Limiting the Use of Port Blocking Advances Internet Neutrality

by Alissa Cooper [1]
August 20, 2013

In debates over Internet neutrality, “port blocking” may not be getting the headlines these days, but it was once a more common practice among Internet service providers (ISPs) and is still in use today. A new report [2] from the Broadband Internet Technical Advisory Group (BITAG) , of which CDT is a member, makes a strong recommendation against the practice of port blocking unless no other reasonable alternatives exist. The report discusses alternatives to port blocking for ISPs to consider and other steps to minimize its impact when deployed.

From CDT’s perspective, the report and its recommendations make a significant contribution to the debate about Internet neutrality. Port blocking by its nature discriminates among Internet traffic and often is used to thwart specific applications. Minimizing its use and establishing safeguards for when it does get used therefore help to keep the Internet more neutral and open.

Port Blocking Defined

Internet applications, such as email and web browsing, make use of multiple kinds of address information on the network, including IP addresses and port information, to send data between computers on the Internet. IP addresses and port numbers are analogous to street addresses and apartment numbers – a letter can reach a particular apartment building based solely on street address (the IP address), but an apartment number (the port) is needed for the letter to reach an individual unit in the building.

“Port blocking” refers to the practice of an ISP identifying Internet traffic by its port number (and some information about the transport protocol in use) and blocking it from reaching its destination – as if it were sifting through the mail and trashing letters destined for a particular apartment number. Because certain port numbers are often used by particular applications, port blocking can potentially prevent the use of particular applications altogether.

Port blocking has a variety of uses and those uses have changed over time. One of the original and enduring motivations for port blocking is to prevent network attacks and abuse associated with particular application protocols whose designs are insecure. For example, some operators block TCP port 25, which can be used to send email, because it lacks security features to prevent abuse by spammers. Similarly, some operators block ports associated with application protocols that have been exploited by worms and other network attacks over the years.

Port blocking has also been used to enforce ISPs’ terms of service, including terms that prevent the hosting of web servers, as described above. Port blocking was once viewed as a useful tool for managing capacity and bandwidth-intensive applications such as peer-to-peer file-sharing applications. However, increased network capacity and more sophisticated application designs have caused most residential ISPs to seek other ways of managing capacity. Port blocking has also been used to hinder competing applications, such as when the ISP Madison River used port blocking in 2005 to prevent access to Voice over IP services [3].

Effects of Port Blocking on Applications and Users

Because of the tight coupling that some applications have to specific ports, port blocking can complicate application design and development and create uncertainty about whether applications will function properly. Port blocking can cause applications to “break” by preventing applications from using the ports they were designed to use. Application developers have responded by using randomized, unpredictable ports, or by using a very limited set of ports that are highly unlikely to be blocked. In general blocking ports does not cause applications to vanish from the Internet, but rather

induces a cat-and-mouse game whereby application development becomes increasingly complex to evade blocked ports.

It may not be obvious to Internet users why an application affected by port blocking is not working properly, because the application may simply be unable to connect or fail silently. Users may seek assistance from the ISP's customer service, online documentation, or other knowledgeable sources if they cannot diagnose the problem themselves, but users' ability to respond to port blocking depends on their technical sophistication and the extent to which workarounds are available.

Recommendations

BITAG recognizes that there can be security benefits to port blocking, but that overall it can also have detrimental effects for users, application developers and the Internet ecosystem. Its recommendations emphasize the limited use of port blocking and the need to facilitate user choice and support in the event that ISPs do choose to block ports. Specifically:

- ISPs should avoid port blocking unless they have no reasonable alternatives available for preventing unwanted traffic and protecting users. If port blocking is deemed necessary, it should only be used for security purposes. Port blocking should not be used for ongoing capacity management, to enforce non-security terms of service, or to disadvantage competing applications.
- ISPs that can reasonably provide to their users opt-out provisions or exceptions to their port blocking policies should do so.
- ISPs should publicly disclose their port blocking policies. • ISPs should make channels available to communicate with applications providers and users about the effects of port blocking.
- ISPs should revisit their port blocking policies on a regular basis and reassess whether the threats that required the port blocking rules continue to be relevant.
- When port blocking is implemented in a home router or other consumer device, port blocking rules should be user-configurable.

In an ideal world, the full space of ports would be available to every Internet application. In reality, some operators may view port blocking as a necessary evil. By following BITAG's recommendations, ISPs can minimize the harmful effects of port blocking on applications and users.

Copyright © 2013 by Center for Democracy & Technology.
The content on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL:
https://cdt.org/blogs/alissa-cooper/2008limiting-use-port-blocking-advances-internet-neutrality

Links:
[1] https://cdt.org/personnel/alissa-cooper
[2] http://www.bitag.org/documents/Port-Blocking.pdf
[3] http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf