CUSTOMER BRIEF

IPBGP
IP Trust Intelligence

IP 可信度评分与家庭宽带真实性识别服务

Huicast Telecom Limited

Confidential Customer Package

team@huicast.cn

Version 2026.06

Table of Contents

IPBGP 产品介绍

IPBGP 是一套用于 IP 可信度评分与家庭宽带真实性识别的服务。面向金融风控、反作弊、安全运营、广告流量质量和内容合规场景。

客户提交一个 IP 后，IPBGP 会返回一份风险判断：系统会判断这个 IP 更接近真实用户，还是更接近代理、云服务器、自动化脚本、家庭宽带代理、匿名网络或高风险基础设施。系统同时给出可信度分、家庭宽带概率、风险标签和可解释原因，方便客户直接接入现有风控策略。

背景

现在很多攻击流量已经不再只来自明显的数据中心。代理池、家庭宽带代理、被入侵家庭宽带设备、云主机和自动化脚本经常混在一起，单靠静态名单很难处理。

客户常见的问题是：

1. ASN 属于家庭宽带运营商，实际却是代理出口。
2. 看起来像普通访问，背后却是批量注册、撞库、刷量、抢购脚本或 AI Agent 自动化流量。
3. 多个 IP 情报供应商给出不同结论，业务团队不知道该信谁。
4. 拦截时缺少解释，客服、运营和合规团队很难复盘，且难以根据自身需求自定义规则。
5. 风控策略太硬会误伤真实用户，相对开放的规则又挡不住攻击流量。

IPBGP 的目标是把这些模糊判断变成可执行的风险分数和证据。

IPBGP 提供的数据

IP 信任评分

IPBGP 为每个 IP 输出 0-100 的可信度分。客户可以按业务风险设置不同策略：

1. 高可信：正常放行。
2. 中等可信：增加人机验证（CAPTCHA）、限速或进入人工复核。
3. 低可信：拦截、加强人机验证（CAPTCHA）、降权或加入风险队列。

家庭宽带真实性判断

IPBGP 会判断 IP 背后的网络属性、历史风险、匿名化迹象、异常行为和位置一致性，输出其属于家庭宽带网络的概率和置信度。客户可以用它识别真实家庭宽带、移动网络、企业网络、云服务器、代理、VPN、Tor、家庭宽带代理和被滥用设备。

IPBGP 提供的风险标签

IPBGP 会给出清晰的风险标签，例如：

1. 代理或 VPN 风险
2. Tor 或匿名网络风险
3. 云服务器或托管网络风险
4. 家庭宽带代理风险
5. 恶意扫描或 C2 风险
6. 地理位置异常风险
7. 服务暴露异常风险

这些标签可以直接进入风控规则、告警系统或运营后台。

IPBGP 提供可解释证据

IPBGP 不只给结论，也给原因。

客户可以看到某个 IP 为什么被判为高风险，哪些证据提高了可信度，哪些证据拉低了分数。这样风控团队可以调规则，安全团队可以做复盘，客服和合规团队也能解释处理依据。

我们的优势

判断更细

传统 IP 库通常把 IP 分成 ISP、IDC、VPN 等几类。IPBGP 会进一步判断“它像不像真实用户”，而不是停留在静态分类上。

这对家庭宽带代理、被入侵家庭宽带设备、云服务器伪装和混合代理池尤其重要。

证据更完整

IPBGP 不是单一名单判断。系统会综合网络归属、路由稳定性、匿名化风险、威胁情报、服务暴露、地理一致性和客户自有样本。

客户拿到的是综合判断，不是某个来源的一条命中。

更适合落地

客户不需要自己拼接多个 IP 库，也不需要维护复杂的信号规则。IPBGP 直接输出分数、概率、风险标签和解释，接入风控系统后就能用于放行、人机验证（CAPTCHA）、限速和拦截。

