Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Geo-blocking in context

Realities, risks and recommendations

Content complexity
MODERATE

Table of contents

Executive summary

Occasionally, public commentary on cybersecurity incidents refer to the apparent location of network traffic, based on Internet Protocol (IP) addresses. While this data can help with initial threat detection and analysis, it can't reliably indicate the intent, identity, or origin of malicious activity.

In cybersecurity incidents, technical indicators like IP addresses must be considered in context. They may point to infrastructure used in an attack, but not necessarily who is responsible for the attack.

The purpose of this publication is to provide decision makers with an overview of geographical-based IP blocking – also known as geo-blocking. Geo-blocking refers to deny listing or blocking network traffic based on the geographical assignment of IP addresses. It also emphasises the limitations of geo-blocking and the importance of applying layered measures to reduce the risk of blocking legitimate users.

Audience

This guidance is intended for decision makers and cybersecurity practitioners. It highlights what to be aware of when identifying the source of a threat and the potential implications of geo-blocking in a broader cybersecurity strategy.

Attribution in practice

Identifying and assessing malicious activity involves technical investigation, contextual analysis, and information sharing. Rarely is it based on a single data point, such as an IP address or domain name.

While IP addresses, domain names and network logs provide valuable leads, they can also be intentionally manipulated or misrepresented. Malicious actors frequently use techniques such as virtual private networks (VPNs), anonymisation services, and compromised infrastructure to conceal their identities and location.

Cybersecurity practitioners should rely on a layered approach, drawing on a combination of indicators, behavioural patterns and cross-validated information when assessing cyberthreats. This methodology helps ensure conclusions are accurate, balanced, and reflects the broader context rather than being based on isolated or potentially misleading signals.

An IP address is not a GPS coordinate

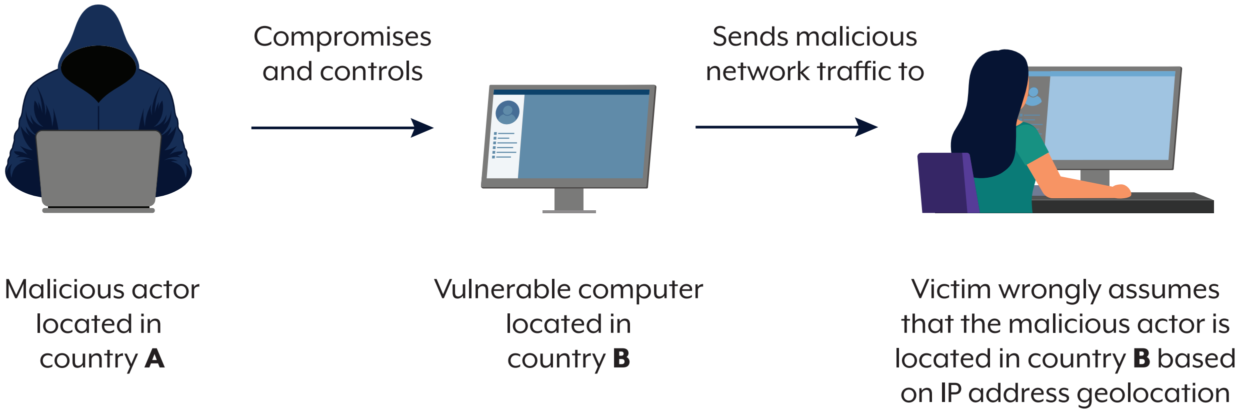
An IP address is a unique identifier assigned to a device that is connected to a network, allowing it to communicate with other devices. For example, **192.168.0.1** is an IP address.

While IP addresses are generally distributed by region, they are not fixed to a specific location or individual.

There are many reasons an IP address may appear to originate from one country while the individual or system behind it is elsewhere:

- Traffic may be routed through a VPN or The Onion Router (Tor) exit node.
- The IP address may belong to a cloud service provider with global customers.
- Thousands of users may share a single IP address due to carrier-grade network address translation.
- The device may be part of a botnet or otherwise compromised without the owner's knowledge.
- In some distributed denial-of-service (DDoS) attacks, IP addresses may be spoofed.

