

SIEMENS西门子 828D数字控制系统 6FC5370-5AA40-0AA0

产品名称	SIEMENS西门子 828D数字控制系统 6FC5370-5AA40-0AA0
公司名称	浔之漫智控技术(上海)有限公司
价格	.00/件
规格参数	西门子:代理经销商 操作面板:全新原装 假一罚十 德国:正品现货 实体经营
公司地址	上海市松江区石湖荡镇塔汇路755弄29号1幢一层 A区213室
联系电话	15801815554 15801815554

产品详情

S7-300/S7-400/PC CP 的安全 设置防火墙 S7-300/S7-400/PC CP 的本地防火墙规则 S7-300 CP/S7-400 CP/PC CP 概述 启用数据包过滤规则 如果在本地安全设置中启用了 CP 的安全功能，则在初始状态下可访问所有 CP 以及通过 CP 进行访问。要启用单个数据包过滤规则，请选中“激活防火墙”(Activate firewall)复选框。然后将启用所需的服务。由于连接组态比手动设置的规则具有更高的优先级，因此将自动创建防火墙规则。说明 gaoji防火墙模式中的详细防火墙设置

在gaoji防火墙模式下，可对单个的节点设置防火墙规则。要切换到gaoji防火墙模式，请选中“在gaoji模式下激活防火墙”(Activate firewall in advanced mode)复选框。带 VPN 的防火墙组态如果安全模块被添加到 VPN 组，那么默认情况下将启用防火墙。此外，“仅通道通信”(Tunnel communication only)复选框被启用。这意味着通过外部接口仅允许传送加密的 IPsec 数据。外部数据流量被阻止。

如果取消选择该复选框，则允许隧道通信以及在其它复选框中选择的通信类型。更新连接规则 如果对 CP 的连接组态进行了更改，则也会更改与连接相关的防火墙规则。要显示修改的防火墙规则，请单击“更新连接规则”(Update connection rules)按钮。随后，会在gaoji防火墙模式下显示经过修改的防火墙规则。默认模式下的日志设置与防火墙规则的关系“预定义的 IP 规则”和“预定义的 MAC 规则”中的日志设置不会影响因组态连接而自动创建的防火墙规则。例如，这意味着不能记录属于已组态连接的通过隧道传输的帧。在gaoji防火墙模式中，可以将记录扩展到自动生成的连接防火墙规则中。使用预定义 MAC 规则组态防火墙 - CP 343-1如何访问该功能 1. 选择待编辑的模块。 2. 选择“Firewall > Predefined MAC rules”条目。

在冗余关系的安全模块上加载组态（仅适用于 V4 及更高版本的 SCALANCE S623/S627-2M）

针对主模块组态的冗余关系的属性必须同时加载到主模块和次模块。要加载该组态，必须使用工程师站可通过其访问安全模块的物理 IP 地址。不能使用冗余关系的虚拟 IP 地址进行加载。指定一个不同的地址在“目标子网中的兼容设备”(Compatible devices in target subnet)对话框区域中，可以指定与本地安全设置中的 IP 地址/FQDN 地址不同的 IP 地址/FQDN 地址。为此，需要在“地址”(Address)表列的可编辑单元格中输入模块的 IP 地址/FQDN 地址。加载后，可通过本地安全设置中的 IP 地址/FQDN 地址访问安全模块。固件版本也可以将 SCALANCE S 模块的组态下载到固件版本比 STEP 7 中 SCALANCE S 模块的固件版本更高的 SCALANCE S 模块中。运行模式可在 SCALANCE S 模块运行期间下载组态。重新启动 SCALANCE S 模块以激活组态更改。说明特性只要模块尚未设置 IP 地址（即，在首次组态之前），模块和组态计算机之间就不会有路由器。如果将 PC 从 SCALANCE S 的内部接口交换到外部接口，那么将会禁用从该 PC 到 SCALANCE S 的访问约 20 分钟。组态状态每次下载之前，将检查安全模块上的现有组态并同要从 STEP 7 项目下载的组态进行比较。如果模块组态源自当前要用于下载的 STEP 7 项目且这些组态之间有差异，可以只将模块和项目组态之间有差异的文件下载到安全模块。在某些情况下，这样可加快下载速度。传输固件在传输新固件之前，需考虑的事项要将新固件传输到安全模块，必须满足以下条件：您具有传输固件所需的权限；请参见安全功能用户管理的特殊功能(页 457)部分。