可按业务调优

不同客户的风险偏好不同。广告反作弊、电商抢购、账号安全、支付风控和内容合规的阈值不会完全一样。

IPBGP 支持根据客户场景调整评分权重、风险阈值和解释口径，让结果更贴近业务。

技术说明（简版）

IPBGP 的判断不是靠单一名单，也不是简单查询某个 IP 分类库。IPBGP 会把几类信号放在一起看：

1. IP 背后的 ASN、前缀、上游网络和路由稳定性。
2. 网络类型更像家庭宽带、移动、企业、云服务、托管机房还是匿名网络。
3. 公开威胁源、blocklist、匿名网络出口和客户自有样本。
4. 开放端口、代理服务、证书特征、服务指纹和同网段异常密度。
5. 地理位置、网络路径和历史行为是否一致。

这些信号会进入同一个评分模型，最后输出 `trust score`、`residential_probability`、风险标签和证据列表。客户看到的是可直接使用的结果，不需要自己维护复杂规则。

适用场景

账号安全

用于登录、注册、找回密码、改绑、支付和提现等链路，识别撞库、批量注册、账号接管和代理访问。

广告反作弊

用于点击、展示、转化和流量采购质量评估，识别机房流量、代理流量、家庭宽带代理和异常流量。

电商和抢购

用于秒杀、优惠券、票务、限量商品和库存保护，识别脚本、代理池、云服务器和批量下单行为。

内容合规

用于地域访问控制、版权保护和跨区访问识别，判断 IP 位置与网络行为是否一致。

安全运营

用于 WAF、API 网关、SOC 和威胁分析，给安全告警补充 IP 风险画像和网络上下文。

API 响应与多语言

IPBGP 的 API 响应保持英文。字段名、枚举值、风险标签、动作建议和解释文本都使用英文，避免客户在系统集成时同时维护多套语言文案。

每条风险项和证据项都会带稳定代码，例如 `tor_exit`、`cloud_hosting`、`known_public_resolver`、`public_blocklist_hit`。客户可以把这些代码映射到自己的中文、英文、日文或其他语言文案，不需要解析自然语言。

响应中也会保留英文说明，方便调试和人工排查。面向终端用户或运营后台展示时客户只需要按照响应代码做本地化即可。

产品形态

IPBGP 支持多种接入方式：

1. API 查询：适合接入业务系统、风控引擎、安全网关和数据平台。
2. Web 查询控制台：适合风控、安全、运营和客服团队人工查询。
3. 批量分析：适合日志回放、广告流量清洗、注册/登录记录分析。
4. 私有化部署：适合对数据安全、合规和内部集成要求较高的客户。

API 响应示例

以下是产品 API 的演示响应，用于产品演示和客户沟通。JSON 响应保持英文。客户做多语言展示时，应使用 `code` / `i18n_key` 映射自己的文案。示例分数和证据为演示口径，不代表实时生产查询结果。

检测覆盖样例矩阵

这张表把产品能覆盖的主要检测场景放在一起。部分场景涉及受感染设备、开放代理、家庭宽带用户出口或蜜罐，不适合公开真实 IP。此类 IP 使用文档保留地址替代展示；实际查询会返回对应 IP 的实时结果。

场景	示例 IP	API 主要返回
公共 DNS / Anycast 基础设施	`1.1.1.1`	`decision=review`，`risk.public_resolver`，`risk.anycast_infrastructure`，`risk.non_residential`
大型公共 DNS 基础设施	`8.8.8.8`	`decision=review`，`risk.public_resolver`，`risk.infrastructure_ip`，`risk.non_residential`
云服务商地址段	`13.32.0.1`	`decision=challenge`，`risk.cloud_hosting`，`risk.non_residential`，`evidence.cloud_provider_cidr`
Tor 出口节点	`185.220.101.1`	`decision=block`，`risk.tor_exit`，`risk.anonymous_network`，`anonymization.is_tor=true`
高风险公开 blocklist 命中	`130.12.44.211`	`decision=block`，`risk.public_blocklist_hit`，`risk.high_abuse_likelihood`
开放服务端口	`45.33.32.156`	`decision=review`，`risk.server_exposed`，`evidence.open_server_ports`