These factors make IP addresses unreliable indicators of origin or identity.


Compromises and controls
Sends malicious network traffic to
Malicious actor located in country **A**
Vulnerable computer located in country **B**
Victim wrongly assumes that the malicious actor is located in country **B** based on IP address geolocation

Using IP reputation services and geolocation tools

Some organisations might exclusively consider commercial IP reputation services as validation toward geo-blocking a location. These services assign risk scores to IP addresses based on whether an IP address is linked to suspicious activity such as VPN use, proxies, botnets, or previously observed malicious behaviour. This reputation score or risk rating can assist cybersecurity practitioners in making decisions that are more informed based on historical data, behavioural patterns, and threat intelligence.

However, IP reputation services should not be solely relied upon. Reputation can quickly become outdated or inaccurate, leading to false positives or false negatives, blocking legitimate users, or missing actual threats.

Incident responders might use a public record listing, such as WHOIS, to obtain basic information about an IP address that is contributing to an attack. This might include the country and organisation assigned to the IP address. These domain query tools offer a quick and accessible way to assess incoming traffic, identify patterns and inform immediate decisions. For example, they could assess if geo-blocking is an appropriate short-term mitigation strategy.

However, this approach has the same risks in misattribution and inefficiencies.

To be most effective, IP reputation services and public IP geolocation tools should be incorporated into a broader threat intelligence platform that aggregates many sources of information.

Benefits and risks of geo-blocking

As with other cybersecurity mitigations, there are many benefits and risks to using geo-blocking. Decision makers and cybersecurity practitioners should understand the potential benefits, risks and outcomes when considering implementing geo-blocking.

Potential benefits

Reduces malicious and non-operational traffic

Geo-blocking can reduce the volume of inbound traffic and log noise from regions with no direct business relevance, therefore lowering the exposure to malicious attacks and increasing the likelihood that malicious activity will be identified.

Enhances defensive posture

Applying geolocation limitations to the network perimeter serves as an additional access control layer that enforces restrictions based on a geographic location. It helps reduce exposure by filtering traffic from regions where no trusted users are expected to connect. This complements access controls such as authentication and encryption.

Potential risks

When considering geo-blocking, be aware of the potential for unintended consequences and inefficiencies when implemented as a standalone control. Some limitations and inefficiencies include the following:

- Legitimate users, such as travelling individuals or expatriates, may be inadvertently blocked from services when they have a genuine need.
- Malicious actors can easily bypass geographic restrictions using VPNs or proxy services.
- Threats may emerge from within the permitted region through compromised local devices.

Locked, stocked and geo-blocked - a hypothetical case study of unintended consequences

Taylor, an Australian citizen travelling overseas on holiday, attempted to log into her bank portal to check her balance. Unexpectedly, she could not access the bank's website.

The bank had recently temporarily implemented geo-blocking to mitigate attacks against the bank's website that mostly originated from overseas. The foreign IP address used by Taylor's computer was automatically blocked due to the geo-blocking.

This situation affected multiple customers, causing an influx of phone calls to the bank. Customers who were impacted also started to voice their frustrations on social media. The bank's IT and security staff attempted to manually verify customer identities and implement exceptions to allow access to the bank's website from specific foreign IP addresses used by customers. This exception process was time consuming, imperfect and unsustainable due to the number of affected customers and their IP addresses changing over time.

This case illustrates how geo-blocking, if not implemented with exception handling or user-aware policies, can disrupt legitimate use cases. Organisations should carefully assess the operational impacts of geographic restrictions, especially when critical services may need to be accessed globally.

If geo-blocking is implemented, it should be applied as part of a defence-in-depth approach to cybersecurity strategy. Decision makers should take a risk-based approach and consider their organisation's operational requirements, including where users, partners or systems legitimately operate. Cybersecurity practitioners should monitor the implementation for unintended consequences.

