

汉土私有云 · 私域组网白皮书

项目	说明
产品名称	私域组网 (Private Domain Network, 简称 PDN)
品牌	汉土私有云
核心理念	隐私安全 · 资产自有 · 互通协作
文档性质	产品与技术白皮书 (对外口径)
文档版本	1.0
适用对象	决策层、架构师、集成商、企业网管与现场工程负责人
对照文档	本目录各端操作手册；产品需求只认仓库内 PRD

1. 执行摘要

私域组网是一套面向企业与工业现场的 **零信任异地组网平台**。它不要求公网固定 IP，也不要求把业务端口暴露到互联网，即可把分布在不同城市、不同运营商、不同云厂商上的电脑、服务器、手机和边缘硬件，连成同一张加密内网。

一句话能力：

一枚组网 Token，一张虚拟局域网。
同一空间内的已交付终端，用各自的虚拟 IP 互访，像在同一间办公室里。

相对传统专线、云厂商 VPN 和各类「组网盒子」，本系统坚持三件事：

- 控制权可私有化**：管控面 (hantu_pdn) 可官方托管，也可完整部署在企业自己的机房或专网。
- 先到达、再优化**：同一空间、双方在线时，组网必须先通（允许先走中继 / 保障）；通了之后再升直连，而不是「打洞失败就断网」。
- 数据面端到端加密**：用户业务走汉土加密通道。能直连则点对点，不经第三方搬业务包；打不通再走平台中继或保障线路。

现网已交付：**Windows 客户端、Linux 客户端、安卓客户端、汉土云盒 / 云盒 plus / 云路由、私域组网服务器**。iOS 与 macOS 客户端 **尚未交付**。

2. 要解决的问题

跨地域协作长期被三类成本卡住：

传统做法	现场痛点
运营商专线 / MPLS	开通慢、月租高、改点困难，门店与临时工地用不起
公网映射 / 端口转发	暴露攻击面，家庭宽带与 4G 几乎拿不到稳定入口
云厂商 VPN / 零信任网关	账号体系重、流量出域、密钥与审计不在自己手里
消费级「组网软件」	多端协议不一致、弱网易掉、工控下位机还要再装客户端

工业与门店还有第四个问题：**下位机不能装软件**。PLC、摄像机、老工控机只能插网线。没有硬件网关，组网到不了现场总线。

私域组网的目标不是替代运营商骨干网，而是在现有宽带、4G/5G 和跨云 VPC 之上，叠一张 **按 Token 隔离的加密叠加网**，把「能不能通」从专线采购里解放出来。

3. 产品定位

3.1 它是什么

- **控制面**：一条全局长连接信令，负责鉴权、地址分配、名单、选路意图、踢人与升级元数据。
- **数据面**：各端内核或本机上的汉土加密通道，分配叠加网地址（常见形态为 10.9.0.0/24 一类空间网段，具体以空间 IPAM 为准）。
- **打洞协助**：STUN 只为 **本端那一个数据面听口** 探家庭 NAT 映射。探测自己通了不算成功，必须对端能完成通道握手。
- **中继与保障**：打洞失败时，由平台做 UDP 中继或加密兜底，保证先通。
- **边缘网关**：汉土云盒系列把组网能力透传到 LAN 口，下位机免装客户端。

3.2 它不是什么

- 不是公共翻墙、不是全局代理、不是把整机上网流量强行送进隧道（安卓默认只走组网网段）。
- 不是把管控机当成用户面网关：管控不下发「整段叠加网都走中心节点」的路由，避免所有业务被中心拖死。
- 不是多 Token 同时在线的「一机多网」开关：换空间须更换 Token 后重新连接。
- 不是用公网 ICMP 判断组网死活：界面在线只认活着的信令连接。

