SIEMENS西门子 电源模块 6SL3130-6TE23-6AA3

产品名称	SIEMENS西门子 电源模块 6SL3130-6TE23-6AA3
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 电源模块: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

VPN 概述 设备支持以下 VPN 系统 IPsec VPN（仅适用于 SCALANCE S615 和 SCALANCE SC64x-2C） OpenVPN（仅适用于 SCALANCE S615） IPsec VPN 可在 “ Security ” > “ IPsec VPN (页 918) ” 中组态 IPsec 连接。 借助 IPsec VPN，帧将以隧道模式传输。要使设备建立 VPN 隧道，远程网络必须具有 VPN 网 关作为伙伴。 对于 VPN 连接，设备区分两种模式： Roadwarrior 模式 在此模式下，伙伴的地址固定，或者输入从中建立连接的 IP 范围。设备从伙伴学习可访 问的远程子网。 标准模式 在此模式下，将yongjiu输入伙伴或远程子网的地址。设备既可作为 VPN 客户端主动建立连接，也可以被动等待伙伴建立连接。 IPsec 方法 在隧道模式下，设备使用 IPsec 方法建立 VPN 隧道。要传输的帧在发送到伙伴 VPN 网关前 会完全加密并为其提供新报头。伙伴接收到帧后进行解密并转发给接受者。 为确保安全，IPsec 协议组采用多种协议： IP 验证报头 (AH) 会处理源的验证和识别。 封装安全有效载荷 (ESP) 会加密数据。

状态检查防火墙 仅需指定一条用于从源到目标的查询方向的防火墙规则。将隐式添加第二条规则。例如，数据包过滤器会识别出计算机 “ A ” 正与计算机 “ B ” 通信，然后才允许响应。因此，如果计算机 “ A ” 未先发出请求，计算机 “ B ” 将无法进行查询。 在 “ 安全 > 防火墙 ” (Security > Firewall) (页 901) 下组态防火墙。 说明 通过第 2 层的 IP 数据包（同一 VLAN 内） 如果通过交换机端口（第 2 层）发送来自设备的 IP 数据包，则根据防火墙规则不会检查这些 IP 数据包。防火墙对第 2 层转发的数据包没有影响。IP 地址伪装 IP 地址伪装是一种简化的源 NAT。对于通过该接口发送的每个传出数据包，源 IP 地址均替 换为该接口的 IP 地址。调整后的数据包发送到目标 IP 地址。对于目标主机，查询似乎始终 来自同一发送方。外部网络无法直接访问内部节点。借助 NAPT，可通过设备的外部 IP 地址 访问内部节点的服务。 如果内部 IP 地址不能或不应在外部转发（例如，因为内部网络结构应保持隐藏而导致），则 可使用 IP

