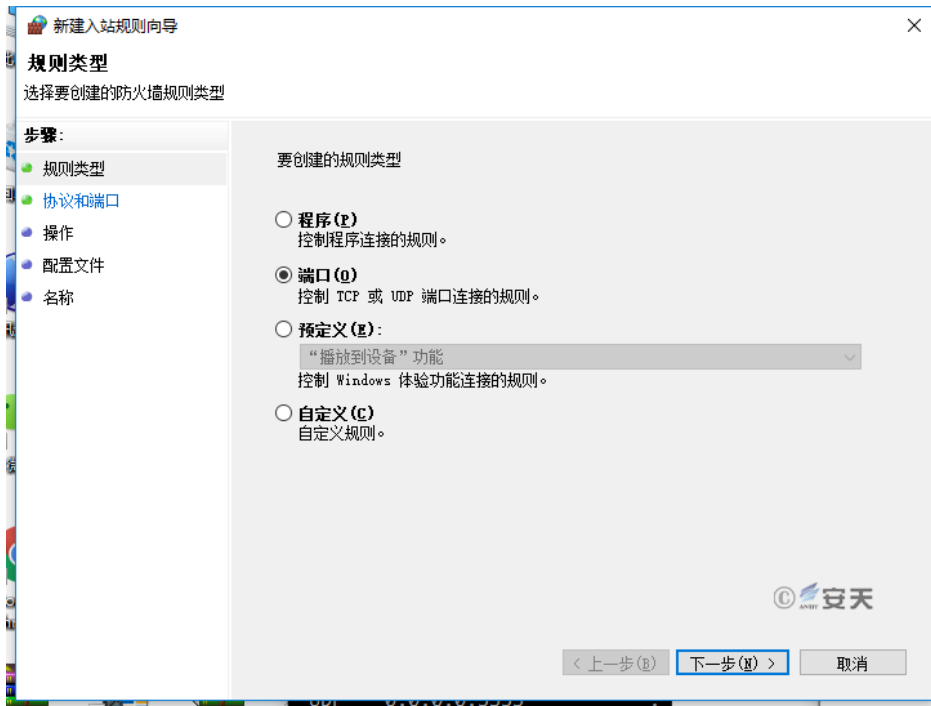
本地计算机上的高级安全 Windows 防火墙

名称	组	配置文件
aaapt		公用
aaapt		所有
aaapt		公用
aaapt		公用
aaapt		所有
aaapt		公用
aaapt		公用
aaapt		公用