3.3 核心理念

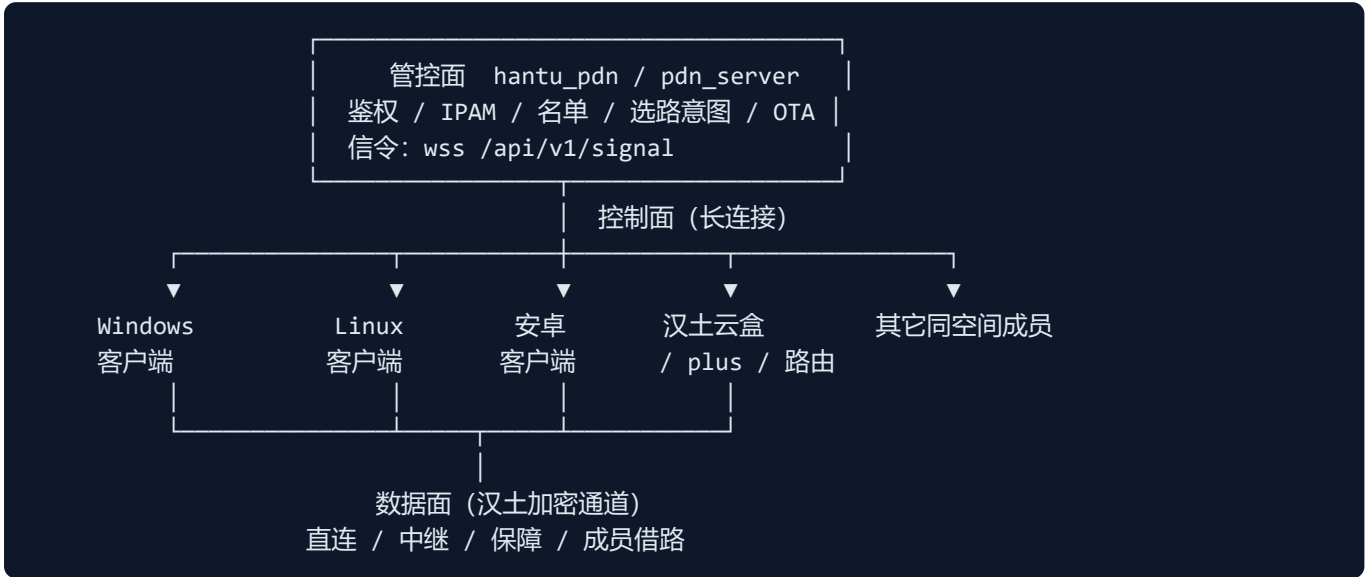
隐私安全。一 Token 一组网，空间之间逻辑隔离，默认互不可见。直连时业务包点对点加密，不经管控转发。

资产自有。密钥、设备名单、审计日志可以留在自建管控上。官方 API 只是一种接入入口，不是把网络所有权交给公有云。

互通协作。 Windows、Linux、安卓、云盒加入同一 Token 即可互访。现场用云盒，总部用服务器，出差用手机，不要求同一操作系统。

4. 总体架构

系统分成四层。决策层看「谁连谁」，工程层看「哪条通道在搬包」。



4.1 两个平面，互不替代

平面	载体	职责	明确不做
控制面	一条 WebSocket 长连接	入网、离线、地址、名单变化、选路意图、能力询问、踢人、升级通知	不搬用户业务包；不用 HTTP 轮询探活；不周期全量拉名单
数据面	汉土加密通道	叠加网上的业务互通	不承担「在不在线」判定
打洞协助	STUN	为数据面听口问路	不单独再开一套打洞端口
中继	汉土中继 （优先 UDP，必要时 TCP 明文）	对称 NAT / 打洞失败时转发用户数据	不是在线判定
保障	汉土保障线路 （加密兜底）	UDP 被墙时的兜底	不是优选路径，也不是在线判定

在线只认 **信令 WebSocket 还活着**（意外闪断有短宽限）。用户主动离开或被踢，立刻离线。界面绿点跟这条连接走；连接按钮、速率、本机虚拟 IP 跟数据面走。测 Ping 失败 **不会** 把绿点打成离线。

4.2 大脑与手脚

选路由管控统一出方案，终端负责测量与执行：

- **终端（手脚）**：环境就绪后再入网；盯数据面握手；从本端听口做 STUN；到不了对端时上报「到不了」；被点名才回能力；执行名单与借路安装。
- **管控（大脑）**：分配地址、交换坐标、通知互打；通道握手确认后才把路径粘成直连；需要借路时先通知中间成员装转发，再改两端。

