SIEMENS西门子 3VA1 IEC断路器 3VA1 096-4ED32-0AA0

产品名称	SIEMENS西门子 3VA1 IEC断路器 3VA1 096-4ED32-0AA0
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 低压断路器: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

身份验证 设备 ID (Device ID) 输入在 SINEMA RC 中为模块生成的设备 ID。 设备密码 (Device password) 输入在 SINEMA RC 中组态的模块的设备密码。 最大字符数： 127 可选设置 在 “ 安全 > VPN > 可选设置 ” 参数组中通过参数 “ 连接类型 ” 对连接建立进行组态。 更新间隔 可通过此参数设置 CP 在 SINEMA RC 服务器上查询组态的间隔。 请注意，如果将 SINEMA RC 服务器的组态设置更改为 0（零），则 CP 将无法再与 SINEMA RC 服务器建立连接。 “ 连接类型 ” 该参数的两个选项将在连接建立中具有以下作用： – 自动 模块建立与 SINEMA RC服务器的连接。在连接参数由 SINEMA 远程连接服务器更改之前，OpenVPN 连接都会保持。如果连接中断，则 CP 会自动重新建立连接。 如果 SINEMA 远程连接服务器更改了连接参数，则 CP 将在上述组态的更新间隔结束后请求获取新的连接数据。 – PLC 触发器 该选项用于模块通过 SINEMA RC 服务器进行的偶发通信。 如果要在模块和 PC 之间建立临时连接，则可使用该选项。例如，临时连接通过 PLC 变量建立，可用于提供服务。 说明 连接中止 如果由于固件更新或 “ 下载到设备 ” 而导致 CPU 停止，则 OpenVPN 连接将中止。 仅在启用 “ 自动 ” 选项后才能使用这些功能。 建立连接的 PLC 变量 如果已选择选项 “ PLC 触发器 ”，则当 PLC 变量 (Bool) 变为值 1 时模块会建立一个连接。操作期间可根据需要通过使用 HMI 面板等方式设置 PLC 变量。 将 PLC 变量重置为 0 后，会再次终止连接。 调试期间手动设置时钟 说明 使用 Security/SINEMA RC 时的时钟同步 使用安全功能（例如 SINEMA Remote Connect）时，CP 需要当前时间以在伙伴或 SINEMA RC 服务器上进行验证。 首次建立连接之前，CP 会从 NTP 服务器接收时间。 CP 作为 VPN 连接的被动用户 设置通过被动用户建立 VPN 连接的权限 如果 CP 通过网关连接另一个 VPN 用户，则需要将建立 VPN 连接的权限设置为 “ Responder ” 。 以下典型组态中会出现这种情况： VPN 用户（主动） 网关（动态 IP 地址） Internet 网关（固定 IP 地址） CP（被动） 按如下方法，组态将 CP 作为被动用户建立 VPN 连接的权限： 1. 在 STEP 7 中，转到设备和网络视图。 2. 选择 CP。 3. 在本地安全设置中，打开 “ VPN ” 参数组。 4. 对于每个将 CP 作为被动 VPN 用户的 VPN 连接，将默认设置 “ Initiator/Responder ” 更改为设置 “ Responder ” 。防火墙

