Appendix 1
Solve the Connection Issue to ThingsBoard on Windows

明玉瑞 Yurui Ming

yrming@gmail.com

声明
Disclaimer

- 本讲义在准备过程中由于时间所限，所用材料来源并未规范标示引用来源。所引材料仅用于教学所用，作者无意侵犯原著者之知识版权，所引材料之知识版权均归原著者所有；若原著者介意之，请联系作者更正及删除。

  The time limit during the preparation of these slides incurs the situation that not all the sources of the used materials (texts or images) are properly referenced or clearly manifested. However, all materials in these slides are solely for teaching and the author is with no intention to infringe the copyright bestowed on the original authors or manufacturers. All credits go to corresponding IP holders. Please address the author for any concern for remedy including deletion.

问题
Problem

- 有读者反映，当在服务器或教师机上安装ThingsBoard之后，从其他机器连接ThingsBoard，连接超时。本附录主要讲该问题的解决。
- 注意，连接超时不同于连接拒绝。连接拒绝表明可能没有启动ThingsBoard服务。可以从命令行执行如下命令验证服务是否启动：

  net start | findstr /i thingsboard

- 原则上，执行完上述命令，需要列出与如下类似结果：

```
C:\Users\Lenovo>net start | findstr /i thingsboard
   ThingsBoard Server Application
```

- 如果没有列出任何结果，则需要首先以管理员权限启动服务：

  net start thingsboard

```
C:\Windows\system32>net start thingsboard
请求的服务已经启动。
```

问题
Problem

- 当连接超时，首先要检查确保创建了相应的入站规则，可以从命令行执行如下命令验证：

  netsh advfirewall firewall show rule name=all | findstr /N 8080

- 原则上，执行完上述命令，需要列出与如下类似结果；如果没有列出任何结果，则需要按下面步骤创建规则。

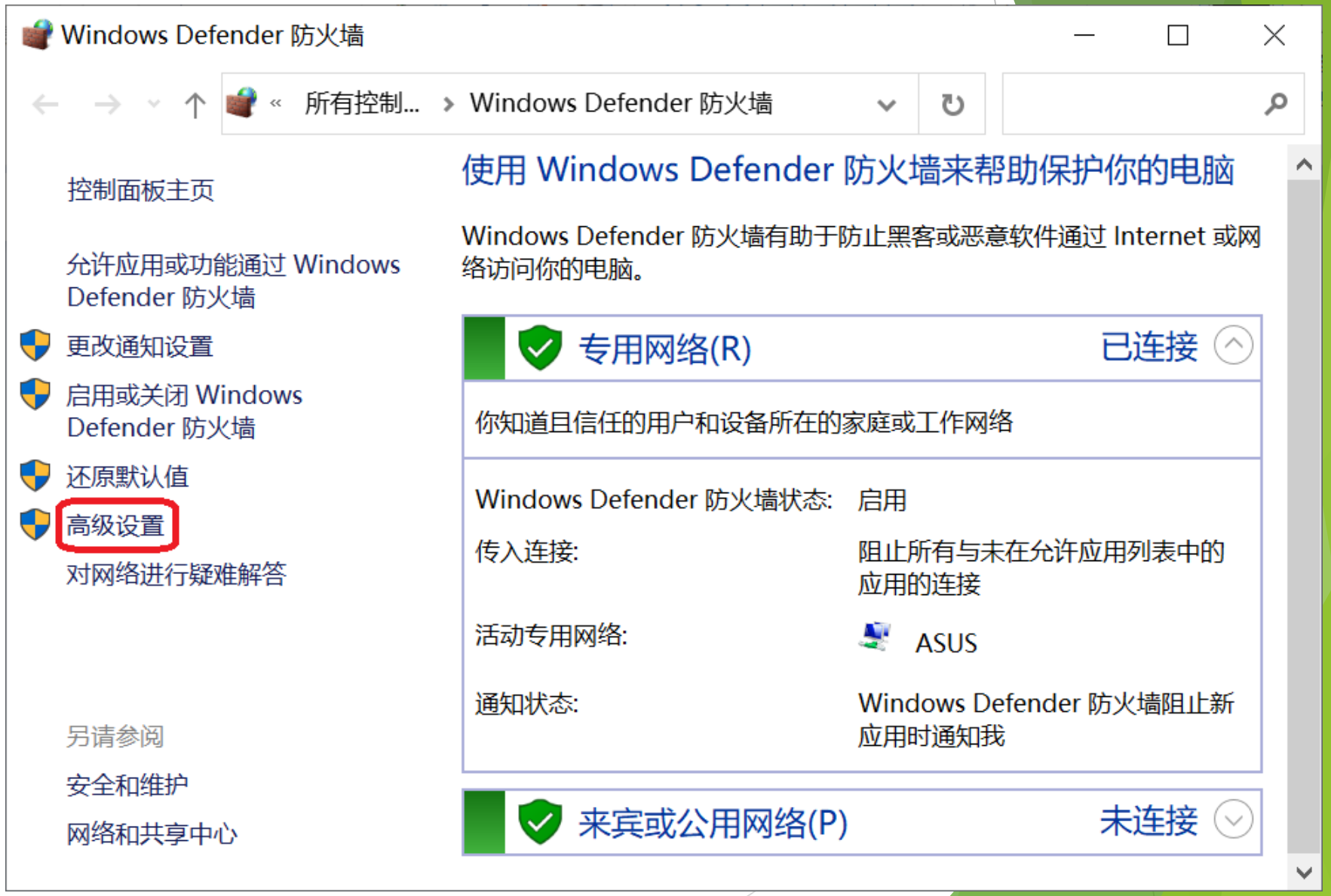
```
C:\Users\Lenovo\Desktop\物联网建设>netsh advfirewall firewall show rule name=all | findstr /N 8080
147:本地端口:                             8080,1883,5683
431:本地端口:                             8080
```

