CUSTOMER BRIEF

IPBGP
IP Trust Intelligence

IP trust scoring and home broadband authenticity service

Huicast Telecom Limited

Confidential Customer Package

team@huicast.cn

Version 2026.06

Table of Contents

IPBGP Product Brief

IPBGP is an IP trust scoring and home broadband authenticity service. It is built for risk control, anti-fraud, security operations, traffic quality review, and content access policy.

When a customer submits an IP address, IPBGP returns a risk decision. The service checks whether the IP looks like a real user endpoint, or whether it is closer to a proxy, cloud server, automated script, home broadband proxy, anonymous network, or high-risk infrastructure. The response includes a trust score, home broadband probability, risk labels, and explainable evidence that can be used directly in an existing risk workflow.

The Problem

Attack traffic no longer comes only from obvious data centers. Proxy pools, home broadband proxies, compromised home broadband devices, cloud hosts, and automation traffic are often mixed together. A static list is not enough.

Common customer problems include:

1. The ASN belongs to a home broadband operator, but the IP is actually used as a proxy exit.
2. The visit looks normal, but behind it are bulk signups, credential stuffing, click fraud, purchase bots, or AI agent traffic.
3. Different IP intelligence vendors return different answers, and the business team does not know which one to trust.
4. Blocking decisions are hard to explain, which makes review difficult for support, operations, and compliance teams.
5. Rules that are too strict hurt real users. Rules that are too loose let attack traffic through.

IPBGP turns these unclear cases into a score, a decision, and a set of evidence items.

Data Returned by IPBGP

IP Trust Score

IPBGP returns a 0-100 trust score for each IP. Customers can map the score to their own business actions:

1. High trust: allow.
2. Medium trust: add CAPTCHA, rate limit, or send to manual review.
3. Low trust: block, add stronger verification, downrank, or put into a risk queue.

Home Broadband Authenticity

IPBGP reviews network ownership, historical risk, anonymization signals, abnormal behavior, and location consistency. It returns the probability and confidence that an IP belongs to a real home broadband network.

Customers can use it to separate real home broadband, mobile networks, enterprise networks, cloud servers, proxies, VPNs, Tor exits, home broadband proxies, and abused devices.

Risk Labels

IPBGP returns clear risk labels, including:

1. Proxy or VPN risk
2. Tor or anonymous network risk
3. Cloud or hosting network risk
4. Home broadband proxy risk
5. Malicious scanning or C2 risk
6. Location mismatch risk
7. Exposed service risk

These labels can be used in risk rules, alerting systems, or internal review dashboards.

Explainable Evidence

IPBGP returns the decision and the reason behind it.

A customer can see why an IP was marked high risk, which evidence increased trust, and which evidence reduced the score. Risk teams can tune rules. Security teams can review incidents. Support and compliance teams get a clear basis for their decision.

Why Teams Use IPBGP

Finer Judgement

Most IP databases classify an address as ISP, IDC, VPN, and a few other broad types. IPBGP goes further and asks a more useful question: does this IP behave like a real user endpoint?

That matters for home broadband proxies, compromised home devices, cloud servers pretending to be user traffic, and mixed proxy pools.

Better Evidence

IPBGP is not a single list lookup. It combines network ownership, route stability, anonymization risk, public threat intelligence, exposed services, location consistency, and customer samples.

The customer gets one decision backed by multiple signals, not a raw hit from one source.

Easier Integration

Customers do not need to stitch together several IP databases or maintain a large set of signal rules. IPBGP returns scores, probabilities, labels, and evidence that can be used for allow, CAPTCHA, rate limit, review, and block actions.

Tuned to the Customer's Business

Risk tolerance changes by business. Advertising fraud, ecommerce abuse, account security, payment risk, and content policy do not use the same thresholds.

IPBGP can adjust scoring weights, risk thresholds, and explanation style for the customer's use case.

Short Technical Note

IPBGP does not rely on a single list or a simple IP type lookup. It reviews several groups of signals together:

1. ASN, prefix, upstream network, and routing stability.
2. Whether the network looks like home broadband, mobile, enterprise, cloud, hosting, or anonymous infrastructure.
3. Public threat sources, blocklists, anonymous network exits, and customer samples.
4. Open ports, proxy services, certificate traits, service fingerprints, and abnormal subnet density.
5. Whether location, network path, and history agree with each other.

These signals are scored together. The final response includes `trust score`, `residential_probability`, risk labels, and evidence. Customers receive a result they can use without maintaining the rules themselves.

Use Cases

Account Security

Used for login, signup, password reset, account binding, payment, and withdrawal flows. IPBGP helps detect credential stuffing, bulk registration, account takeover, and proxy access.

Ad Fraud

Used for click, impression, conversion, and traffic quality review. IPBGP helps detect data center traffic, proxy traffic, home broadband proxies, and abnormal traffic.

Ecommerce and Limited Inventory

Used for flash sales, coupons, ticketing, limited goods, and inventory protection. IPBGP helps detect scripts, proxy pools, cloud servers, and bulk ordering behavior.

Content Policy

Used for regional access control, copyright protection, and cross-region access review. IPBGP checks whether IP location and network behavior match.

Security Operations

Used by WAF, API gateway, SOC, and threat analysis workflows. IPBGP adds IP risk context and network background to security alerts.

