

Controlling Peer to Peer (P2P) Traffic

A Compliance Solution for the Higher Education Opportunity Act

Overview

As institutions of higher learning, colleges and universities need IT to provide users with open access to an increasing array of network resources. IT must balance the requirement of providing an open, collaborative learning environment with the need to protect students, faculty, administration, guests and IT systems from an ever-increasing variety of risks. The network communication technologies that have accelerated collaboration and learning are also being used by Peer to Peer (P2P) applications for the illegal distribution of copyright-protected content. Providing visibility and control for the traffic that traverses the university's network becomes extremely important when trying to balance the need for open access while ensuring compliance and network security.

While many might argue that P2P has legitimate use on campus, a study of Internet usage done by Envisional and posted on the MPAA [website](#) found that that many uses are not legal, and this represents real risk for the university and its systems.

“Approximately 23.8% of global Internet traffic is infringing, with bit torrent specifically accounting for almost half of that amount (representing 11.4% of global Internet traffic)...Of the top 10,000 found ... excluding pornography, only one swarm in the top 10,000 offered legitimate content and 99.24% of all material in the top 10,000 swarms was copyrighted.”

– Technical Report: An Estimate of Infringing Use of the Internet — Summary, Envisional, January 2011

Copyright infringement is a problem that has drawn the attention of legislators, and over the past year received enough attention to become a regulatory issue for higher education networks.

This paper will discuss the Higher Education Opportunity Act, how it impacts higher educational institutions and how Enterasys can provide technology solutions to control Peer to Peer traffic while reducing the cost and complexity of managing the infrastructure.

The Higher Education Opportunity Act (HEOA) — Now In Effect

HEOA requires colleges and universities that participate in any Title IV, HEA programs to meet the act's requirements for combating the unauthorized distribution of copyrighted material by users of an institution's network. The act requires institutions to take steps to combat the unauthorized distribution of copyrighted materials through illegal downloading or peer-to-peer distribution of intellectual property. These [regulations](#) went into effect July 1, 2010.

Based upon HEOA regulations, an institution must include comply with the following rules:

- The use of one or more technology-based deterrents
- Mechanisms for educating and informing its community about appropriate versus inappropriate use of copyrighted material
- Procedures for handling unauthorized distribution of copyrighted material, including disciplinary procedures

Solution Benefits

Increases compliance

- Reduces complexity and risk by embedding active, automated security into the network fabric
- Improves security and compliance by mapping acceptable use policy to network implementation
- Increases compliance policy enforcement options

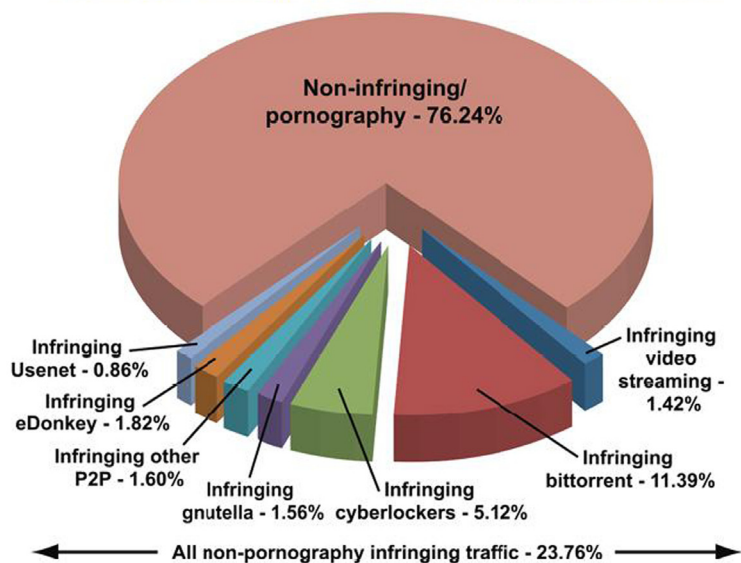
Lower operational costs

- Lowers the cost of responding to security and compliance events through automated response options

- Procedures for periodically reviewing the effectiveness of the plans to combat the unauthorized distribution of copyrighted materials by users of the institution's network using relevant assessment criteria

It is left to each institution to determine relevant assessment criteria. No particular technology measures are favored or required for inclusion in an institution's plans, and each institution retains the authority to determine what its particular plans for compliance will be.