终端不自己宣布「我要直连」，也不自己指定借路成员。这样四端行为一致，避免各端各写一套打洞状态机。

4.3 动态 Mesh，而不是中心转发网

默认模型是成员之间的 Mesh：

1. 能局域网直连，走局域网。
2. 能 IPv6 直连，走 IPv6。
3. 能打洞，走公网 P2P。打洞是 **有向** 的：对端能当入口，本端就可以发起。
4. 直连起不来，走汉土中继（优先 UDP，其次 TCP 明文）。
5. UDP 中继也不可用，走汉土保障（TLS）。
6. 某一对长期到不了、空间里又有合适的中间成员时，可以 **成员借路**（界面亦称汉土 ABC）：先让中间成员装好转发，再改这一对。借路不是把所有流量送回管控机。

验收底线：**同一空间、双方信令在线且都能连上管控时，叠加网必须能通**（允许先走中继 / 保障）。最优延迟是通了之后的事。空 Token、版本被拒、对端离线、策略隔离，不在这条保证内。

5. 智能选路与通道语义

现场人员在节点详情里看到的，是对端当前实际通道，不是「本机能力广告」。

界面用语	含义	限速
L1 局域网直连	同出口或同机房，延迟通常最低	不限（Token 数字管不到）
L2 IPv6 直连	原生 IPv6 端到端	不限
P2P 网络	公网 UDP 点对点	不限
汉土中继	经平台中继转发（UDP 优先，必要时 TCP 明文）	用户数据 按空间 Token 的 Mbps 限制
汉土保障线路	经平台加密通道兜底	同样只限这条上的用户数据
成员借路 / 汉土 ABC	经空间内另一台已与目标直连的成员转发	视该段实际通道

原则：

- **先到达、再优化。** 入网先占中继，交换坐标并互打通道握手；握手成功才固化直连。未握手成功禁止「看起来像 P2P」。
- **只升不无故降。** 直连优于借路，借路优于中继，中继优于保障。质量明显变差且空闲时可以拆开重选；有用户大流量时不切。
- **丢失只认曾经拥有。** 这一对曾经通道握手成功，后来握手超时且没有再成功，终端才报丢失。从未打通过、测 Ping 不通、公网 ping 管控域名，都不是丢失。管控收到后只换这一对，不按「握手年龄」丢弃合法报告。
- **能力不常发。** 终端不被点名就不上报能力画像，避免弱网和嵌入式设备被探测拖死。

打洞为数据面服务：每端加密通道 **只用一个 UDP 听口**，STUN 必须从该口发出。禁止再开临时口把错误映射上报给管控。

6. 组网空间、Token 与带宽

6.1 — Token 一组网

组网空间是隔离的基本单位。凭证是 **组网 Token**，格式必须以 `NET_TOKEN_` 开头。

- 未配置 Token：**禁止连接、禁止自动入网。**
- 没有内置官方 Token。设置页默认空，由管理员发放或用户申请后填写。
- 更换 Token 必须先断开再连。同一设备同一时间只加入一个空间。
- 「汉土私有云官方 API」是客户端里的 **接入入口**，不是 Token 本身。官方模式不在设置页回显真实管控 URL。

地址由管控按空间做 IPAM：设备上报公钥，绑定一台一址（/32）。可见性默认按空间成员；封禁与删除踢人，并通知他人从名单去掉。

现网单套管控实例的叠加地址池仍是共享默认网段、按 Token 隔离可见性，全实例大约 **250 台** 量级上限。需要更大的平面，应规划多套管控或后续独立地址池，而不是在一台管控上无限扩。

6.2 Token 级 QoS（必须按这句话理解）

限速数字 **只认该空间 Token 上的 Mbps**。

- **只限用户数据，且主要限制中继 / 保障。** P2P（含局域网直连）不限。信令、保活、STUN 问路、数据面握手与保活 **不限**。
- **限速 ≠ 转化效率。** 封装、中继绕路、用户态转发造成测速低于底网或低于 Token 数字，不叫「限速生效」，也不应用它去改 Token。
- 终端 **禁止** 把限速套在叠加网卡上，否则直连也会被误伤。安卓不套系统 QoS。执行点在中继 / 保障的数据转发。