场景	示例 IP	API 主要返回
C2 / 恶意 IOC 命中	`198.51.100.66`	`decision=block`，`risk.malware_ioc`，`risk.c2_infrastructure`，`evidence.public_threat_ioc`
开放 SOCKS5 代理	`198.51.100.77`	`decision=block`，`risk.open_proxy`，`evidence.socks5_proxy_confirmed`
HTTP 代理 + SOCKS 同时开放	`198.51.100.88`	`decision=block`，`risk.open_proxy`，`risk.proxy_density_high`，`evidence.http_and_socks_open`
同网段代理密度异常	`198.51.100.89`	`decision=block`，`risk.proxy_density_high`，`evidence.subnet_proxy_density`
公开服务 TLS 证书	`93.184.216.34`	`decision=review`，`risk.server_exposed`，`evidence.ca_tls_certificate`
IP 证书 / 自建实验室倾向	`198.51.100.24`	`decision=review`，`evidence.ip_certificate`，`risk.low_residential_confidence`
邮件服务器 / SMTP 暴露	`198.51.100.25`	`decision=review`，`risk.mail_server`，`evidence.smtp_service_exposed`
家庭宽带	`198.51.100.31`	`decision=allow`，`risk.none`，`evidence.residential_network_prior`
移动网络 / CGNAT 辅助信号	`100.64.12.34`	`decision=allow`，`evidence.mobile_or_cgnat_network`，`trust.residential_probability=high`
RPKI 无效或路由异常	`198.51.100.44`	`decision=review`，`risk.routing_anomaly`，`evidence.rpki_invalid`
地理位置与网络路径不一致	`198.51.100.55`	`decision=challenge`，`risk.geoip_mismatch`，`evidence.latency_geo_mismatch`
短期高频轮换 / 历史不稳定	`198.51.100.56`	`decision=challenge`，`risk.ip_churn`，`evidence.history_churn_fast`
观测到扫描行为	`198.51.100.99`	`decision=block`，`risk.honeypot_observed_scan`，`evidence.honeypot_observation`
家庭宽带代理样本命中	`198.51.100.108`	`decision=block`，`risk.residential_proxy`，`evidence.proxyware_signature`
服务指纹命中高风险模式	`198.51.100.109`	`decision=block`，`risk.c2_infrastructure`，`evidence.jarm_high_risk_match`
IPv6 家庭宽带前缀模式	`2001:db8:100:200::42`	`decision=allow`，`evidence.ipv6_residential_pattern`，`trust.residential_probability=high`

示例 1：公共 DNS / Anycast 基础设施

客户请求：

```
GET /v1/ip/1.1.1.1?verbose=true
Authorization: Bearer <token>
```

API 响应：


```
{
  "ip": "1.1.1.1",
  "version": "v1",
  "classification": {
    "connection_type": "datacenter",
    "is_residential": false,
    "is_hosting": false,
    "is_mobile": false,
    "is_datacenter": true,
    "type_confidence": 96
  },
  "trust": {
    "score": 54,
    "residential_probability": 0.01,
    "confidence": 92,
    "decision": "review",
    "decision_code": "REVIEW_INFRASTRUCTURE_IP",
    "summary_code": "SUMMARY_PUBLIC_RESOLVER_NON_RESIDENTIAL",
    "summary": "This IP is public DNS and Anycast infrastructure. It is not a normal residential
user endpoint."
  },
  "risks": [
    {
      "code": "public_resolver",
      "i18n_key": "risk.public_resolver",
      "severity": "medium"
    },
    {
      "code": "anycast_infrastructure",
      "i18n_key": "risk.anycast_infrastructure",
      "severity": "medium"
    },
    {
      "code": "non_residential",
      "i18n_key": "risk.non_residential",
      "severity": "medium"
    }
  ],
  "network": {
    "asn": 13335,
    "asn_name": "Cloudflare",
    "as_type": "content_network",
    "prefix": "1.1.1.0/24",
    "is_anycast": true,
    "rpki_status": "valid"
  },
  "evidence": [
    {
      "code": "known_public_resolver",
      "i18n_key": "evidence.known_public_resolver",
      "category": "network",
      "impact": "negative",
      "weight": 0.7,
      "message": "The IP is a known public DNS resolver and is not expected to be an end-user
residential address."
    },
    {
```

```
      "code": "anycast_infrastructure",
      "i18n_key": "evidence.anycast_infrastructure",
      "category": "network",
      "impact": "negative",
      "weight": 0.6,
      "message": "The IP is served through Anycast infrastructure."
    },
    {
      "code": "no_public_abuse_hit",
      "i18n_key": "evidence.no_public_abuse_hit",
      "category": "reputation",
      "impact": "positive",
      "weight": 0.2,
      "message": "No public abuse-feed hit was found in the current snapshot."
    }
  ],
  "recommended_action": {
    "login": "challenge",
    "signup": "challenge",
    "payment": "review",
    "content_access": "allow_with_low_residential_confidence"
  }
}
```