3.10.3.1 检查到达帧和离去帧时的防火墙顺序 每个到达帧或离去帧都会经过 MAC 防火墙（第 2 层）。 如果帧在此层级被丢弃，则 IP 防火墙（第 3 层）不会对其进行检查。 这表示，通过合适的 MAC 防火墙规则，可以限制或阻止 IP 通信。 参见 已编程的连接：防火墙规则的限制 (页 47) CPU 的虚拟接口 (页 43) 3.10.3.2 源 IP 地址的表示法（gaoji防火墙模式） 如果在 CP 的gaoji防火墙设置中指定源 IP 地址的地址范围，请确保表示法正确无误： 仅使用连字符来分隔两个 IP 地址。 正确：192.168.10.0-192.168.10.255 不要在两个 IP 地址之间输入任何其它符号。 错误：192.168.10.0 - 192.168.10.255 如果错误地输入范围，则不会使用防火墙规则。 3.10.3.3 HTTP 和 HTTPS 不可使用 IPv6 在工作站的 Web 服务器上无法通过 IPv6 协议使用 HTTP 和 HTTPS 通信。 如果在本地安全设置的 “ 防火墙 > 预定义的 IPv6 规则 ” (Firewall > Predefined IPv6 rules) 条目中启用防火墙： 所选复选框 “ 允许 HTTP ” (Allow HTTP) 和 “ 允许 HTTPS ” (Allow HTTPS) 没有作用。 3.10.3.4 连接的 VPN 隧道防火墙设置 gaoji防火墙模式中的 IP 规则 如果已组态 CP 间的连接，则在gaoji防火墙模式下操作 CP 时，请注意以下设置。 在 “ 安全 > 防火墙 > IP 规则 ” (Security > Firewall > IP rules) 参数组中，选择 “ Accept ” 设置进行两个 CP 的隧道连接。如果不启用该选项，则将终止并重新建立 VPN 隧道连接。 这适用于 CP 154x-1 与 CP 343-1 Advanced、CP 443-1 Advanced、CP 1628 或 CP 1243-1 等之间的连接。 参见 防火墙激活情况下的在线安全诊断和下载到站设置 (页 80) 3.10.4 在线功能 3.10.4.1 防火墙激活情况下的在线安全诊断和下载到站设置 针对在线功能设置防火墙 若已启用安全功能，请按照下面列出的步骤进行操作。 全局安全功能： 1. 选择条目 “ 防火墙 > 服务 > 为 IP 规则定义服务 ” (Firewall > Services > Define services for IP rules)。 2. 选择 “ ICMP ” 选项卡。 3. 插入一个类型为 “ Echo Reply ” 和一个类型为 “ Echo Request ” 的新条目。 CP 的本地安全功能： 现在选择 S7 站中的 CP。 1. 在 CP 的本地安全设置中，在 “ 安全 > 防火墙 ” (Security > Firewall) 参数组中启用gaoji防火墙模式。 2. 打开 “ IP 规则 ” (IP rules) 参数组。 3. 在表中，按如下方式为之前已创建的全局服务插入新的 IP 规则： – 操作：Accept；从：外部；至：站；服务 > ICMPv4/6 服务 > Echo Request（此前全局创建的服务） – 操作：Accept；从：站；至：外部；服务 > ICMPv4/6 服务 > Echo Reply（以前全局创建的服务） 4. 对于 “ Echo Request ” 服务的 IP 规则，在 “ 源 IP 地址 ” (Source IP address) 下输入工程师站的 IP 地址。基于这些规则，只能通过防火墙从包含 ICMP 数据包 (ping) 的工程师站访问 CP。 说明 在线安全诊断和下载的附加服务 如果希望使用 “ 在线安全诊断 ” (Online security diagnostics) 或 “ 下载到设备 ” (Download to device) 功能，则需要创建附加规则或禁用 “ Echo Request ” / “ Echo Reply ” 服务。 3.10.4.2 通过端口 8448 执行在线安全诊断 通过端口 8448 执行安全诊断 要求： 激活防火墙后，必须启用访问权限。 如果要在 STEP 7 Professional 中执行安全诊断，请按下列步骤进行操作： 1. 在 STEP 7 中选择 CP。 2. 打开 “ 在线和诊断 ” 快捷菜单。 3. 在 “ 安全性 ” 参数组中，单击 “ 在线连接 ” 按钮。 这样，即可通过端口 8448 执行安全诊断。 3.10.5 日志设置 - 过滤系统事件 系统事件值设置太高时产生的通信问题 如果过滤系统事件的值设置得过高，则您可能无法实现zuijia通信性能。 大量输出错误消息可延迟或阻止通信连接的处理。 在 “ Security > 日志设置 > 组态系统事件 ” (Security > Log settings > Configure system events) 中，将 “ 等级： ” (Level:) 参数设为值 “ 3（错误） ” (3 (Error))，以便确保建立可靠的通信连接。网络身份验证 网络身份验证和 EAP 方法 根据 “ IEEE 802.1X ” 规范，CP 支持网络身份验证。 网络身份验证用于 CP 可通过同样支持 IEEE 802.1X 的交换机访问网络的组态。CP 必须先对自身进行身份验证，然后才能实现网络访问。 CP 身份验证可通过检查 CP 自身身份的交换机处理，也可通过身份验证服务器或组态的 RADIUS 服务器处理。 身份验证通信是通过 Extensible Authentication Protocol (EAP) 运行的，用于向网络验证 CP 身份和密钥交换，以保障通信安全。 组态 1. 选择 CP。 2. 在本地安全设置中选择 “ 网络身份验证 ” (Network authentication) 条目并启用此选项。 3. 选择一种 EAP 方法： 4. 对所选 EAP 方法进行相应设置。 支持下列身份验证方法。 EAP 方法 MD5 MD5 方法无法抵御中间人攻击和字典式攻击。 建议使用安全性更高的方法。 TLS TLS 会建立加密 TLS 连接，并提供对客户端和网络的基于证书的相互认证。 PEAP PEAP 过程分为两个阶段。第一阶段会建立安全隧道，随后会在该隧道中执行另一身份验证 程序。 与 TLS 方法不同的是，PEAP并不一定要在第一阶段验证客户端的身份。因此组态客户端证书为可选项。 组态，程序块 3.10 安全性 CP 1543-1 操作说明, 07/2021, C79000-G8952-C289-08 83 TTLS TTLS 属于 TLS 的扩展，过程也分为两个阶段。通过加密通道（或隧道）提供对客户端和网络的基于 证书的相互认证。

与 TLS 相反，TTLS 仅需要服务器端证书。 MSCHAPv2 此方法最初用于登录 Microsoft 网络，但现在也供其它应用程序使用。此方法仅在安全隧道中使用。 PWD PWD 不加密也可使用。可在隧道中使用（例如 TTLS），也可单独使用。 建议使用安全性更高的方法。
验证方法的设置 对所使用的 EAP 方法进行以下设置。