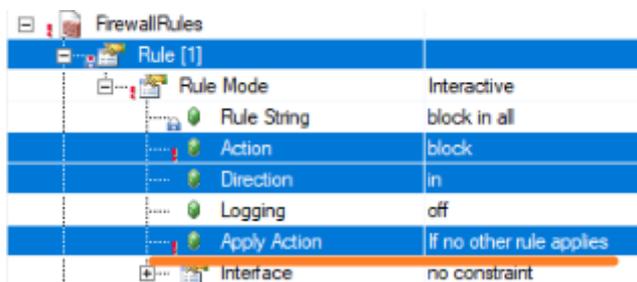


## 背景知识

- [023贝加莱操作系统支持防火墙功能吗](#)
- [024如何在Automation Studio中配置防火墙](#)

## 配置基本规则

- 添加 Firewall rule 时需要注意:
  - 对于同一规则
    - 如果先放行, 那么后续再添加的阻挡策略就不会生效;
    - 反之, 如果先阻挡, 那么后续的放行就不会生效。
  - 如果希望对同一规则下增加例外
    - Apply Action 设置为 If no other rule applies



- 防火墙功能在仿真模式下, 相关功能会存在异常, 因此建议在硬件 PLC 上测试。

## 检查 PLC 上开放端口方式

- 端口扫描工具
  - <https://www.advanced-port-scanner.com/cn/>
- 默认情况下开启 ModbusTCP Slave 功能的 PLC 开放的端口

◦ **10.86.13.250**

**状态:** 确定  
**操作系统:**  
**IP:** 10.86.13.250  
**MAC:** 00:60:65:5F:38:52  
**制造商:** BERNECKER RAINER INDUSTRIE-ELEKTRONIC GmbH  
**NetBIOS:**  
**用户:**  
**类型:**  
**日期:** 2094-01-31 10:56:59 UTC±00:00  
**备注:**

服务	详情
Port 80 (TCP)	
Port 111 (TCP)	rpcbind
Port 502 (TCP)	

# 案例一：只允许指定 IP 访问 PLC

## 配置方式

- 只允许 IP 为 10.86.13.249 的设备访问

FirewallRules		Rule [3]	
Rule [1]		Rule Mode	Interactive
Rule Mode	Interactive	Rule String	pass in quick from 10.86.13.249/32 to me
Rule String	block in all	Action	pass
Action	block	Direction	in
Direction	in	Logging	off
Logging	off	Apply Action	Immediately
Apply Action	If no other rule applies	Interface	no constraint
Interface	no constraint	Internet Protocol	no constraint
Internet Protocol	no constraint	Response	off
Response	off	Source Address	must match
Source Address	no constraint	IP Address	10.86.13.249
Destination Address	no constraint	Netmask (CIDR)	32
Group	none	Destination Address	me
Rule [2]		Group	none
Rule Mode	Interactive	Rule Mode	Interactive
Rule String	block out all	Rule String	pass out quick from me to 10.86.13.249/32
Action	block	Action	pass
Direction	out	Direction	out
Logging	off	Logging	off
Apply Action	If no other rule applies	Apply Action	Immediately
Interface	no constraint	Interface	no constraint
Internet Protocol	no constraint	Internet Protocol	no constraint
Response	off	Response	off
Source Address	no constraint	Source Address	me
Destination Address	no constraint	Destination Address	must match
Group	none	IP Address	10.86.13.249
		Netmask (CIDR)	32
		Group	none

## 实现效果

- PC 的 IP 地址为 10.86.13.249 可以访问

- IP settings

IP assignment: Manual

IPv4 address: 10.86.13.249

IPv4 subnet prefix length: 24

IPv4 gateway: 10.86.13.1

Edit
- | Target type description | IP Address   | Subnet Mask   | Host name     | AR Version | Serial Number |
|-------------------------|--------------|---------------|---------------|------------|---------------|
| 5APC2200.AL18...        | 10.86.13.252 | 255.255.255.0 | br-automation | H04.73     | F0AC0168586   |
| X20CP1585               | 10.86.13.250 | 255.255.255.0 | br-automation | H04.73     | C3AE0206887   |

ANSL: tcpip/COMT=2500 /DAIP=10.86.13.250 /REPO=11159 /ANSL=1 /PT=11169 X20CP1585 H4.73 RUN

- PC 的 IP 地址为 10.86.13.248 不可以访问

- 

Target type description	IP Address	Subnet Mask	Host name	AR Version	Serial Number
54PC2200.AL18-...	10.86.13.252	255.255.255.0	br-automation	H04.73	F0AC0168586
X20CP1585	10.86.13.250	255.255.255.0	br-automation	H04.73	C3AE0206887

无法访问

tcpip/COMT=2500 /DAIP=10.86.13.250 /REPO=11159 /ANSL=1 /PT=11169 OFFLINE

## 案例二: PLC 只开放指定 IP 与指定端口号提供访问

### 配置方式

- 只允许 IP 为 10.86.13.249 的 PC 设备访问

- 

### 实现效果

- 端口扫描工具无法扫到其他端口

o

10.86.13.250

**状态:** 确定  
**操作系统:**  
**IP:** 10.86.13.250  
**MAC:** 00:60:65:5F:38:52  
**制造商:** BERNECKER, RAINER INDUSTRIE-ELEKTRONIC GmbH  
**NetBIOS:**  
**用户:**  
**类型:**  
**日期:**  
**备注:**

服务 详情

- 通过 AS 软件能够连接此 PLC

o ANSL: tcpip/COMT=2500 /DAIP=10.86.13.250 /REPO=11159 /ANSL=1 /PT=11169 X20CP1585 H4.73 RUN

- PLC 的 ModbusTCP Slave 与 Web 服务例如 SDM 均无法访问

## 案例三：关闭指定端口

### 配置方式

- 关闭 PLC 上开启的 111 端口

FirewallRules		FirewallRules	
Rule [1]		Rule [2]	
Rule Mode	Interactive	Rule Mode	Interactive
Rule String	block in proto tcp from any to any port = 111	Rule String	block out proto tcp from any port = 111 to any
Action	block	Action	block
Direction	in	Direction	out
Logging	off	Logging	off
Apply Action	If no other rule applies	Apply Action	If no other rule applies
Interface	no constraint	Interface	no constraint
Internet Protocol	TCP	Internet Protocol	TCP
Source Port	no constraint	Source Port	equal (=)
Destination Port	equal (=)	Port	111
Response	off	Destination Port	no constraint
Source Address	no constraint	Response	off
Destination Address	no constraint	Source Address	no constraint
Group	none	Destination Address	no constraint
		Group	none

### 实现效果

- 可见原先默认开放的 111 端口已被关闭



---

## 10.86.13.250

**状态:** 确定  
**操作系统:**  
**IP:** 10.86.13.250  
**MAC:** 00:60:65:5F:38:52  
**制造商:** BERNECKER RAINER INDUSTRIE-ELEKTRONIC GmbH  
**NetBIOS:**  
**用户:**  
**类型:**  
**日期:** 2000-01-01 00:53:26 UTC+00:00  
**备注:**

服务	详情
Port 80 (TCP)	
Port 502 (TCP)	