社区免费申请写入的带宽以当时管控入库为准（现网免费申请为 **5 Mbps**，指该空间 Token 上的中继数字，不是「只能接 5 台设备」）。

6.3 入网码

管控台与 Windows / Linux / 安卓设置页可 **生成入网码**（二维码或同等文本），一次带上接入入口与 Token，供安卓扫码或其它端粘贴。入网码不是登录，只是代替手工填写。边缘终端当前不生成入网码，请到管控台或其它端生成。

7. 已交付端

中文	对外英文	形态	日常入口
Windows 客户端	<code>hantu_windows_client</code>	桌面 + 后台服务 + 系统托盘	<code>hantu-admin.exe</code>
Linux 客户端	<code>hantu_linux_client</code>	单二进制 + 本机 Web + systemd	浏览器 本机:17890
安卓客户端	<code>hantu_android_client</code>	应用 + 系统通道前台服务	App「汉士私有云-异地组网」
汉士云盒	<code>hantu_cloud_box</code>	边缘硬件，MT7628	LAN 口 Web <code>192.168.148.1:17890</code>
汉士云盒 plus	<code>hantu_cloud_box_plus</code>	云盒 + 4G 上行	同上
汉士云路由	<code>hantu_cloud_router</code>	同套边缘固件，口数 / 性能按硬件	同上
私域组网服务器	<code>hantu_pdn</code>	管控 + 信令 + 打洞协助 + 中继 / 保障	管理网页 / 自建 API

未交付：iOS 客户端、macOS 客户端。官网若仍出现这两项，以本文与 PRD 为准。

7.1 各端角色

端	适合谁	要点
Windows	运维工作站、办公 PC	界面不跑隧道；信令与数据面在后台服务。关窗口进托盘，不是退出
Linux	云主机、机房服务器	无桌面也能常驻。关浏览器不影响组网。Web 密码只保护本机管理页
安卓	巡检、出差、应急	扫码入网；状态栏保活；不要当热点或旁路路由器
云盒系列	门店、工控、无人值守	下位机免装客户端 ；开机可自动上网再自动入网

四端入网协议同一套，不按操作系统另开控制面。踢人走信令，不靠中继广播「删对端」。点断开：拆数据面；退出程序或清空 Token：正式离开并立刻离线。

7.2 边缘网关为什么单独成端

云盒不是「又一个 Linux 客户端」。它是现场网关：

- 上行：WAN、Wi-Fi 客户端，plus 还可 4G。
- 下行：LAN 口 DHCP。未入网时下发管理网段；入网成功后下发 **组网网段**，让工控机、摄像机直接拿到虚拟 IP。
- 管理口 `192.168.148.1:17890` 在入网后仍然保留，与组网虚拟 IP 并存。
- 恰好一台下位机时，访问云盒虚拟 IP（管理页与 SSH 除外）可转到这台设备，适合「一店一工控」。
- 运行时是 OpenWrt 上的常驻 C 进程加内核加密通道，不是用定时脚本轮询当热路径。配置写入专用存储，整包升级后仍在。

8. 入网生命周期

对使用者，最短路径始终是：

1. 拿到 Token（或扫入网码，或官方一键申请免费空间）。
2. 保存配置。
3. 点连接（或开机自动连接）。
4. 用虚拟 IP 访问对端。

对系统，入网是一条闸门流水线：

环境清单通过

- 带 Token 升级到信令长连接
- 下发身份、地址、中心对端
- 本端宣告「引导完成」
- 先核对版本目录（不对齐则升级；强制升级则先不选路）
- 中继占位，保证先能通
- 听口 STUN，上报映射
- 交换坐标，双方互打通道握手
- 握手成功才固化直连，否则留在中继 / 保障
- 运行中映射变化再报事实；到不了再求助或报丢失