示例 2：Tor 出口节点

客户请求：

```
GET /v1/ip/185.220.101.1?verbose=true
Authorization: Bearer <token>
```

API 响应：


```
{
  "ip": "185.220.101.1",
  "version": "v1",
  "classification": {
    "connection_type": "hosting",
    "is_residential": false,
    "is_hosting": true,
    "is_mobile": false,
    "is_datacenter": true,
    "type_confidence": 97
  },
  "trust": {
    "score": 9,
    "residential_probability": 0.0,
    "confidence": 96,
    "decision": "block",
    "decision_code": "BLOCK_TOR_EXIT",
    "summary_code": "SUMMARY_TOR_EXIT_HIGH_RISK",
    "summary": "This IP is a Tor exit node and should be treated as high-risk anonymous traffic."
  },
  "risks": [
    {
      "code": "tor_exit",
      "i18n_key": "risk.tor_exit",
      "severity": "critical"
    },
    {
```

```
      "code": "anonymous_network",
      "i18n_key": "risk.anonymous_network",
      "severity": "high"
    },
    {
      "code": "non_residential",
      "i18n_key": "risk.non_residential",
      "severity": "high"
    }
  ],
  "anonymization": {
    "is_proxy": true,
    "is_vpn": false,
    "is_tor": true,
    "provider": "Tor"
  },
  "network": {
    "as_type": "hosting",
    "is_anycast": false,
    "rpki_status": "unknown"
  },
  "evidence": [
    {
      "code": "tor_exit",
      "i18n_key": "evidence.tor_exit",
      "category": "anonymization",
      "impact": "negative",
      "weight": 0.98,
      "message": "The IP appears in Tor exit-node data."
    },
    {
      "code": "anonymous_network",
      "i18n_key": "evidence.anonymous_network",
      "category": "network",
      "impact": "negative",
      "weight": 0.9,
      "message": "The network role is closer to anonymous traffic relay than end-user access."
    }
  ],
  "recommended_action": {
    "login": "block_or_strong_challenge",
    "signup": "block",
    "payment": "block",
    "content_access": "block_or_policy_review"
  }
}
```


示例 3：公开 blocklist 命中

客户请求：

```
GET /v1/ip/130.12.44.211?verbose=true
Authorization: Bearer <token>
```