地址伪装。NAPT NAPT（网络地址和端口转换）是一种目标
NAT，通常称为端口转发。借此，可从外部访问被 IP 地址伪装或源 NAT 隐藏的内部节点的服务。
转换来自外部网络并用于设备的外部 IP 地址（目标 IP 地址）的传入数据包。目标 IP 地址替
换为内部节点的 IP 地址。除了地址转换外，还可进行端口转换。 可用于端口转换的选项如下： 源端口
目标端口 响应 单个端口 同一端口 如果端口相同，则将在不进行端口转换的情况下转发帧。 单个端口
单个端口 将源端口转换为目标端口。 端口范围 单个端口 将端口范围内的端口转换成同一端口 (n:1)。
端口范围 相同的端口范 围 如果端口范围相同，则将在不进行端口转换的情况下转发帧。 端口范围
其他端口范围 将源端口转换成目标范围内的任意空闲端口。
对于单一连接，这些端口通常会转换成目标范围内的第一个 端口。
如果同时进行多个连接，可使用循环方法将这些端口转换成 目标范围内的空闲端口。 单个端口
端口范围 将源端口转换成目标范围内的任意空闲端口。对于单一连
接，这些端口通常会转换成目标范围内的第一个端口。如果
同时进行多个连接，可使用循环方法将这些端口转换成目标
范围内的空闲端口。端口转发将允许外部节点访问内部网络的某些服务，例如 FTP、HTTP。 可在 “ 第 3
层 ” (Layer 3) > “ NAT ” > “ NAPT ” 下组态 NAPT。 源 NAT 与在地址伪装中相同，将转换源 NAT
中的源地址。除此之外，还可以限制传出数据包。其 中包括对某些 IP 地址或 IP
地址范围的限制和对某些接口的限制。 如果内部 IP 地址不能或不应在外部转发（例如，因为使用了
192.168.x.x 等专有地址范围而 导致），则可使用源 NAT。 可在 “ 第 3 层 ” (Layer 3) > “ NAT ” > “ 源
NAT ” (Source NAT) 下组态源 NAT。 NETMAP 借助
NETMAP，可将多个复杂子网转换为一个不同的子网。在此转换中，IP 地址子网部分将
发生更改，主机部分将保留。使用 NETMAP 进行转换时，仅需满足一条规则。NETMAP 可 转换源 IP
地址和目标 IP 地址。使用目标 NAT 和源 NAT 进行转换时则需要满足大量规则。 NETMAP 还可用于
VPN 连接。 可在 “ 第 3 层 ” (Layer 3) > “ NAT ” > “ NETMAP ” 下组态 NETMAP。 NAT 和防火墙
防火墙和 NAT 路由器支持 “ 状态检查 ” 机制。如果启用从内部到外部的 IP 数据通信，内部
注释可启动到外部网络的通信连接。 外部网络的回复帧可通过 NAT
路由器和防火墙，而无需将其地址额外包含在防火墙规则和 NAT
地址转换中。对于不属于来自内部网络查询的回复的帧，将被丢弃，无需匹配防火墙规 则。证书
证书类型 设备使用不同的证书来验证各种节点。 证书 用于... CA 证书 CA 证书是由Certificate Authority
签发的证书，从此认证机构获取服 务器证书、设备证书和伙伴证书。CA 证书具有由证书颁发机构签名
的私钥，可供获取证书。 建立连接时，将自动在设备和伙伴的 VPN 网关之间进行密钥交换。
无需手动交换密钥文件。 IPsec VPN (页 918) 服务器证书
要在设备和另一个网络参与方之间建立安全通信（例如 HTTPS、
VPN...），需要使用服务器证书。服务器证书是加密的 SSL 证书。服 务器证书源自最老的有效
CA，即使其已 “ 停止服务 ” 亦如此。关键 在于 CA 的有效期。 SINEMA RC (页 822) 设备证书
具有设备可用来进行自行识别的私钥（密钥文件）的证书。 IPsec VPN (页 918) 伙伴证书 伙伴的 VPN
网关用来基于设备进行自行识别的证书。 安全关联 (SA)
包含了伙伴之间协商的规范，例如，密钥有效期、加密算法和新验证周期 等信息。 Internet 密钥交换
(IKE) 是一种密钥交换方法。密钥交换分两个阶段进行： – 阶段 1
在该阶段，加密、验证和完整性检查等安全服务尚不可用，因为仍需创建所需密钥和 IPsec SA。阶段 1
用于为阶段 2 建立安全 VPN 隧道。为此，通信伙伴将协商 ISAKMP 安 全关联 (ISAKMP
SA)，此关联定义了所需安全服务（算法，所使用的验证方法）。因 而，后续消息和阶段 2 将安全。 –
阶段 2 阶段 2 用于协商所需 IPsec SA。与阶段 1 相似，交换在以下方面达成了一致：验证方
法、算法和加密方法（用于通过 IPsec AH 和 IPsec ESP 保护 IP 数据包）。 消息交换受在阶段 1 协商的
ISAKMP SA 的保护。凭借在阶段 1 中协商的 ISAKMP SA， 节点的身份已知且完整性检查方法已存在。
验证方法 CA 证书、设备和伙伴证书（数字签名）
证书用于不对称加密系统，其中每个节点（设备）均具有一对密钥。每个节点都具有伙
伴的密钥、私钥和公钥。私钥允许设备自行验证以及生成数字签名。 预共享密钥
预共享密钥用于对称加密系统。每个节点只有一个用于数据包解密和加密的密钥。通过
通用密码进行验证。 本地 ID 和远程 ID IPsec 将在 VPN 连接建立期间使用本地 ID 和远程 ID
对伙伴（VPN 端点）进行唯一标识。 加密方法 支持以下加密方法。该选择取决于阶段和密钥交换方法
(IKE)：VPN 伙伴的要求 VPN 伙伴必须支持 IPsec 及以下组态才能成功建立 IPsec 连接：