Estimate of infringing use of global internet bandwidth



Source: Technical Report: An Estimate of Infringing Use of the Internet – Summary, Envisional, January 2011

Controlling P2P Traffic

To meet the challenge of controlling P2P traffic and providing a secure networking environment, higher learning institutions must deploy technologies that enable the enforcement of the institution's policies regarding the use of the network and distribution of content across that network. Institutions gain cost efficiencies when the technology chosen also functions to predict, prevent and automatically respond to other threats such as worms, viruses and spyware.

Enterasys provides key networking and security solutions that address peer-to-peer file exchange legal liability issues, and can also be leveraged to solve other network security challenges. Enterasys provides detection and control capabilities by embedding security technologies directly into the network fabric to respond to threats proactively, increase operational efficiency, reduce deployment complexity, and scale as the network expands over time. Security is no longer just bolted on, but pervasively integrated throughout the wired and wireless infrastructure.

Dealing with P2P Compliance

Solutions that address P2P compliance need two basic elements. The first element detects a user running a P2P application and the second element enforces the university's acceptable use policy.

Detection

Enterasys solutions provide three ways to detect users running P2P applications:

1. A Network Access Control (NAC) agent can be configured to detect P2P applications running on a user's computer
2. Enterasys IPS P2P signatures can be deployed to detect P2P packets as they traverse the network
3. Enterasys Security Information & Event Manager (SIEM) can use behavior-based analytics to detect P2P flows

Enforcement

Enterasys P2P solutions can be configured with a wide range of enforcement options ranging from logging the event and warning the user of the consequences of illegal file sharing to dropping P2P traffic and suspending a chronic offender's network access. In addition to detecting P2P applications, Enterasys provides two solutions for controlling P2P traffic on the network.

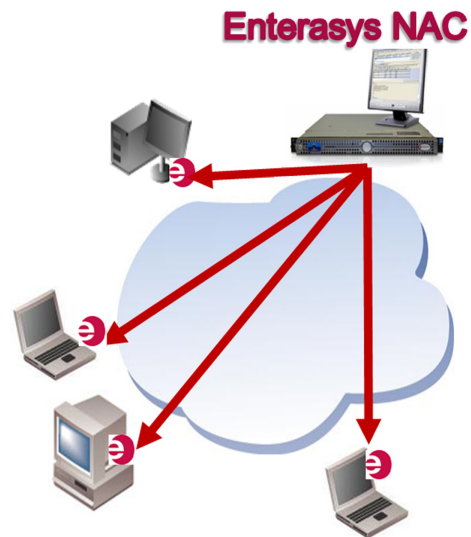
Solution Flexibility

Enterasys provides institutions with the ability to address compliance with HEOA in controlling P2P and its use within the campus network. Solution 1 focuses on whether or not an end-user can run P2P applications on their systems. Solution 2 focuses on using detection technologies to monitor how P2P is being used. While the solutions take different approaches to the problem, they provide flexibility to the institution in determining how to implement controls that are in line with the institution's culture.

Network Access Control (NAC)

The Enterasys NAC assessment agent solution can be configured to detect P2P programs on end user systems. The first time the user authenticates onto the network, an assessment agent is downloaded onto the user end system. The agent runs in the background and can be configured to detect P2P programs. When an unapproved program is detected the agent can be configured to terminate the program and report the activity or allow the program to continue and provide a report to network administrators.

Case Study — A major U.S. university uses the Enterasys NAC solution to deal reactively with the problem of students using P2P programs. The university network sees about 65,000 unique connections per day and their approach to enforcement relies entirely on voluntary compliance. When a P2P application is detected on a user device, the user is presented with a pop-up informing him/her of the hazards and legal consequences of illegal file-sharing. After the warning has been given and acknowledged, it is left up to the user to decide if he/she wants to continue using the program. The goal of the solution is to inform users who may be unaware of the hazards and consequences of illegal file sharing. This university has been recognized by the student and local newspapers as offering a good solution to addressing peer-to-peer compliance while matching the culture of personal responsibility and growth fostered by the university.