- 注意，如果有多个服务侦听例如8080端口的情况，可以将所有规则拷贝到剪贴板上，然后粘贴到记事本时，逐条分析：

  netsh advfirewall firewall show rule name=all | clip

方案
Solution

- 执行 firewall.cpl，打开 Windows 防火墙，然后选择高级设置。

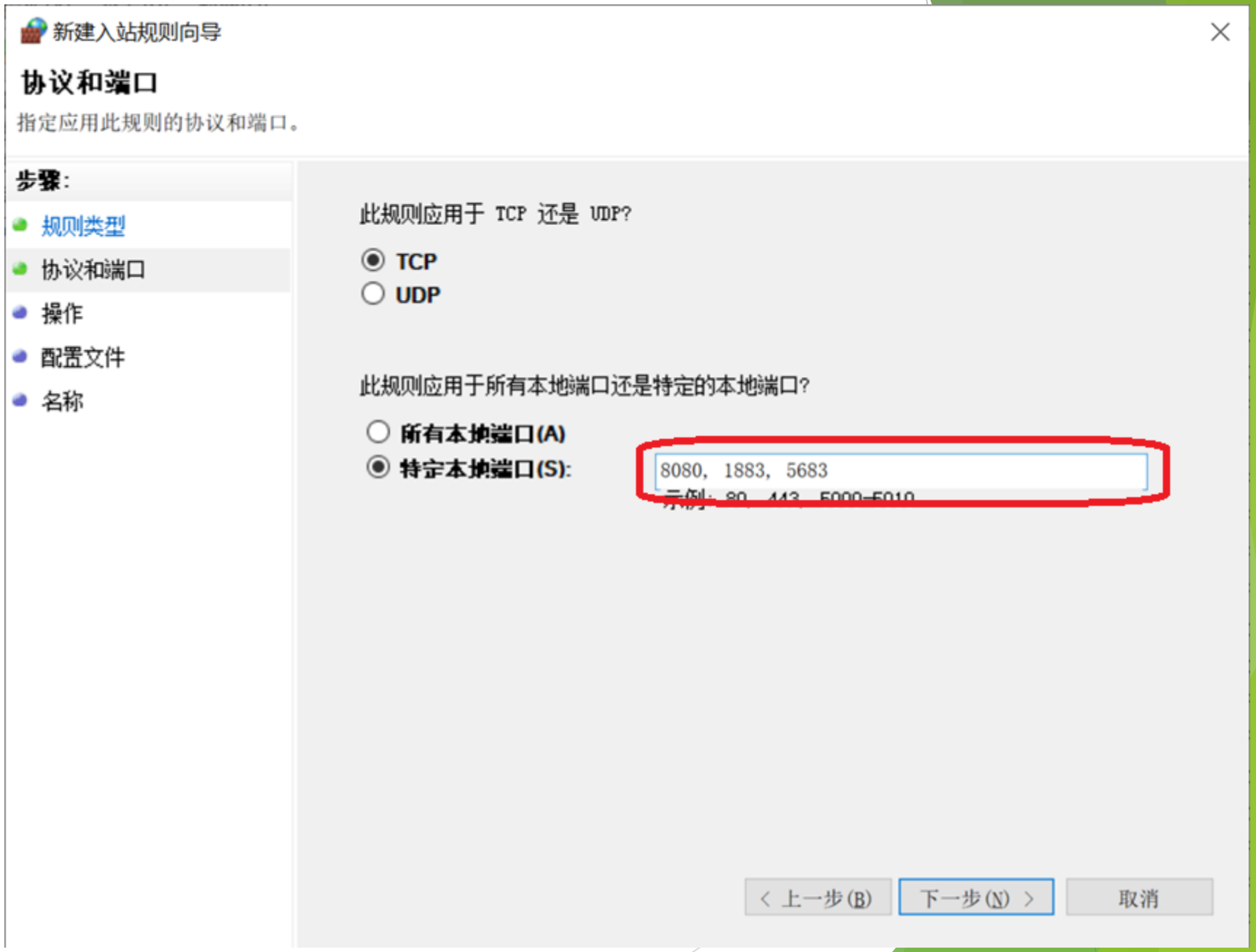


方案
Solution

- 在左侧面板中点击入站规则，然后在右侧操作面板中点击新建规则。

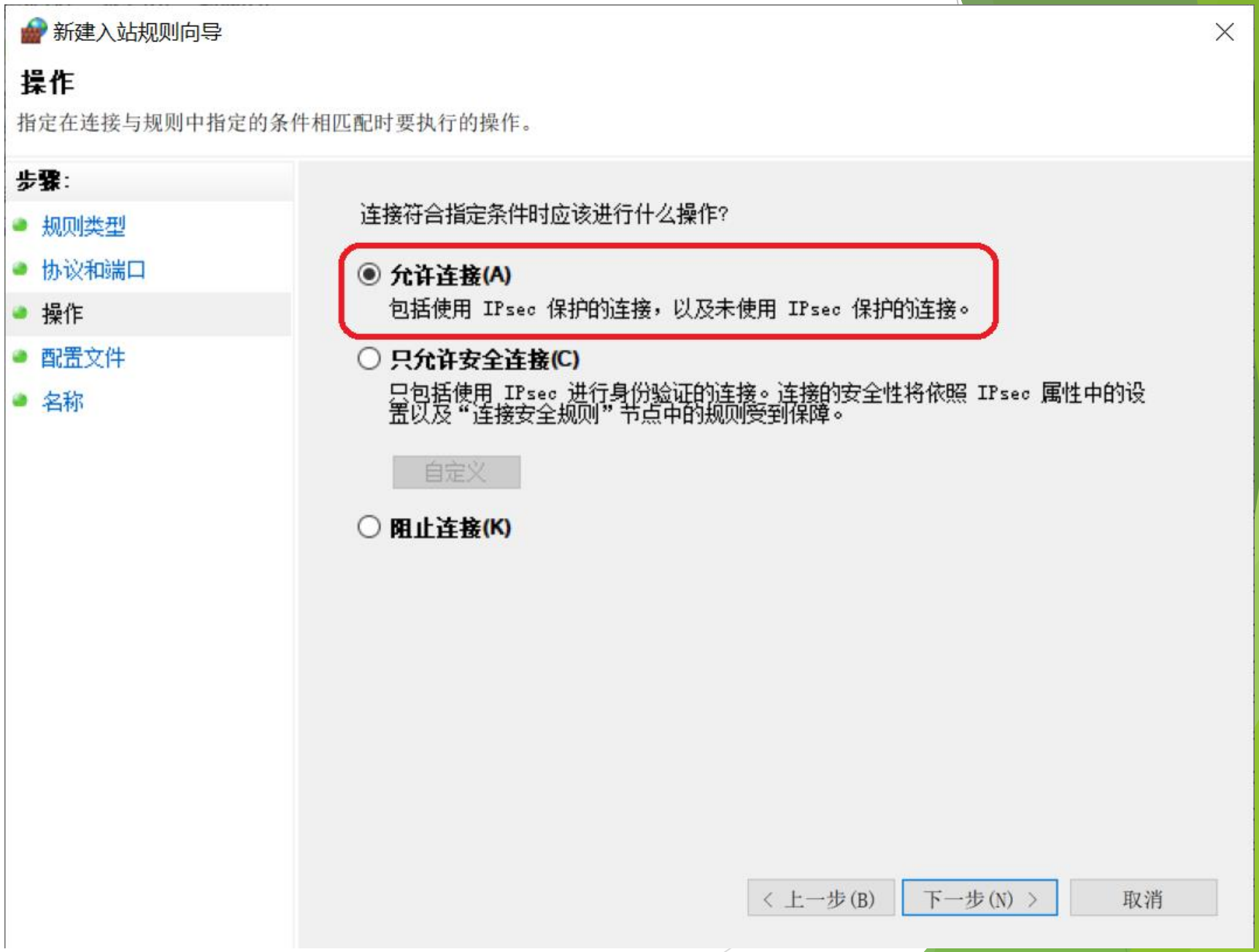