通过伙伴证书、CA 证书或预共享密钥进行的验证 IKEv1 或 IKEv2 至少以下 DH 组之一的支持：Diffie-Hellman 组 1、2、5 和 14 - 18 3DES 或 AES 加密 MD5、SHA1、SHA256、SHA384 或 SHA512 隧道模式 如果 VPN 伙伴位于 NAT 路由器的下游，伙伴必须支持 NAT-T。或者，NAT 路由器必须知道 IPsec 协议（IPsec/VPN 透传）。 NAT 穿越 (NAT-T) 设备和远程网络的 VPN 网关之间可能存在 NAT 路由器。并非所有 NAT 路由器都允许 IPsec 帧 通过。这意味着可能需要将 IPsec 帧封装进 UDP 数据包才能通过 NAT 路由器。 失效伙伴检测 仅当 VPN 伙伴支持 DPD 时才可实现。DPD 检查连接是否仍正常或者线路中是否已存在中断。 没有 DPD 时，根据组态情况，可能需要等到 SA 有效期满或必须手动重新启动连接。为检查 IPsec 连接是否仍正常，设备会自行向 VPN 伙伴站发送 DPD 查询。如果在经过一段时间后 VPN 伙伴站无回复，则与 VPN 伙伴站的连接将被视为无效。在阶段 1 中组态 DPD 的设置。OpenVPN 借助 OpenVPN，可建立虚拟专用网络 (VPN)。作为 OpenVPN 客户端，设备可建立到远程网 络的 VPN 连接。 在 “ 安全 ” > “ OpenVPN 客户端 (页 928) ” 中组态 OpenVPN 客户端。 VPN 连接通过虚拟设备驱动程序、TAP 和 TUN 设备建立。在此期间，创建虚拟网络接口，这 些接口相当于设备的物理接口，并表示 VPN 隧道的端点。 设备支持以下内容： TUN 设备：路由模式 LAN 接口和虚拟网络接口位于不同的 IP 子网中。虚拟隧道接口由 OpenVPN 服务器从专 用子网分配一个虚拟 IP 地址。IP 数据包（第 3 层）在虚拟隧道接口和 LAN 接口之间路由。 验证方法 证书：CA 证书和设备证书 证书用于不对称加密系统。每个节点（设备）都具有伙伴的密钥、私钥和公钥。私钥允 许设备自行验证以及生成数字签名。 用户名/密码 访问受用户名和密码限制。 加密方法 设备还支持以下方法： BF CBC AES128 CBC AES192 CBC AES256 CBC DES EDE3 VPN 连接建立 设备支持通过以下选项建立 VPN 连接。 OpenVPN：安全 > OpenVPN > 连接 (页 921) (Security > OpenVPN > Connections) IPsec VPN：安全 > IPsec VPN > 连接 (页 928) (Security > IPsec VPN > Connections) SINEMA RC：系统 > SINEMA RC (页 822) (System > SINEMA RC)