安全模块中组态一个 IP 地址。进行安全传输

通过安全连接进行固件传输，这样就可以从不受保护的进行固件传输。固件本身也具有签名和加密。这将确保只有经过认证的固件才能下载到 SCALANCE S 模块。传送后必须重新启动只有在 SCALANCE S 模块重新启动后才，新下载的固件会生效。如果传输中断和终止，模块将使用旧版本的固件再次启动。默认模式下的日志设置与防火墙规则的关系“预定义的 IP 规则”和“预定义的 MAC 规则”中的日志设置不会影响因组态连接而自动创建的防火墙规则。例如，这意味着不能记录属于已组态连接的通过隧道传输的帧。在 gaoji 防火墙模式中，可以将记录扩展到自动生成的连接防火墙规则中。使用预定义防火墙规则组态防火墙 - CP 1628 使用预定义 IP 规则组态防火墙 - CP 1628 如何访问该功能 1. 选择待编辑的模块。2. 选择“Security > Firewall > Predefined IP rules”条目。默认模式下的日志设置与防火墙规则的关系“预定义的 IP 规则”和“预定义的 MAC 规则”中的日志设置不会影响因组态连接而自动创建的防火墙规则。例如，这意味着不能记录属于已组态连接的通过隧道传输的帧。在 gaoji 防火墙模式中，可以将记录扩展到自动生成的连接防火墙规则中。使用预定义 MAC 规则组态防火墙 - CP 1628 如何访问该功能 1. 选择待编辑的模块。2. 选择“Security > Firewall > MAC rules”条目。默认模式下的日志设置与防火墙规则的关系“预定义的 IP 规则”和“预定义的 MAC 规则”中的日志设置不会影响因组态连接而自动创建的防火墙规则。例如，这意味着不能记录属于已组态连接的通过隧道传输的帧。在 gaoji 防火墙模式中，可以将记录扩展到自动生成的连接防火墙规则中。S7-300-/S7-400-/PC-CP IP 数据包过滤方向含义 gaoji 防火墙模式的 IP 规则中通信方向“从”和“至”的可能选择。组态访问列表模块特定的功能该功能不适用于 CP 1628。含义可使用 IP 访问列表对某些 IP 地址设置访问保护。已创建的列表条目和相应权限在 CP 的本地设置的“防火墙 > IP 规则”(Firewall > IP rules)条目中显示(gaoji 防火墙模式)。说明安全激活后已更改的行为激活 CP 的安全功能后，访问保护将只应用于外部接口。也可通过在 gaoji 防火墙模式下组态适合的防火墙规则，将访问保护应用于内部接口。CP 也会对来自尚未发布的 IP 地址的 ARP 请求进行响应(第 2 层)。如果 CP 的 IP 访问列表不包含任何条目，且您为 CP 激活了安全，则将激活防火墙，并防止从外部位置访问 CP。在 gaoji 防火墙模式下组态对应的防火墙规则，以便访问 CP。激活安全时 IP 访问列表条目的效果在 CP 的本地设置中启用安全后，将在 gaoji 防火墙模式下创建相应的规则。针对您在地址列表中指定的 IP 地址创建防火墙规则“Accept > 外部 > 站”(Accept > External > Station)。IP 访问列表中的 IP 地址可相应地用作源 IP 地址。此外，也可将已定义的 IP 地址范围中的 IP 地址集成到相应的防火墙规则中。编辑要求编辑所创建的防火墙规则之前，必须满足以下条件：对于使用 STEP 7 进行编辑：“组态安全”(Configure security)组态权限对于使用 Web 服务器进行编辑：模块权限“Web：扩展 IP 访问控制列表”(Web:Expand IP access control list)超出本地安全设置范围的 IP 访问列表编辑要求在具体 CP 的部分中介绍。连接相关的自动防火墙规则含义对于使用 CP 组态的连接，STEP 7 会自动创建防火墙规则，允许在指定方向(CP 主动/被动)上与

CP 的伙伴进行通信。同时会考虑连接建立方向。要在启用了gaoji防火墙模式时显示这些防火墙规则，需要单击“更新连接规则”(Update connection rules)按钮。随后，会在gaoji防火墙模式下显示防火墙规则。说明手动释放UDP组播连接不会为UDP组播连接自动创建防火墙规则。要启用连接，请在gaoji防火墙模式中手动添加相关防火墙规则。根据所组态的连接建立方式，可创建以下3级防火墙规则。如果安全模块在VPN组中，方向“外部”将变为“通道”。这只适用于支持VPN的CP。在这些防火墙规则的“源IP地址”(Source IP address)和“目标IP地址”(Destination IP address)列中输入连接伙伴的IP地址。更改连接组态如果对CP的连接组态进行了更改，则也会更改与连接相关的防火墙规则。要显示修改的防火墙规则，请单击“更新连接规则”(Update connection rules)按钮。自动创建的防火墙规则的约定优先级规则具有最高的优先级，因此插入到本地规则集的顶部。删除规则无法删除规则。可以启用日志记录，并分配服务。还可以插入传输速度和注释。更改操作如果将操作从“Accept”设置为“丢弃”，或反之，则该设置将在系统同步更新期间再次被覆盖。如果要保留更改，则选择“Accept*”或“Drop*”操作。在这种情况下，只同步了IP地址，操作和方向仍与设置相同。系统同步更新后，即使操作不改为“Accept*”或“Drop*”，记录、服务、传输速度和注释的设置也会保留。如果删除了已组态的连接，相应的规则将从列表中删除。