# 背景知识

- 023贝加莱操作系统支持防火墙功能吗
- <u>024如何在Automation Studio中配置防火墙</u>

# 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
      - 🗆 : 📷 FirewallRules 😑 📲 Rule (1) 🖮 🚰 Rule Mode Interactive 🚡 🌒 🛛 Rule String block in all 🔒 🖗 Action block in off Logging 🔒 👂 Apply Actio If no other rule appl Interface no constraint +-
- 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

0

- <u>https://www.advanced-port-scanner.com/cn/</u>
- 默认情况下开启 ModbusTCP Slave 功能的 PLC 开放的端口
  - 10.86.13.250

服务	详情
Port <b>80</b> (TCP)	
Port <b>111</b> (TCP)	rpcbind
Port <b>502</b> (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]	
i <b>⊨ j</b>		🚊 🛶 🎦 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
🚊 🕂 📴 🖬 🛉 📴	no constraint	👳 🖙 Internet Protocol	no constraint
🚊 👘 🚰 Internet Protocol	no constraint	🕂 🖙 Response	off
🚊 🖷 🚰 Response	off	🚊 📲 Source Address	must match
🚊 🖬 🚰 Source Address	no constraint	🔤 🔋 🕄 🖓 🔤	10.86.13.249
🚊 🔤 🚰 Destination Address	no constraint	🌒 Netmask (CIDR)	32
🖬 🖬 🚰 Group	none	庄 👔 🚰 Destination Address	me
, <b>⊨</b> , <b>≧</b> Rule [2]		료 🖙 Group	none
🚊 🛶 🚰 Rule Mode	Interactive	🖣 📲 🚰 Rule [4]	
🔤 👘 👷 🕄 Rule String	block out all	🛓 🚽 🚰 Rule Mode	Interactive
🦳 🦉 🏶 🖓 🖓	block		pass out quick from me to 10.86.13.249/32
🖳 🧯 Direction	out	🍀 Action	pass
🍀 Logging	off	🔋 🌒 Direction	out
🔤 🧯 🖓 Apply Action	If no other rule applies	🍀 Logging	off
📺 🚰 Interface	no constraint	🍀 Apply Action	Immediately
📺 🚰 Internet Protocol	no constraint	😐 🖙 Interface	no constraint
🚊 🛶 🚰 Response	off	😐 🖙 Internet Protocol	no constraint
🙀 👾 🚰 Source Address	no constraint	😐 🖙 Response	off
🚊 🛶 🚰 Destination Address	no constraint	庄 🗤 🚰 Source Address	me
🖬 🖬 🚰 Group	none	🚊 🛶 🚰 Destination Address	must match
		🔤 🔋 🕄 🕅 🖓	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 sett	ings				
	IP assigr	iment:		Manual	PC	的IP设置
	IPv4 address:			10.86.13.249		
	IPv4 sub	net prefix ler	ngth:	24		
	IPv4 gat	eway:		10.86.13.1		
	Edi	t				
Target type description		IP Address	Subnet Mask	Host name	AR Version	Serial Number
5APC22	00.AL18	10.86.13.252	255.255.255.0	br-automation	H04.73	F0AC0168586
nd in Files   🍎 🛛 🛷 X20CP	1585	10.86.13.250	255.255.255.0	br-automation	H04.73	C3AE0206887
ANGLI train (COMT-2500 (DAL	D_10.06.12	250 /DEDO-11	150 (ANSL - 1 /0	-11160 V20CD	1505 14 72	DUN

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

	IP settings	5			
	IP assignment	:	Manu	al	PC的IP
	IPv4 address:		10.86.	13.248	
	IPv4 subnet p	refix length:	24	_	
	IPv4 gateway:		10.86.	13.1	
	Edit				
		_		无	法访问
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
tcpip	/COMT=2500 /D/	AIP=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