版本过低或在黑名单时，入网在升级前就会被拒绝，并给出下载地址。此时还没有长连接，必须先升客户端 / 固件。设置页的「检查更新」是人手动动作，禁止当成心跳去打。

离开：用户点断开或退出，使用正式关闭。内部重连不是离开，对端不应闪离线。

9. 安全模型

9.1 身份与密钥

- 入网凭证是空间 Token，等同入网密钥。泄露 Token 等于把空间门打开。
- 设备以数据面公钥为稳定身份；设备编码（SN）用于人读与幂等，与公钥冲突时以公钥为准。
- 信令升级时用 Token 做一次性签名，并校验时间窗与一次性随机数，降低重放。
- 业务帧走 TLS 上的长连接；用户数据包走汉土加密通道。

9.2 隔离

- 不同 Token 默认互不可见、不能互访。
- 删除设备会回收地址并通知同空间刷新。
- 封禁 / 踢人由管控制台执行。Windows 界面可做部分操作；Linux / 安卓 / 云盒请用管控制台。

9.3 本机管理面

Linux 与云盒有本机 Web 管理密码，**不是**管控运维账号。Windows 本机 GUI 不设这道口令。安卓无本机 Web。管理端口不要暴露到公网。

9.4 审计与共创

入网、正式离开、踢人、封禁、ACL、免费空间申请等进入审计。

共创中心给缺陷与建议，不给「帮我分析这条线路为什么慢」。线路由终端与管控自动换档。勾选诊断资料时，本机打一份可分析快照（版本、SN、组网 IP、在线与通道、剥掉私钥的数据面状态等），**不含私钥、完整 Token、管理密码**。

9.5 明确不做的安全捷径

- 不用公网 ICMP 宣判叠加网死亡。
- 不把从未打通的路径报成「丢失」。
- 不在热路径上全量同步名单。
- 不把限速套到直连网卡。
- 不收集通讯录、短信、精确位置等与组网无关的个人信息。

10. 运维、升级与稳定性

10.1 自动升级

管控发布新包后，在线终端经信令获知，按平台目录下载：

- Windows / Linux：替换进程或二进制，组网中普通升级可跳过，强制升级才中断。
- 安卓：下载后须系统确认安装，不能静默覆盖。
- 云盒：整包固件写入，刷前固化配置；设置页可检查 / 立即升级。刷写须保持供电。

设置页对比本机与目录哈希。人手检查更新只允许点一次，禁止启动和每次连接都去问。

10.2 自愈

- Windows：缺驱动或后台服务异常时，可提权自愈。
- Linux：systemd 托管，意外退出拉起。
- 安卓：前台通知降低被杀概率；蜂窝与 Wi-Fi 切换后重新探测映射。
- 云盒：开机恢复 WAN / Wi-Fi → 自动入网 → 给 LAN 口下发组网地址。看门狗保护辅助进程，不把正常弱网当成整机复位理由。

10.3 弱网与 4G

4G 闪断有短宽限，避免界面狂闪离线。保障线路用于 UDP 被限制的网络，不作为「平时就该走的高速通道」。测速请同时看通道类型：直连对照不能用来证明中继质量。

11. 典型场景

11.1 企业异地分支与总部

总部一台云盒或 Linux 客户端，分厂电脑加入同一 Token。OA、ERP、NAS 用虚拟 IP 互访，不必申请专线，也不必把业务端口映射到公网。

11.2 工业边缘与物联网运维

野外机房、门店弱电间部署云盒或云盒 plus。摄像机和 PLC 只插 LAN。工程师在公司用 Windows 或手机，SSH / 远程桌面直连现场虚拟 IP。plus 在无宽带时用 4G 保上行。