方案
Solution

- 将需要放行的端口都填上，然后点击下一步：



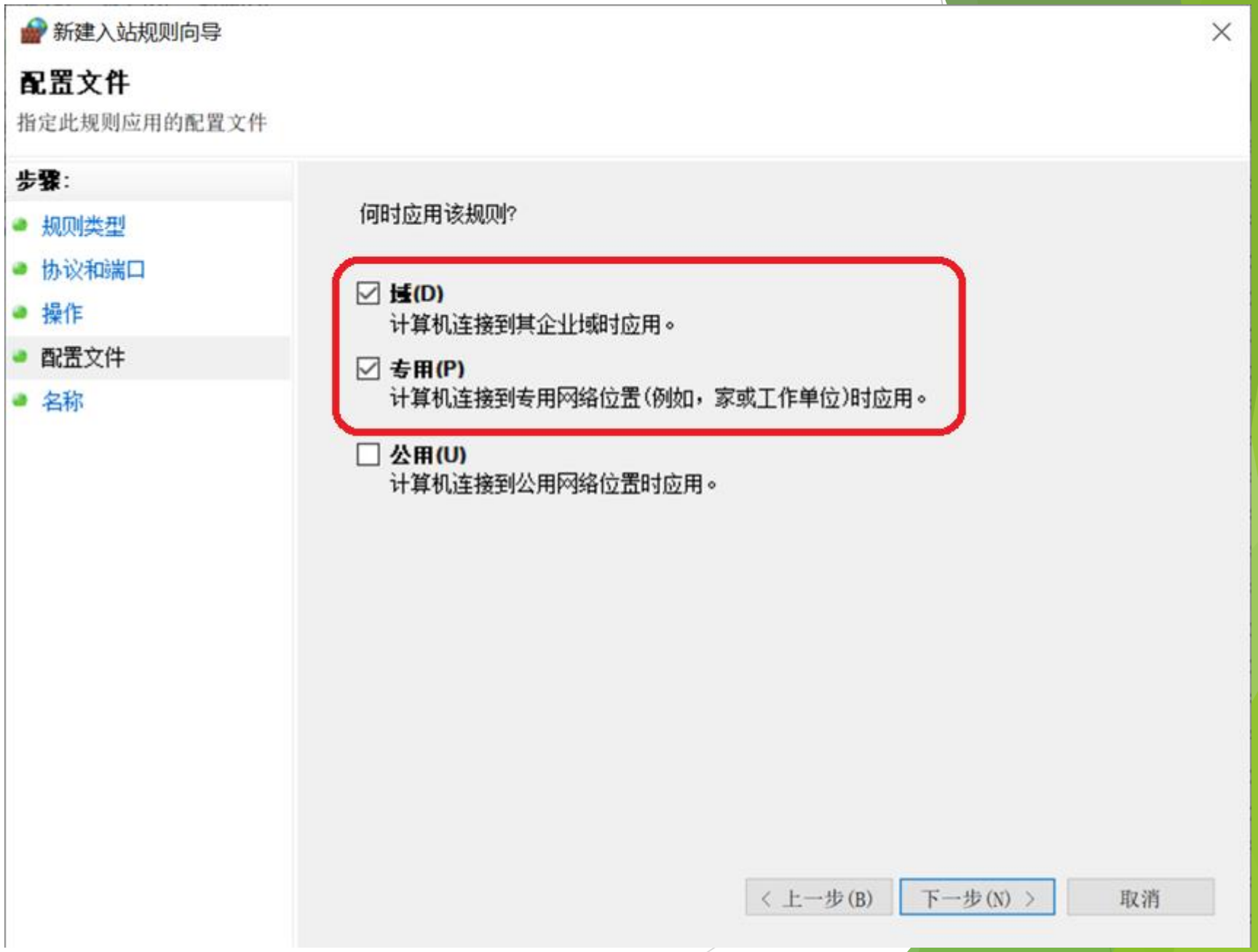
方案
Solution

- 操作选择允许连接，然后点击下一步：



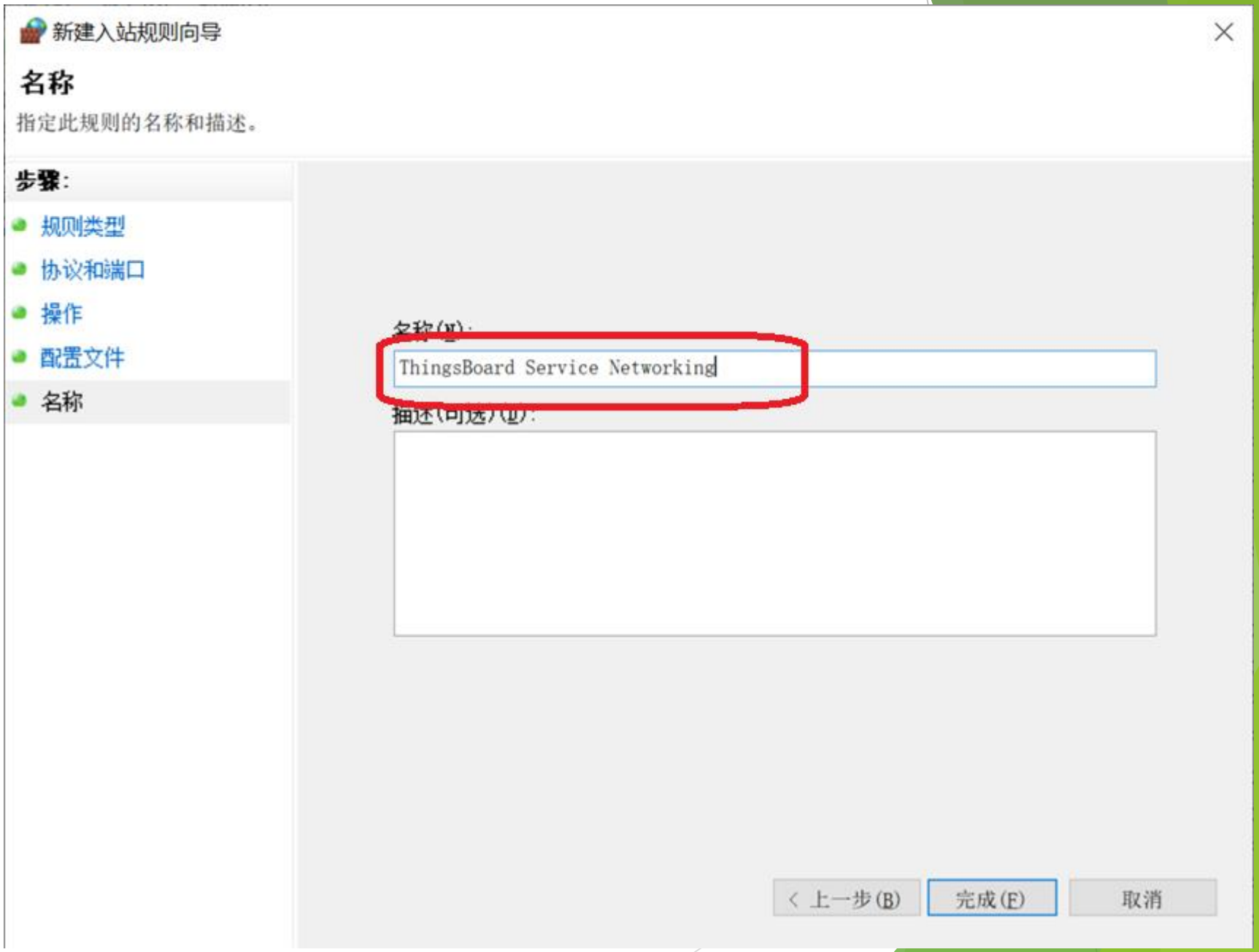
方案
Solution

- 视情况做适当勾选：



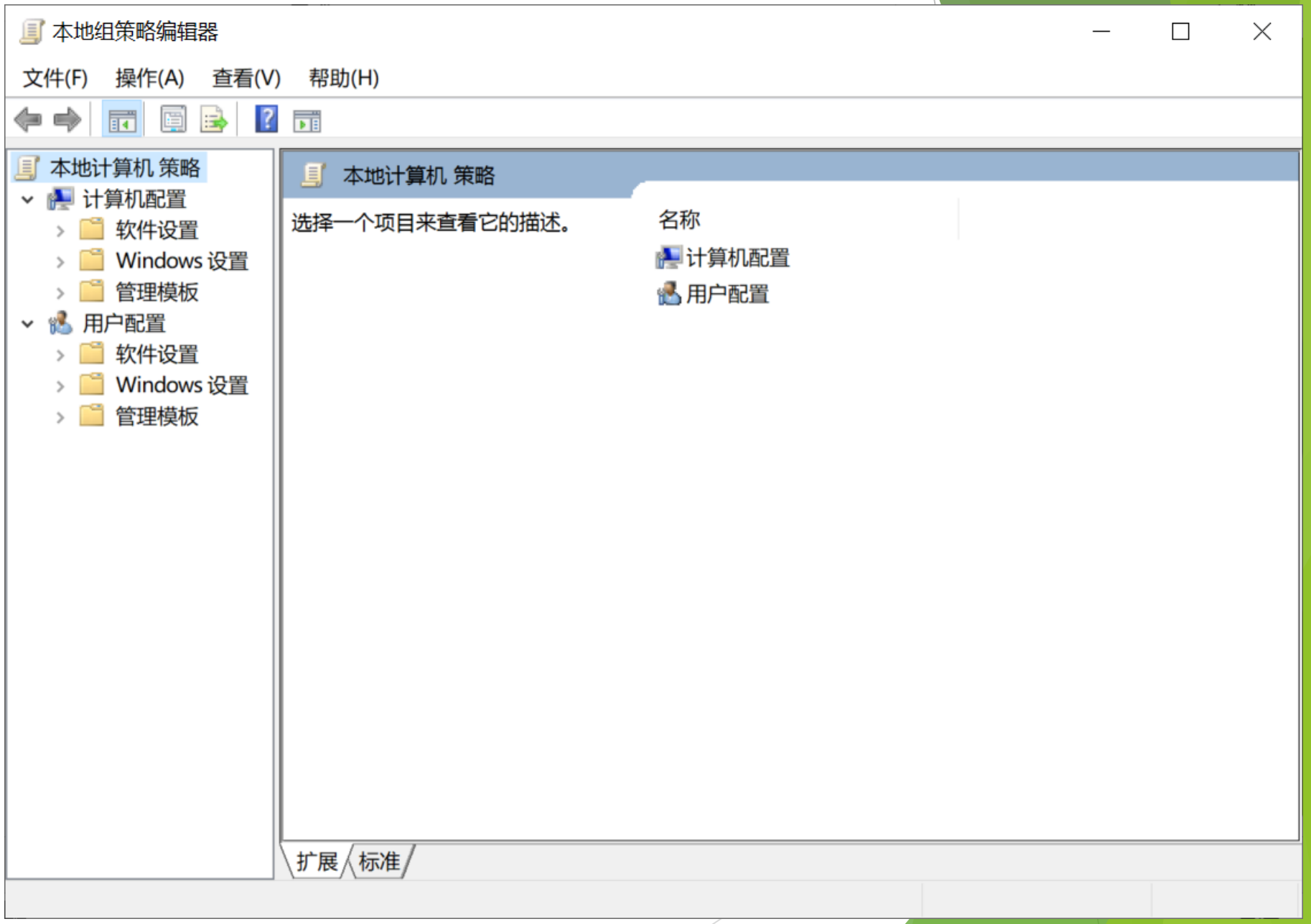
方案
Solution

- 输入名称点击完成：



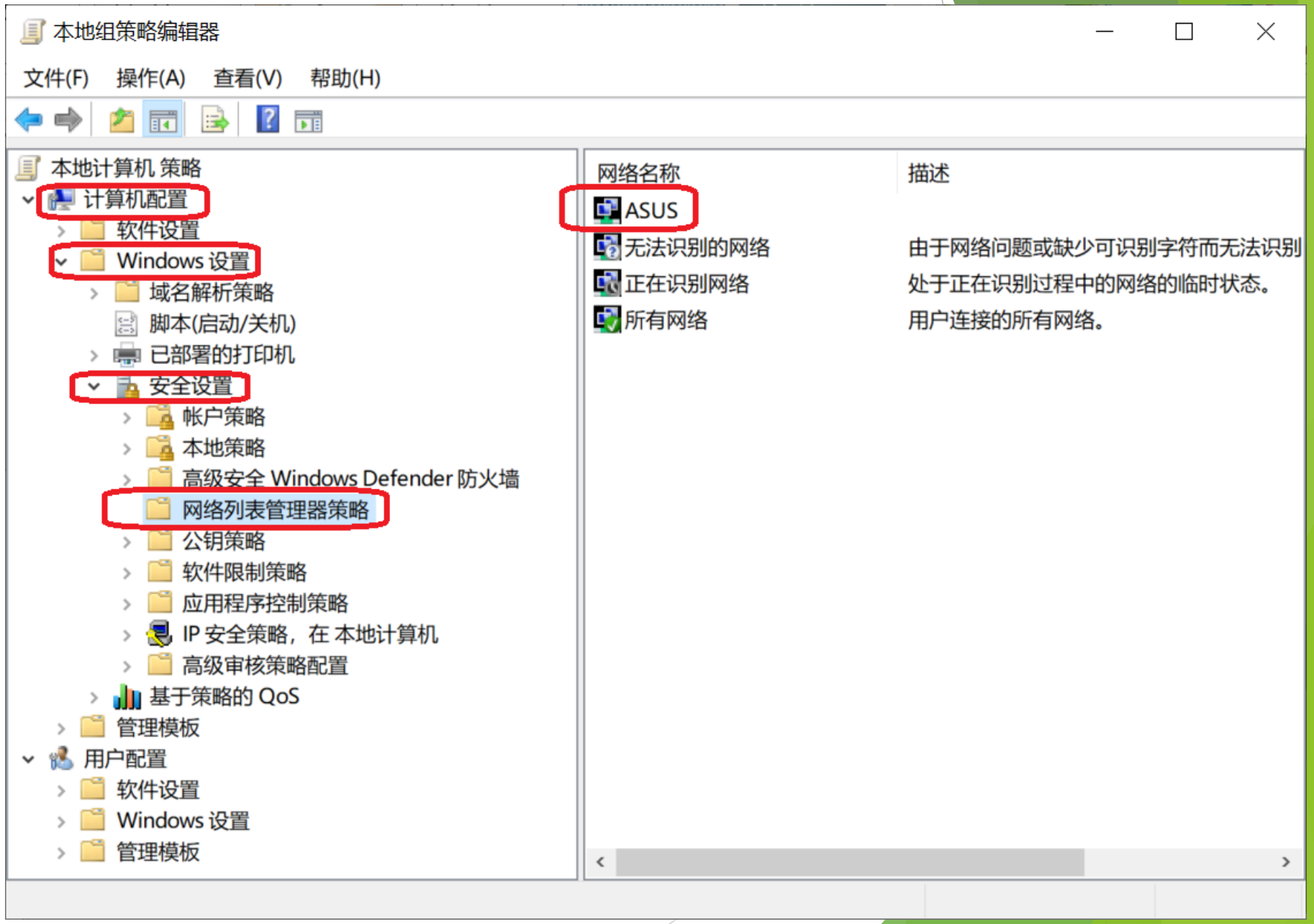