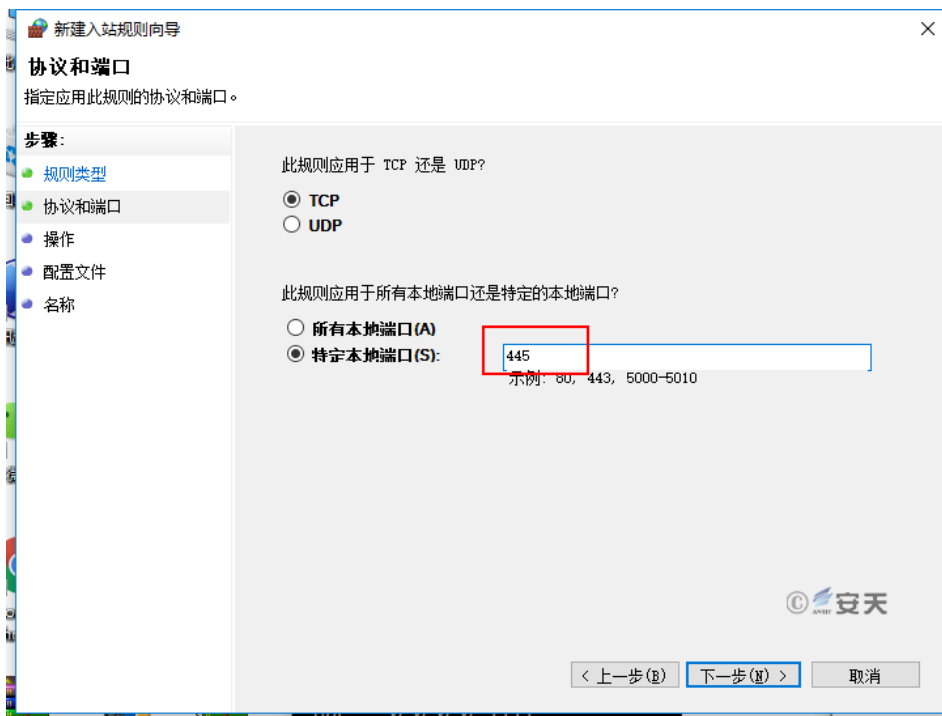
操作

- 入站规则
- 新建规则...
- 按配置文件筛选
- 按状态筛选
- 按组筛选
- 查看
- 刷新

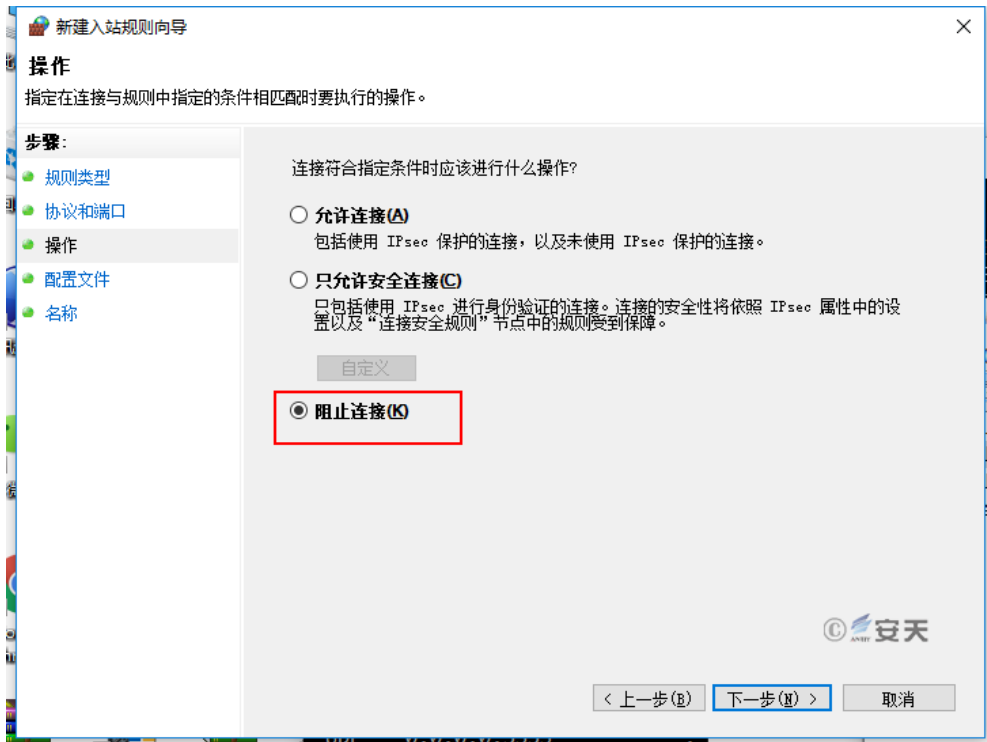
## 选择端口、下一步



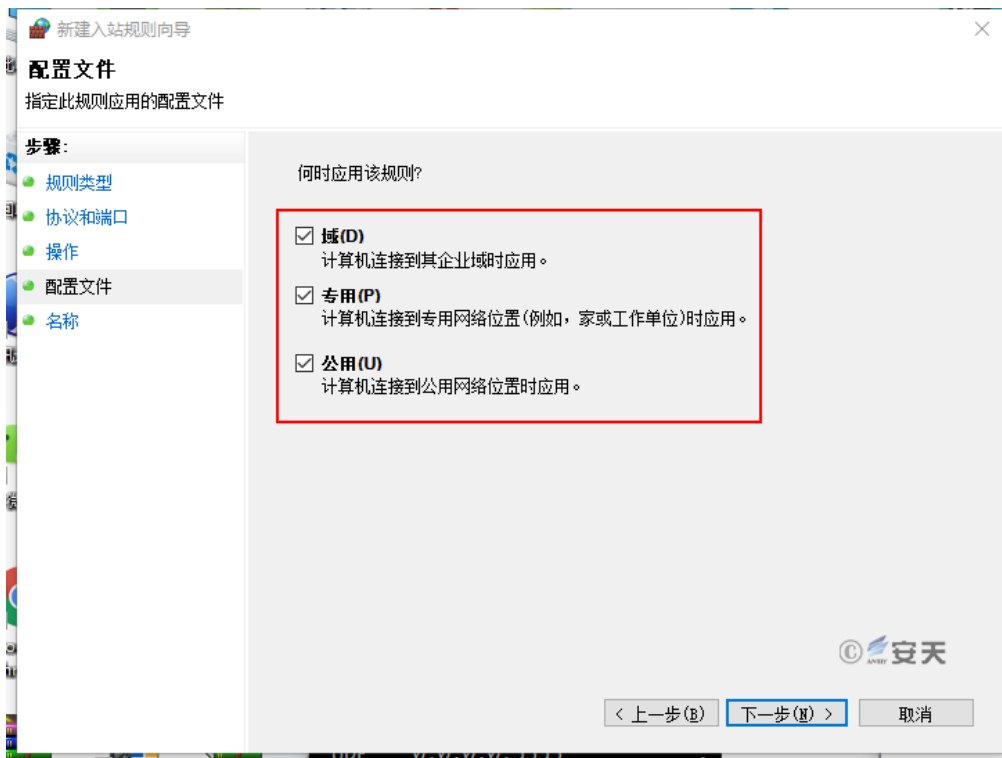
特定本地端口，输入 445，下一步



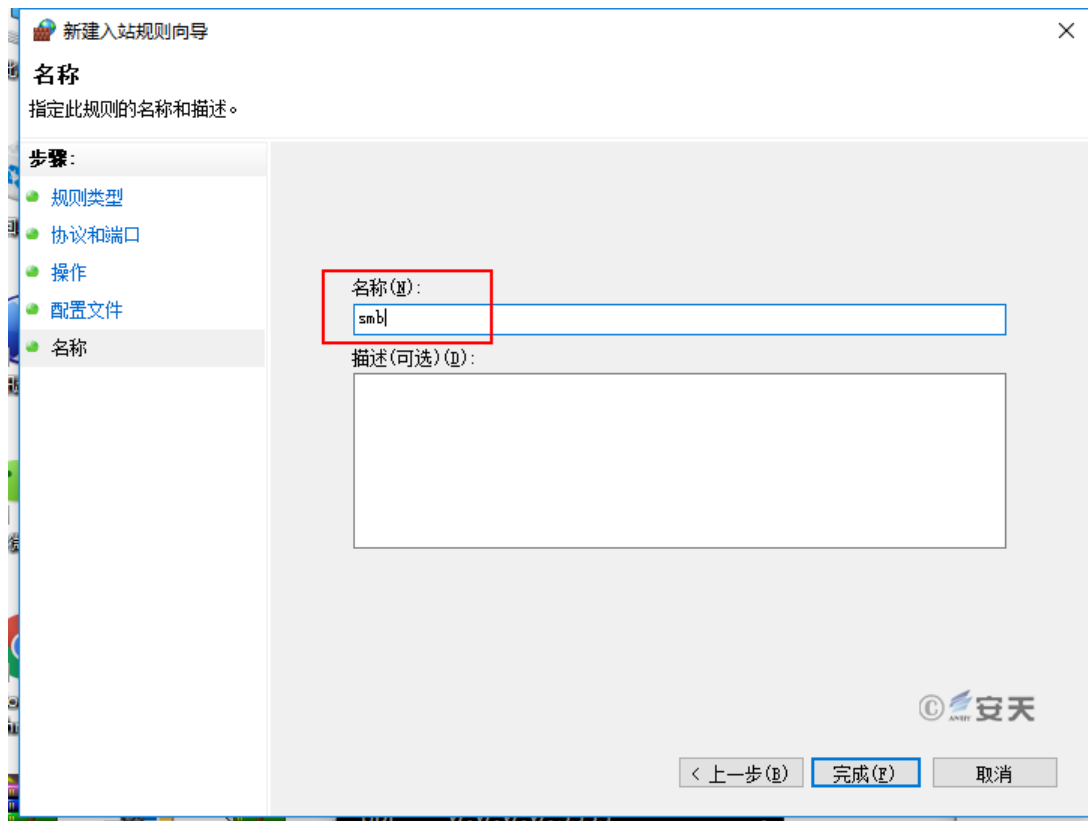
选择阻止连接，下一步



配置文件，全选，下一步



名称，可以任意输入，完成即可。



## XP 系统的处理流程

依次打开控制面板，安全中心，Windows 防火墙，选择启用



点击开始，运行，输入 cmd，确定执行下面三条命令

```
net stop rdr  
net stop srv  
net stop netbt
```

由于微软已经不再为 XP 系统提供系统更新，建议用户尽快升级到高版本系统。

版权所有：安天安全研究与应急处理中心