11.3 远程研发

居家或出差打开 Windows / 安卓客户端，访问 Git、制品库、内网测试集群。客户端默认不把上网流量全部送进隧道，公网浏览仍走本地出口。

11.4 移动巡检与应急

安卓扫码入网，4G/5G 下看监控与传感器。弱网先走中继或保障，保证画面能出；条件好转再升直连。

11.5 跨云与混合云

云主机装 Linux 客户端，本地机房装云盒或另一台 Linux，同一 Token 打通。数据库、对象存储同步走虚拟 IP，减少安全组对公网端口的暴露。

11.6 多客户技术支持

按项目发放不同 Token。支持人员改 Token 后重连，进入目标客户空间。各空间互不串网。不要用同一个 Token 混装多个客户。

12. 三种交付模式

模式	使用者动作	适合	要点
社区免费版	客户端一键申请免费 Token	试用、实验室、小规模验证	官方入口；该空间写入免费档中继带宽；按设备编码幂等，同一设备重复申请得到同一枚 Token
官方托管尊享版	官网申请正式 Token 后手填	不想自建管控、需要平台中继	专属空间；中继 / 保障按该 Token 的 Mbps；P2P 仍不限
私有化自建版	部署 hantu_pdn，客户端选自建 API	密钥与审计必须在内网	客户端隐藏免费 / 正式按钮；Token 由管理员签发

不做：官网支付完成后自动写回客户端。正式 Token 始终由人填或扫码写入。

自建时，企业同时拥有：信令、地址分配、中继 / 保障节点、审计与升级目录。可在完全不出公网的专网里闭环运行，前提是各端能访问这套自建入口。

13. 与常见方案的对照

维度	运营商专线	云厂商 VPN	消费级组网 App	私域组网 PDN
开通	周到月	账号与企业合作	分钟级	分钟级（有 Token 即可）
固定公网 IP	常要	视产品	不要	不要
业务是否出域	不出	常经厂商网关	看厂商	直连时不出；中继仅打洞失败
密钥归属	运营商	云厂商	厂商	可完全自建
工控免装客户端	要再买 CPE	通常要	通常要	云盒 LAN 口透传
多端一致	视套餐	视套餐	常常一端一套	四端同一控制面
弱网	稳定但贵	看区域	易掉	先中继 / 保障，再升直连
限速	套餐带宽	套餐带宽	不透明	只限中继用户数据，数字在 Token 上

本系统不宣称「一定比专线更快」。专线买的是底网质量；PDN 买的是 在现有底网上把人连上，并且能私有化。直连时延迟接近底网；走中继时延迟高于直连，这是连通率换来的。

14. 部署时请建立的预期

1. **先通再快。** 第一次互访看到「汉土中继」或「保障线路」不是失败。对端绿点在、虚拟 IP 能通，才是入网成功。
2. **绿点不是 Ping。** 绿点是信令在。业务请用虚拟 IP 打真实端口。对端防火墙可能拦 ICMP。
3. **云盒入网后，电脑地址会变。** LAN 口从管理网段改发组网网段。运维电脑要重新获取 IP。管理页仍可用 192.168.148.1:17890。
4. **一台管控不是无限平面。** 现网按共享网段隔离可见性。超大规模应拆实例，而不是指望单空间无限扩。
5. **Token 当密钥管。** 不要发到群文件、不要提交仓库、不要截图公示。
6. **升级是运维动作。** 目录放对平台包，终端才能升。云盒刷写要保持供电。
7. **共创不是工单选路。** 线路自动换档；共创只收产品缺陷与建议。

15. 配套文档（本目录）

文档	用途
《汉土私有云私域组网白皮书》（本文）	决策与总体技术口径
Windows / Linux / 安卓 / 边缘终端操作手册	分端安装、界面与排障
《私域组网 App 用途说明》	安卓权限与审核说明
官网介绍页	对外传播，若与本文冲突， 以本文与 PRD 为准

实施与排障若进入协议字段、关码、选路公式，以仓库内信令文档和性能方案为准；那些是工程规范，不是本白皮书的读者义务。

16. 结语

私域组网把「异地要通」从专线采购里拆出来：用一枚 Token 圈出一张网，用一条信令管身份与选路，用加密通道搬业务，用中继和保障兜住打不了洞的现场，用云盒把不会装软件的设备也带进来。

它适合已经有宽带或 4G、但没有固定入口、又不愿把内网端口和密钥交给公有云的组织。

它不适合指望单台管控无限扩容、或把中继测速当成专线指标的场景。

落地建议按这个顺序：先用免费空间在两台 Windows / 一台 Linux 上验证互访，再把门店云盒和手机加进去，最后才把正式 Token 与自建管控放到生产。每一步都用虚拟 IP 验收「通」，再用通道字段验收「快」。

—— 汉土私有云 · 私域组网（PDN）