Geo-blocking and denial-of-service attacks

Network defenders of an Australian online service, might reduce DoS attack exposure by geo-blocking traffic originating outside Australia.

What is denial-of-service (DoS)?

Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks are cyberattacks designed to disrupt or degrade online services such as websites, email, and Domain Name System (DNS) services, to deny access to legitimate users.

This is typically achieved by flooding an online service with data, connections or requests to overwhelm the service and degrade its functionality. A DDoS attack uses multiple devices – often part of a botnet – to launch the attack from many sources at once.

Learn more about DoS attacks:

Preparing for and responding to denial-of-service attacks

While geo-blocking can reduce the volume of malicious traffic, DoS traffic may not originate overseas. Geo-blocking may also impact legitimate users that are temporarily outside Australia, such as travelling customers and staff.

Malicious actors located outside of Australia can use a range of techniques to make their activity appear as if it originates locally.

Malicious techniques include:

- using Australian-based VPNs or Tor exit nodes to mask their true location
- leveraging cloud service providers that assign IP addresses registered to Australia
- exploiting local infrastructure in reflection attacks, such as sending DNS requests to Australian-based resolvers, causing response traffic to be directed at a victim's service
- using source IP address spoofing through volumetric attacks, such as Network Time Protocol amplification and DNS amplification (T1498.002) that can alter the IP address
- compromising devices with Australian IP addresses to launch attacks from within the country, such as:
  - Internet-of-Things (IoT) devices
  - Small Office/Home Office (SOHO) routers
  - laptops or personal computers
  - virtualised systems in cloud environments
  - network edge devices, such as firewalls or gateways.

These methods allow malicious activity to bypass geo-blocking by appearing domestic. As a result, IP geolocation alone should not be relied on to assess the legitimacy or origin of network traffic.

Botnets in the backyard – a hypothetical tale of geo-blocking inefficiency

Dawn operates a popular Australian e-commerce platform and recently implemented geo-blocking to reduce exposure to persistent malicious traffic originating from overseas. The control successfully reduced direct threats from several high-risk regions.

However, a sophisticated threat actor adapted quickly. Instead of launching attacks from overseas, they compromised poorly secured IoT devices located within Australia, such as smart cameras and home routers. The malicious actor then used these devices to build a local botnet, and initiated a DDoS attack against Dawn's platform.

Because the malicious traffic originated from within Australia, it was not blocked by the geo-blocking rules. The attack caused significant disruption, prompting Dawn to review her organisation's cybersecurity strategy.

This case illustrates how geo-blocking alone can't defend against all threats, particularly when attackers exploit infrastructure inside the allowed region. A layered security approach – incorporating network monitoring, anomaly detection, device hardening, and DDoS mitigation – is essential for providing comprehensive protection.

Recommendations

Geo-blocking may be appropriate in certain scenarios, but it should be implemented as part of a layered and risk-based approach. Consider the following best practices when building multiple layers of cybersecurity to protect business operations:

- Evaluate geo-blocking impacts to the service's user base and business model.
- Use IP reputation data and public IP geolocation tools to inform, but not dictate, access decisions.
- Use rate limiting, anomaly detection and behavioural monitoring to identify suspicious activity.
- Implement cloud-based DoS protection (if relevant) for scalability and resilience.
- Segment network traffic and isolate high-risk edge, or externally facing, devices.
- Keep firmware and software up to date across exposed systems.
- Replace end-of-life (EOL) equipment and monitor for unusual access patterns.
- Use phishing resistant multi-factor authentication, replace default passwords with strong passwords or passphrases, and disable password hints.

Conclusion

IP addresses and geolocation data are useful signals in cybersecurity investigations, but they are only one piece of the puzzle. Whether considering attribution or access control through geo-blocking, organisations should avoid relying on IP address geolocation alone.

A considered, context-driven approach helps ensure that cybersecurity decisions are informed, proportional and effective, while reducing the risk of misinterpreting intent and causing disruption to legitimate users.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre