

What is Anti-P2P?

A peer-to-peer (or P2P) computer network is a network that relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers. P2P networks are typically used for connecting nodes via largely *ad hoc* connections. Such networks are useful for many purposes. Sharing content files containing audio, video, data or anything in digital format is very common, and real-time data, such as telephony traffic, is also passed using P2P technology.

A pure peer-to-peer network does not have the notion of clients or servers, but only equal *peer* nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client-server model where communication is usually to and from a central server.

The problem with this is that most of the content is copyrighted and a financial claim can be raised for the downloaded and or shared copyrighted materials.

In some countries the ISP will even close down your internet connection and this can be a big loss if you suddenly loose your internet connection or get a law suit.

Further more the downloading of high amount of content can slow down your internet connection preventing legitimate traffic to pass.

How can P2P be prevented?

In most cases there is a wish to the use of P2P in their own network, but today it is hard to stop this misuse of the company's recourses due the fact that many P2P applications use port 80. This port is also use for web browsing so can not be blocked by a firewall The SecPoint Protector Anti-P2P functionality takes care for this problem and give you the option to completely block those services and programs.