What is P2P?

Peer to peer (P2P) technologies denote a type of application communication architecture that allows individuals to communicate and share data with other individuals without necessarily needing a central server to facilitate the communication. It is important to note that "P2P" refers to a type of application architecture and not a specific end application functionality; i.e. P2P is a technical means to a some greater end. However, "P2P" is often used synonymously to mean "file sharing", as that is one very popular use of P2P technology. There are other application purposes beyond file sharing that leverage P2Pfor example, Skype uses a hybrid P2P architecture to provide VoIP services, and Tor uses a P2P architecture to provide anonymous network routing functionality.

The primary advantage of a P2P approach is that it leverages the resources (e.g. bandwidth, storage, etc.) of the many clients/peers to provide the overall application and network services rather than relying on the resources of one or more central serversthus preventing those central servers from becoming a bottleneck for the entire network. A secondary advantage of a P2P approach is that there is no single central authority that can be blocked or removed and cause the collapse of the whole P2P network; this provides a certain "self-surviving" and robustness quality that may be desired for various reasons.

Figure 1 Traditional client/server network[1]

Figure 2 - P2P network[1]

P2P Threats

P2P applications in use within an enterprise network can pose many threats and concerns:

- **Data leakage**: corporate information or files are knowingly or unknowingly being uploaded
- **Copyright infringement**: users are downloading illegal/copyrighted content
- **Resource consumption**: excessive bandwidth consumption, including potential extra bandwidth consumed while servicing other peers not related to direct user use
- **Access control enforcement**: the decentralized nature of P2P technologies make it difficult to utilize traditional network access control mechanisms to block usage

[1]Http://en.wikipedia.org/wiki/Peer-to-peer

- **Data retention**: properly logging and auditing P2P communication data can be difficult to impossible
- **Malware**: virus, Trojans, or other malware could potentially be downloaded by the user
- **Time ineffectiveness**: time spent using P2P applications is time not spent working

---

The Zscaler Solution

The Zscaler solution can identify various popular P2P applications. Once identified, a location's policy can dictate whether specific P2P traffic types are allowed, blocked, or throttled by a bandwidth limitation. As of Q3/2008, the Zscaler solution offers support for the following P2P applications:

- **Gnutella/Gnutella2**: file sharing networks used by the popular Limewire and BearShare clients.
- **BitTorrent**: file sharing method that relies on certain web sites (called “trackers”) to index all peers that have pieces of a certain file; there are many popular BitTorrent clients available on the Internet.
- **Pando:** a single-vendor commercial and proprietary derivative of BitTorrent that is friendlier to use over HTTP.
- **eDonkey:** file sharing network used by the popular eMule client.
- **Skype:** a single-vendor commercial and proprietary VoIP network.
- **Tor:** an anonymous routing network used to hide where a user is coming from and where they are going to.

Related Media Coverage

- “Alluring MP3s, movies hit Limewire, install malware instead”
  http://arstechnica.com/news.ars/post/20080508-alluring-mp3-movies-hit-limewire-install-malware-instead.html
- “Malware infects Bit-Torrent downloads”
  http://arstechnica.com/news.ars/post/20050617-5007.html
- “Walter Reed Breach might be due to P2P software”
  http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=45&rss=Y#sID301
- “Man busted for using P2P to steal identities of file-sharers”
  http://arstechnica.com/news.ars/post/20070907-man-busted-for-using-p2p-to-steal-identities-of-dozens-of-file-sharers.html