方案
Solution

- 如果在完成上述步骤后，从其他机器连接ThingsBoard，依然连接超时时，则需要将服务器或教学机所在的网络加入专用网络。
- 执行gpedit.msc，打开组策略编辑器：



方案
Solution

- 在左侧树形控件中，导航到网络列表管理器策略，从右侧网络名称列表选择当前所在的局域网络，如作者的服务器所在的网络为ASUS：



方案
Solution

- 双击ASUS，打开属性标签页。然后在网络位置标签页中，将位置类型改为专用：

方案
Solution

- 操作系统使用防火墙配置文件按照连接性、连接数和类别来识别并记录与它们连接的每个网络。在Windows防火墙的高级安全选项中有三种网络位置类型：域、专用、公用。
- 防火墙的域、专用、公用的网络位置类型区别如下：
  - 域：Windows 可以验证对计算机所联接域的域控制器的访问。
  - 专用：由用户或应用程序标识为专用的网络。 只应将可信网络标识为专用网络。 用户很可能希望将家庭网络或小型企业网络标识为专用网络。
  - 公用：除域网络之外，其他所有网络最初都归为公共网络一类。 直接连到 Internet 的网络或者位于公共场所（如机场和咖啡店）的网络应保留为公共网络。
- 对于未分配的情况，则按公用处理。