API Response and Localization

IPBGP API responses stay in English. Field names, enum values, risk labels, action suggestions, and explanation text all use English so customers do not have to maintain several API languages at the same time.

Each risk item and evidence item carries a stable code, such as `tor_exit`, `cloud_hosting`, `known_public_resolver`, and `public_blocklist_hit`. Customers can map these codes to their own Chinese, English, Japanese, or other UI copy without parsing natural language.

English explanation text is still included for debugging and manual review. For user-facing screens or operations dashboards, customers can localize by response code.

Product Formats

IPBGP supports several ways to use the service:

1. API query: for business systems, risk engines, security gateways, and data platforms.
2. Web console: for risk, security, operations, and support teams.
3. Batch analysis: for log replay, traffic cleanup, signup analysis, and login analysis.
4. Private deployment: for customers with stricter data security, compliance, or internal integration requirements.

API Response Examples

The following examples show product API responses for demos and customer discussion. JSON responses stay in English. Customers should use `code` and `i18n_key` to map the response to their own UI copy. Scores and evidence are demonstration values, not live production query results.

Coverage Matrix

This table shows the main detection scenarios covered by the product. Some cases involve compromised devices, open proxies, home broadband user exits, or honeypot observations. Those IPs should not be published in customer material, so documentation-reserved addresses are used for display. A real query returns the result for the submitted IP.

Scenario	Sample IP	Main API Return
Public DNS / Anycast infrastructure	`1.1.1.1`	`decision=review`, `risk.public_resolver`, `risk.anycast_infrastructure`, `risk.non_residential`
Large public DNS infrastructure	`8.8.8.8`	`decision=review`, `risk.public_resolver`, `risk.infrastructure_ip`, `risk.non_residential`
Cloud provider range	`13.32.0.1`	`decision=challenge`, `risk.cloud_hosting`, `risk.non_residential`, `evidence.cloud_provider_cidr`
Tor exit node	`185.220.101.1`	`decision=block`, `risk.tor_exit`, `risk.anonymous_network`, `anonymization.is_tor=true`
Public blocklist hit	`130.12.44.211`	`decision=block`, `risk.public_blocklist_hit`, `risk.high_abuse_likelihood`
Exposed server ports	`45.33.32.156`	`decision=review`, `risk.server_exposed`, `evidence.open_server_ports`
C2 / malicious IOC hit	`198.51.100.66`	`decision=block`, `risk.malware_ioc`, `risk.c2_infrastructure`, `evidence.public_threat_ioc`
Open SOCKS5 proxy	`198.51.100.77`	`decision=block`, `risk.open_proxy`, `evidence.socks5_proxy_confirmed`
HTTP proxy and SOCKS exposed	`198.51.100.88`	`decision=block`, `risk.open_proxy`, `risk.proxy_density_high`, `evidence.http_and_socks_open`
High proxy density in subnet	`198.51.100.89`	`decision=block`, `risk.proxy_density_high`, `evidence.subnet_proxy_density`
Public service TLS certificate	`93.184.216.34`	`decision=review`, `risk.server_exposed`, `evidence.ca_tls_certificate`

Scenario	Sample IP	Main API Return
IP certificate / lab-like setup	`198.51.100.24`	`decision=review`, `evidence.ip_certificate`, `risk.low_residential_confidence`
Mail server / SMTP exposed	`198.51.100.25`	`decision=review`, `risk.mail_server`, `evidence.smtp_service_exposed`
Home broadband	`198.51.100.31`	`decision=allow`, `risk.none`, `evidence.residential_network_prior`
Mobile network / CGNAT signal	`100.64.12.34`	`decision=allow`, `evidence.mobile_or_cgnat_network`, `trust.residential_probability=high`
RPKI invalid or routing anomaly	`198.51.100.44`	`decision=review`, `risk.routing_anomaly`, `evidence.rpki_invalid`
Location and network path mismatch	`198.51.100.55`	`decision=challenge`, `risk.geoip_mismatch`, `evidence.latency_geo_mismatch`
Fast IP churn / unstable history	`198.51.100.56`	`decision=challenge`, `risk.ip_churn`, `evidence.history_churn_fast`
Scanning behavior observed	`198.51.100.99`	`decision=block`, `risk.honeypot_observed_scan`, `evidence.honeypot_observation`
Home broadband proxy sample	`198.51.100.108`	`decision=block`, `risk.residential_proxy`, `evidence.proxyware_signature`
High-risk service fingerprint	`198.51.100.109`	`decision=block`, `risk.c2_infrastructure`, `evidence.jarm_high_risk_match`
IPv6 home broadband prefix pattern	`2001:db8:100:200::42`	`decision=allow`, `evidence.ipv6_residential_pattern`, `trust.residential_probability=high`

Example 1: Public DNS / Anycast Infrastructure

Customer request:

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

API response:

```
{
  "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"
  }
}
```

Example 2: Tor Exit Node

Customer request:

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

API response:

```
{
  "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"
  }
}
```


Example 3: Public Blocklist Hit

Customer request:

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

API response:


```
{
  "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"
  }
}
```


Example 4: Cloud Provider Range

Customer request:

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

API response:


```
{
  "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"
  }
}
```

Example 5: Exposed Server Ports

Customer request:

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

API response:

```
{
  "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"
  }
}
```


Example 6: Open SOCKS5 Proxy

Customer request:

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

API response:


```
{
  "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"
  }
}
```