The advantage of the Enterasys NAC solution is that with one product deployed, a diverse range of responses are available through fine-grained configuration options. At the same time, NAC provides a range of additional capabilities for lowering risk and protecting the network against threats originating from infected or unsecured systems.

Distributed Intrusion Prevention

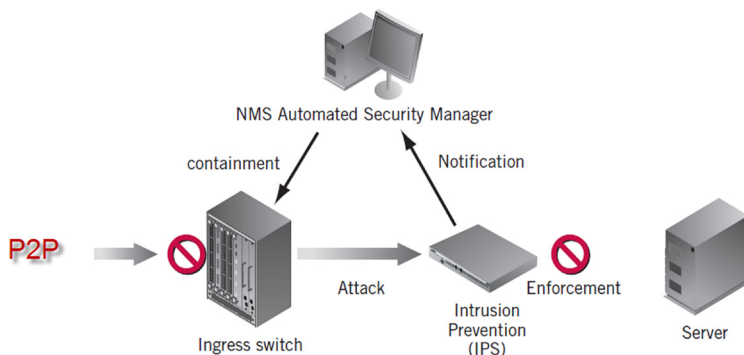
The Enterasys patented Distributed Intrusion Prevention System (IPS) P2P solution uses IPS or Network Based Anomaly Detection (NBAD)/SIEM to detect the presence of P2P traffic on the network and Enterasys Network Management Suite (NMS) software to provide enforcement. When unauthorized P2P traffic is detected, the IP address of the local user is sent to the management console for remediation. The management console locates the infringing system on the network port and the user credentials (optional action) of the person using the P2P program are identified.

A wide range of automated responses can be configured based on the institution's philosophy. Some options include:

- Quarantining the user to limited network access
- Warning the user that they are in violation of university policy
- Rate limiting the user's traffic

The advantage of the Enterasys Distributed IPS solution is that multiple network segments can be monitored with fewer devices than competitive IPS solutions, reducing costs, while at the same time providing user accountability.

Case Study — A large U.S. university uses the Enterasys IPS solution to proactively control unauthorized P2P traffic. Students are offered a licensed service as an alternative to illegal file sharing services. The university has leveraged their IPS system to detect P2P traffic. If unauthorized P2P traffic is detected, the user is redirected to a warning page via web intercept and informed of the potential violation. After acknowledging the warning, the user is granted Internet access. Violations are tracked and reported on. After the third incident the user's network access is suspended pending administrative review. There are very few students that incur three violations in a semester, as the warning and a legal alternative are enough to assist students in making good choices.

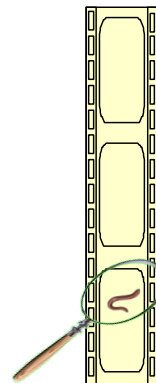


Privacy Concerns

Many higher education institutions struggle with balancing the privacy of students with compliance and security requirements. Enterasys solutions can be configured to monitor protocols, applications and content either separately or all three at the same time. One institution might consider the use of a peer-to-peer protocol a violation of policy, while another might allow the protocol but inspect the content. The monitoring and detection options are flexible to meet the established acceptable use policies of each institution. Additionally the Enterasys solutions can be configured to log and report on as much or as little of the data, user credentials or location of the event as the institution requires for its compliance auditing efforts. Enterasys delivers a flexible and open architecture to automatically sense and respond to a variety of network security threats.

Conclusion

Enterasys switches, IPS, SIEM, NAC and NMS network management applications have been built with embedded security features that enable sophisticated threat isolation and resolution. They are the ideal complement to the firewall, packet inspection and patch management protections already deployed in most higher education networks. Enterasys solutions are unique in their ability to automate the critical process of locating the exact source of a detected security violation and enabling the appropriate response. For higher education institutions this results in a robust compliance solution for mandates such as HEOA.



Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