问题
Problem

- 有读者反映，当在完成上述步骤后，从其他机器连接ThingsBoard，依然连接超时。这时候，需要知道是否有优先级高于允许规则的阻止规则存在。

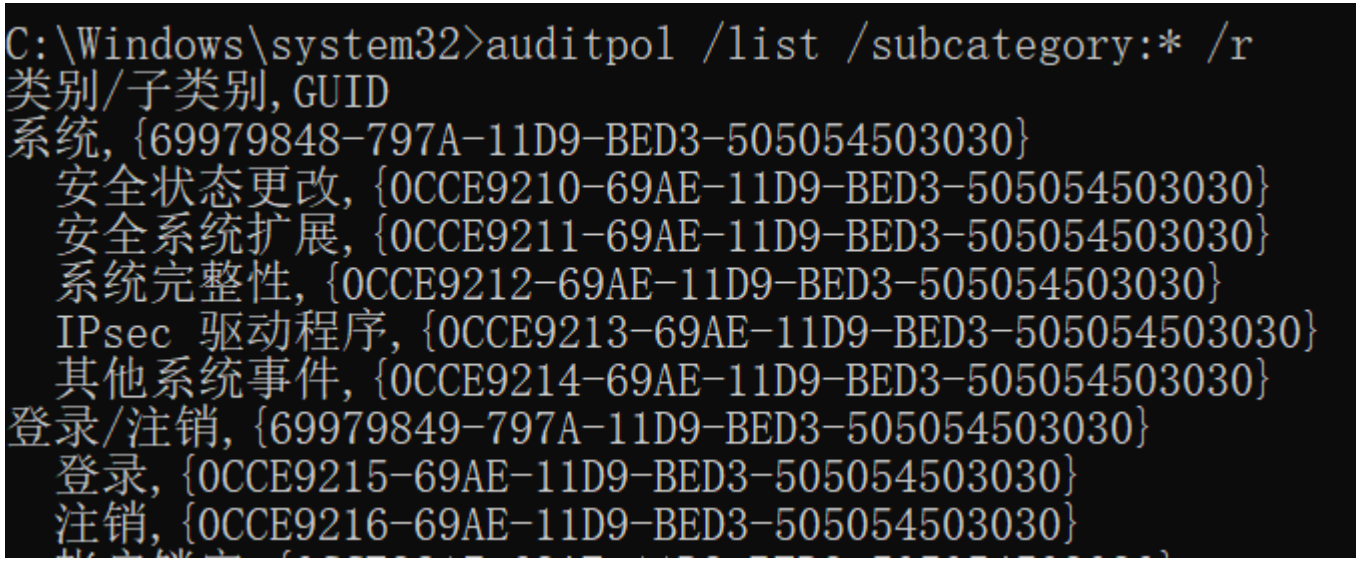
- 在进一步诊断之前，需要引入一些概念。Windows 10中的防火墙是基于Windows筛选平台 (WFP)的。WFP使独立软件供应商(ISV)能够筛选和修改TCP/IP 数据包、监视或授权连接、筛选受 Internet 协议安全性 (IPsec) 保护的通信以及远程过程调用 (RPC)。
- 注意WFP不是防火墙。它是一组系统服务及用户模式和内核模式API，基于它能够开发防火墙和其他监视连接或处理数据包的软件。

- 而审核筛选平台连接决定操作系统在Windows筛选平台允许或阻止连接时是否生成审核事件。此子类别包含有关阻止和允许的连接、阻止和允许的端口绑定、阻止和允许的端口侦听操作以及阻止接受传入连接应用程序的Windows筛选平台事件。