🖃 👔 🧝 FirewallRules		🚰 Rule [3]	
🗖 🗖 Rule [1]		📄 🖮 💒 Rule Mode	Interactive
🖆 🛶 🚰 Rule Mode	Interactive	🔤 👔 🕄 Rule String	pass in log quick proto top from 10.86.13.249/32 to me port = 11169
🔤 🧝 🌒 Rule String	block in all	🕴 Action	pass
🔤 🔋 💭 💭	block	🕴 Direction	in
🏮 Direction	in		on
🍀 Logging	off	🕴 Apply Action	Immediately
🔤 🔋 🖓 Apply Action	If no other rule applies	🛓 💼 😁 Interface	no constraint
🕂 🕂 🚰 Interface	no constraint	🚊 📲 Internet Protocol	TCP
🕂 🔤 📅 Internet Protocol	no constraint	💶 🖬 🚰 Source Port	no constraint
🕂 🕂 🚰 Response	off	🚊 🚽 🚔 Destination Port	equal (=)
😐 😁 🚰 Source Address	no constraint	🦾 🧤 💲 Port	11169
😐 😁 🚰 Destination Address	no constraint	🕂 🐨 😭 Response	off
📃 😐 😁 🚰 Group	none	🚊 📲 Source Address	must match
📮 🔤 🚰 Rule [2]		🖳 🦉 🕼 IP Address	10.86.13.249
🗖 🛶 🚰 Rule Mode	Interactive	🔅 Netmask (CIDR)	32
🔤 🔐 😭 Rule String	block out all	🕂 🕂 🚰 Destination Address	me
🔜 👘 🕄 💭 💭	block	🛓 📩 🚰 Group	none
🔤 🧰 👘 💭 💭 💭 💭	out	Rule [4]	
🕄 Logging	off	🚊 🛶 🚰 Rule Mode	Interactive
🔋 Apply Action	If no other rule applies	🔤 👷 🏶 Rule String	pass out log quick proto tcp from me port = 11169 to 10.86.13.249/32
📃 🛱 Interface	no constraint	🏮 Action	pass
📃 🚊 🔤 Internet Protocol	no constraint	🔤 🔋 Direction	out
📃 🛱 Response	off	y 🏶 Logging	on
🚊 🔤 🚰 Source Address	no constraint	🏮 Apply Action	Immediately
📃 🚊 🔤 Destination Address	no constraint	🚰 Interface	no constraint
😐 🖙 Group	none	📮 🖓 🚰 Internet Protocol	TCP
		🚊 👘 🚰 Source Port	equal (=)
		🛛 🖳 🦉 🖗 Port	11169
		🛄 🔤 🚰 Destination Port	no constraint
		🚰 Response	off
		🗄 🛶 🚰 Source Address	me
		🚊 🛶 🚰 Destination Address	must match
		🔤 🕴 IP Address	10.86.13.249
		🌒 Netmask (CIDR)	32
		😐 🖙 Group	none

## 实现效果

• 端口扫描工具无法扫到其他端口

10.86.13.250

1	状态: 兼作系统:	确定
I	P:	10.86.13.250
N	MAC:	00:60:65:5F:38:52
4	制造商:	BERNECKER RAINER INDUSTRIE-ELEKTRONIC GmbH
N	vetBIOS:	
J.	用户:	
2	类型:	
E	日期:	
1	备注:	
[	服务 详情	
• 通过 AS 软件能够连接	倿此 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

0

• 关闭 PLC 上开启的 111 端口

-	👔 📷 FirewallRules			
•	🚊••• <b>p</b> 🚰 Rule [1]	🚊 👔 📩	7 Rule [2]	
	🛓 📥 🚽 🚰 Rule Mode	Interactive	<sub>2</sub> 🚰 Rule Mode	Interactive
	🔤 👷 🕴 Rule String	block in proto top 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
	🛛 🔤 👘 Port	111	🛓 🖬 🚰 Destination Port	no constraint
	🚰 Response	off	🛓 🗠 🚰 Response	off
	🚊 🔤 🚰 Source Address	no constraint	🛓 🚰 Source Address	no constraint
	🛓 🔤 🚰 Destination Address	no constraint	🛓 🗝 🚰 Destination Address	no constraint
	🗄 🖷 🚰 Group	none	🗄 🚰 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
抹作系统:	
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:	2000 01 01 00/00/20 07 0=00/00
<b>д</b> (т.	

服务	详情
Port <b>80</b> (TCP)	
Port <b>502</b> (TCP)	