API 响应：


```
{
  "ip": "130.12.44.211",
  "version": "v1",
  "classification": {
```

```
    "connection_type": "unknown",
    "is_residential": false,
    "is_hosting": false,
    "is_mobile": false,
    "is_datacenter": false,
    "type_confidence": 72
  },
  "trust": {
    "score": 4,
    "residential_probability": 0.0,
    "confidence": 94,
    "decision": "block",
    "decision_code": "BLOCK_PUBLIC_BLOCKLIST_HIT",
    "summary_code": "SUMMARY_PUBLIC_BLOCKLIST_HIGH_RISK",
    "summary": "This IP is listed in high-risk public blocklist data and should be blocked or
escalated for security review."
  },
  "risks": [
    {
      "code": "public_blocklist_hit",
      "i18n_key": "risk.public_blocklist_hit",
      "severity": "critical"
    },
    {
      "code": "high_abuse_likelihood",
      "i18n_key": "risk.high_abuse_likelihood",
      "severity": "critical"
    },
    {
      "code": "non_residential",
      "i18n_key": "risk.non_residential",
      "severity": "high"
    }
  ],
  "network": {
    "as_type": "unknown",
    "is_anycast": false,
    "rpki_status": "unknown"
  },
  "evidence": [
    {
      "code": "public_blocklist_drop",
      "i18n_key": "evidence.public_blocklist_drop",
      "category": "reputation",
      "impact": "negative",
      "weight": 0.95,
      "message": "The IP or its containing netblock appears in high-risk public blocklist data."
    },
    {
      "code": "community_abuse_feed",
      "i18n_key": "evidence.community_abuse_feed",
      "category": "reputation",
      "impact": "negative",
      "weight": 0.7,
      "message": "The IP also appears in community abuse intelligence."
    },
    {
      "code": "no_residential_evidence",
      "i18n_key": "evidence.no_residential_evidence",
      "category": "classification",
      "impact": "negative",
      "weight": 0.5,
      "message": "No reliable evidence supports a residential-user classification."
    }
  ],
  "recommended_action": {
```

```
    "login": "block",
    "signup": "block",
    "payment": "block",
    "content_access": "block"
  }
}
```

示例 4：云服务商地址段

客户请求：

```
GET /v1/ip/13.32.0.1?verbose=true
Authorization: Bearer <token>
```

API 响应：

```
{
  "ip": "13.32.0.1",
  "version": "v1",
  "classification": {
    "connection_type": "datacenter",
    "is_residential": false,
    "is_hosting": true,
    "is_mobile": false,
    "is_datacenter": true,
    "type_confidence": 94
  },
  "trust": {
    "score": 31,
    "residential_probability": 0.0,
    "confidence": 90,
    "decision": "challenge",
    "decision_code": "CHALLENGE_CLOUD_HOSTING",
    "summary_code": "SUMMARY_CLOUD_HOSTING_NON_RESIDENTIAL",
    "summary": "This IP belongs to a public cloud provider range. It is not necessarily malicious,
but it should not be treated as a residential user."
  },
  "risks": [
    {
      "code": "cloud_hosting",
      "i18n_key": "risk.cloud_hosting",
      "severity": "high"
    },
    {
      "code": "non_residential",
      "i18n_key": "risk.non_residential",
      "severity": "high"
    },
    {
      "code": "automation_friendly_network",
      "i18n_key": "risk.automation_friendly_network",
      "severity": "medium"
    }
  ],
  "network": {
    "asn": 16509,
    "asn_name": "Amazon",
    "as_type": "cloud_hosting",
    "is_anycast": false,
    "rpki_status": "valid"
```

```
  },
  "evidence": [
    {
      "code": "cloud_provider_cidr",
      "i18n_key": "evidence.cloud_provider_cidr",
      "category": "network",
      "impact": "negative",
      "weight": 0.9,
      "message": "The IP is contained in a public cloud provider address range."
    },
    {
      "code": "non_residential_network",
      "i18n_key": "evidence.non_residential_network",
      "category": "classification",
      "impact": "negative",
      "weight": 0.85,
      "message": "The network profile does not match residential broadband or mobile access."
    }
  ],
  "recommended_action": {
    "login": "challenge",
    "signup": "challenge",
    "payment": "review",
    "content_access": "policy_based"
  }
}
```


示例 5：开放服务端口

客户请求：

```
GET /v1/ip/45.33.32.156?verbose=true
Authorization: Bearer <token>
```