方案
Solution

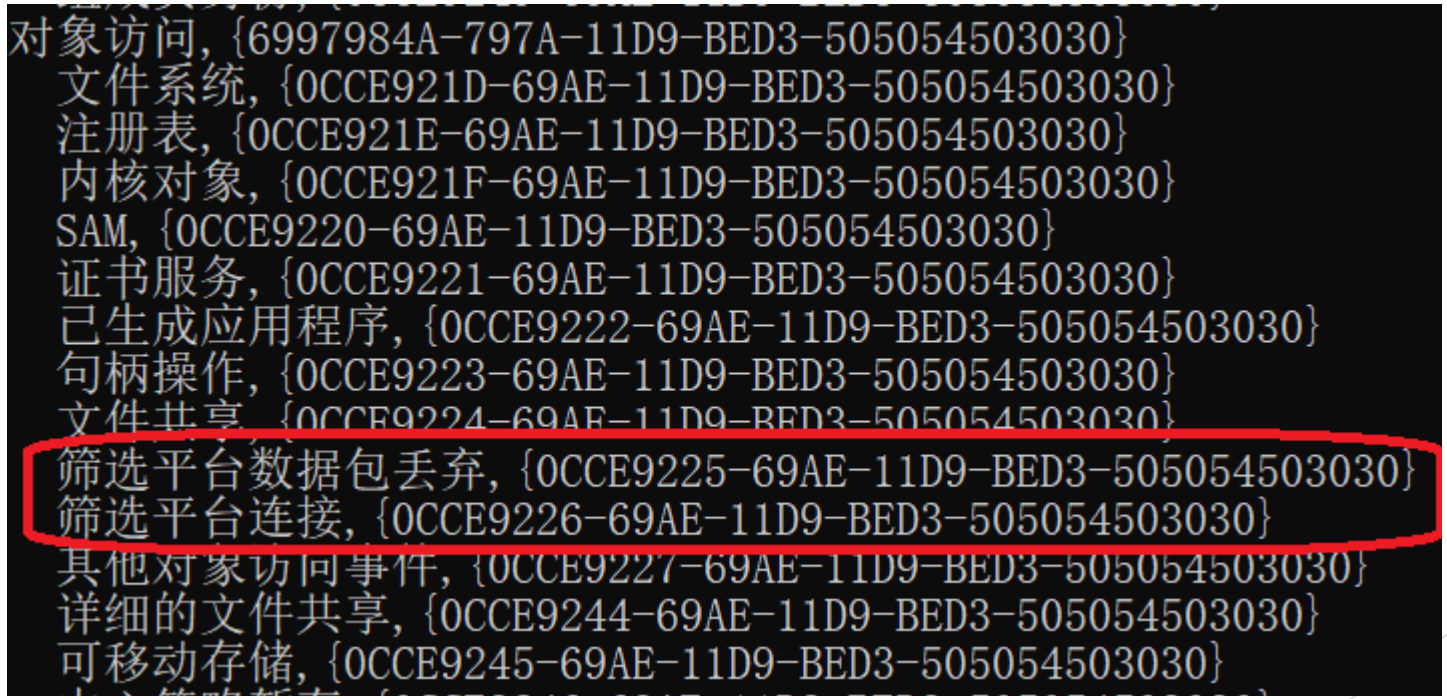
- 首先，以管理员身份启动命令行，枚举可供审核的子类别：

  auditpol /list /subcategory:* /r



方案
Solution

- 我们重点关注两个子类别：



方案
Solution

- 启动这两个子类别的审核：

  auditpol /set /subcategory:{0CCE9225-69AE-11D9-BED3-505054503030} /failure:enable

  auditpol /set /subcategory:{0CCE9226-69AE-11D9-BED3-505054503030} /failure:enable

```
C:\Windows\system32>auditpol /set /subcategory:{0CCE9225-69AE-11D9-BED3-505054503030}  /failure:enable
命令成功执行。

C:\Windows\system32>auditpol /set /subcategory:{0CCE9226-69AE-11D9-BED3-505054503030}  /failure:enable
命令成功执行。
```

方案
Solution

- 生成审核文件，由于会在当前文件夹下生成，因此可以先切换到合适的目录：

  cd some-location-in-your-computer

  netsh wfp show state

```
C:\Windows\system32>cd C:\Users\Lenovo\Desktop\物联网建设

C:\Users\Lenovo\Desktop\物联网建设>netsh wfp show state
数据收集成功；输出 = wfpstate.xml
```

方案
Solution

- 为不影响性能，在生成审核文件候，及时关闭相关子类别的审核：

  auditpol /set /subcategory:{0CCE9225-69AE-11D9-BED3-505054503030} /failure:disable

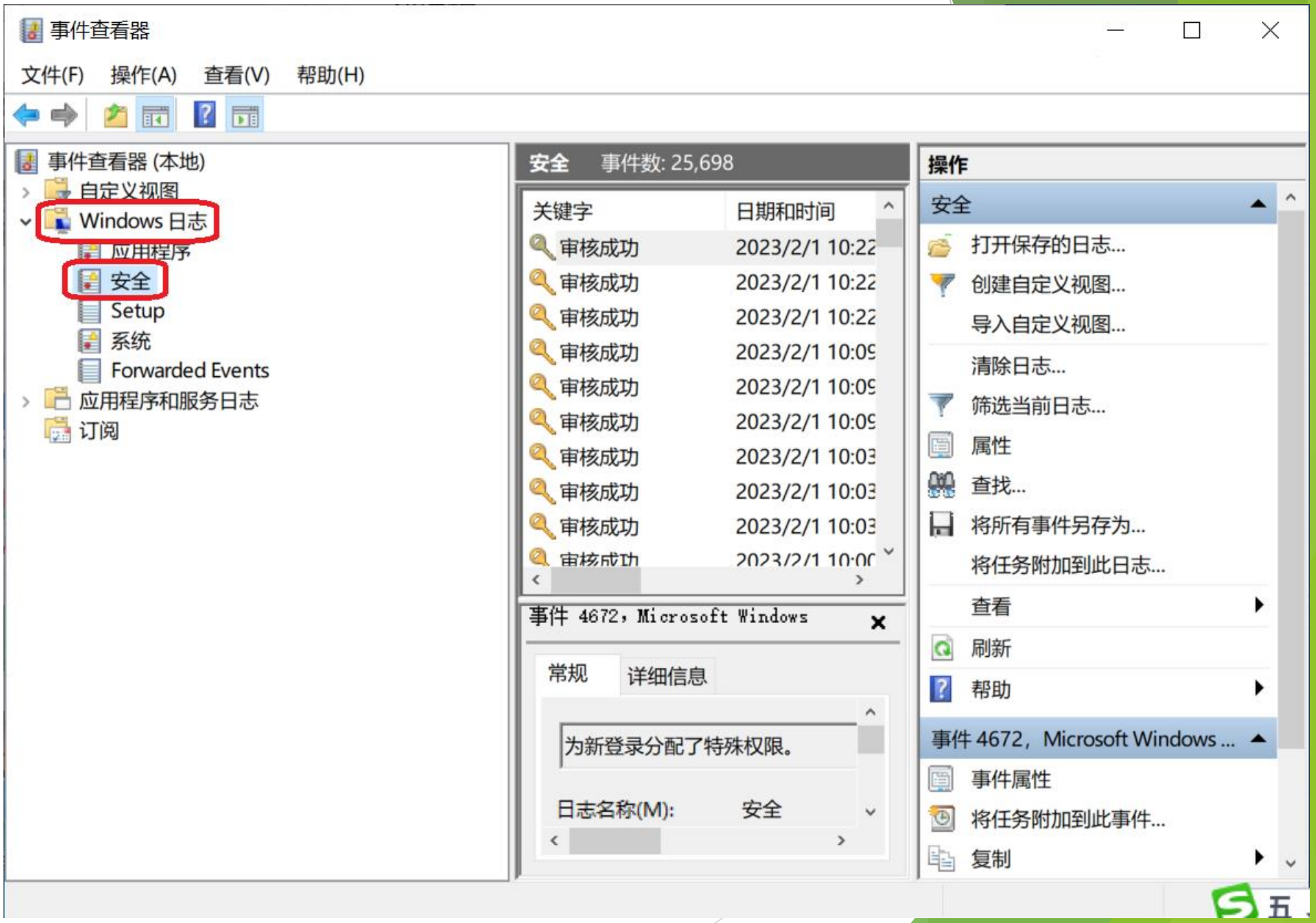
  auditpol /set /subcategory:{0CCE9226-69AE-11D9-BED3-505054503030} /failure:disable

```
C:\Users\Lenovo\Desktop\物联网建设>auditpol /set /subcategory:{0CCE9225-69AE-11D9-BED3-505054503030} /failure:disable
命令成功执行。

C:\Users\Lenovo\Desktop\物联网建设>auditpol /set /subcategory:{0CCE9226-69AE-11D9-BED3-505054503030} /failure:disable
命令成功执行。
```