API 响应：


```
{
  "ip": "45.33.32.156",
  "version": "v1",
  "classification": {
    "connection_type": "hosting",
    "is_residential": false,
    "is_hosting": true,
    "is_mobile": false,
    "is_datacenter": true,
    "type_confidence": 91
  },
  "trust": {
    "score": 28,
    "residential_probability": 0.0,
    "confidence": 88,
    "decision": "review",
    "decision_code": "REVIEW_SERVER_EXPOSED",
    "summary_code": "SUMMARY_OPEN_SERVER_PORTS",
    "summary": "This IP exposes server-like services and should not be treated as a residential
user endpoint."
  },
  "risks": [
    {
      "code": "server_exposed",
```

```
      "i18n_key": "risk.server_exposed",
      "severity": "medium"
    },
    {
      "code": "non_residential",
      "i18n_key": "risk.non_residential",
      "severity": "high"
    }
  ],
  "active": {
    "open_ports": [22, 80],
    "open_proxy": false,
    "tls_cert": "none",
    "tcp_fingerprint": "server"
  },
  "evidence": [
    {
      "code": "open_server_ports",
      "i18n_key": "evidence.open_server_ports",
      "category": "active",
      "impact": "negative",
      "weight": 0.75,
      "message": "The IP exposes server-like ports, which lowers residential probability."
    },
    {
      "code": "tcp_fingerprint_serverlike",
      "i18n_key": "evidence.tcp_fingerprint_serverlike",
      "category": "active",
      "impact": "negative",
      "weight": 0.55,
      "message": "The network fingerprint is closer to a server than an end-user device."
    }
  ],
  "recommended_action": {
    "login": "challenge",
    "signup": "challenge",
    "payment": "review",
    "content_access": "policy_based"
  }
}
```


示例 6：开放 SOCKS5 代理示例

客户请求：

```
GET /v1/ip/198.51.100.77?verbose=true
Authorization: Bearer <token>
```

API 响应：


```
{
  "ip": "198.51.100.77",
  "version": "v1",
  "classification": {
    "connection_type": "hosting",
    "is_residential": false,
    "is_hosting": true,
    "is_mobile": false,
    "is_datacenter": true,
    "type_confidence": 96
```

```
  },
  "trust": {
    "score": 6,
    "residential_probability": 0.0,
    "confidence": 95,
    "decision": "block",
    "decision_code": "BLOCK_OPEN_PROXY",
    "summary_code": "SUMMARY_OPEN_SOCKS5_PROXY",
    "summary": "This IP has a confirmed open SOCKS5 proxy service and should be treated as high-
risk proxy traffic."
  },
  "risks": [
    {
      "code": "open_proxy",
      "i18n_key": "risk.open_proxy",
      "severity": "critical"
    },
    {
      "code": "socks5_proxy",
      "i18n_key": "risk.socks5_proxy",
      "severity": "critical"
    },
    {
      "code": "non_residential",
      "i18n_key": "risk.non_residential",
      "severity": "high"
    }
  ],
  "active": {
    "open_ports": [1080],
    "open_proxy": true,
    "proxy_protocols": ["socks5"],
    "subnet_proxy_density": 0.18,
    "tcp_fingerprint": "server"
  },
  "evidence": [
    {
      "code": "socks5_proxy_confirmed",
      "i18n_key": "evidence.socks5_proxy_confirmed",
      "category": "active",
      "impact": "negative",
      "weight": 0.98,
      "message": "The IP has a confirmed open SOCKS5 proxy service."
    },
    {
      "code": "open_proxy_confirmed",
      "i18n_key": "evidence.open_proxy_confirmed",
      "category": "active",
      "impact": "negative",
      "weight": 0.95,
      "message": "The proxy service was confirmed, not inferred only from an open port."
    },
    {
      "code": "subnet_proxy_density",
      "i18n_key": "evidence.subnet_proxy_density",
      "category": "active",
      "impact": "negative",
      "weight": 0.65,
      "message": "Nearby addresses show elevated proxy density."
    }
  ],
  "recommended_action": {
    "login": "block_or_strong_challenge",
    "signup": "block",
    "payment": "block",
    "content_access": "block_or_policy_review"
```

```
    }
}
```