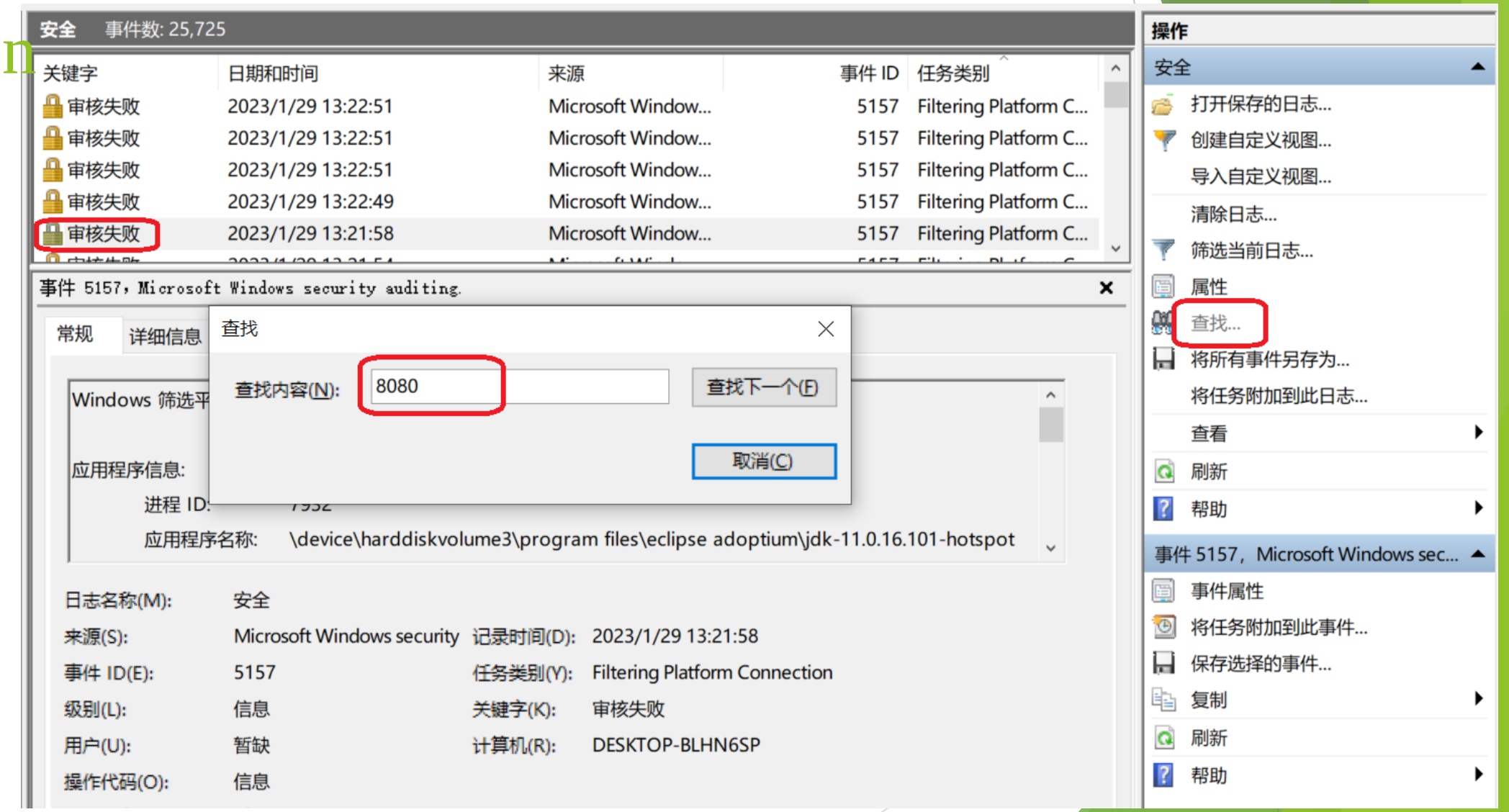
方案
Solution

- 运行eventvwr.msc，打开事件查看器，转到Windows日志，安全子类别：



方案 Solution

- 通过查找特定的信息，如目标端口号，将相应的审核失败的条目找出来。
- 从日志记录里面，基本可以确定问题的源头：



方案
Solution

- 如有必要，可以根据日志条目的时间戳，打开生成的xml文件，一般名称为wfpstate.xml，根据更为详细的信息，进行一步查找相关原因。
- 基本通过上述步骤，能将原因找出来。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<wfpstate>
    <timeStamp>2023-01-29T05:22:38.570Z</timeStamp>
    <sessions numItems="12">
        <item>
            <sessionKey>{e3ea8478-0fb7-43fc-858c-c6e448af3bb8}</sessionKey>
            <displayData>
                <name/>
                <description/>
            </displayData>
            <flags/>
            <txnWaitTimeoutInMSec>6000000</txnWaitTimeoutInMSec>
            <processId>1284</processId>
            <sid>S-1-5-20</sid>
            <username>NT AUTHORITY\NETWORK SERVICE</username>
            <kernelMode>false</kernelMode>
        </item>
        <item>
            <sessionKey>{05bc41c2-50c8-4c6c-badd-35f01b3de747}</sessionKey>
            <displayData>
```