

Application Visibility and Control For K-12

When URL Filtering is Insufficient to Control Student Activities



Technologies Students Use to Circumvent IT Controls

A few examples of the different types of applications that students can use to bypass traditional security detection mechanisms.

Proxy Services – online services that enable students to bypass detection and control.

- KProxy
- Avoidr
- PingFu

Proxy applications – installable on home computers, enabling students to bypass detection mechanisms.

- CGI-Proxy
- PHProxy
- ASPProxy

Tunneling Applications – encrypted applications that are designed to bypass security.

- TOR
- Hopster
- UltraSurf
- Hamachi

Palo Alto Networks identifies more than 600 applications including 20 different proxies and anonymizers, 12 encrypted tunneling applications and more than 40 applications that use evasive P2P technology. For a complete list, please browse the Applipedia at <http://ww2.paloaltonetworks.com/applipedia/>.

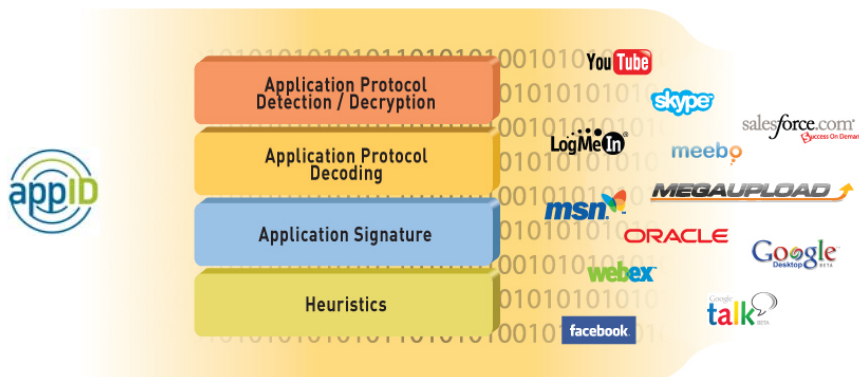
The Problem: Students Actively Bypassing Security Controls

Students are using new class of internet application that is capable of circumventing existing security mechanisms such as firewalls, URL filtering and proxy servers. As a result, K-12 IT departments are placed in a difficult position. State and Federal regulations, school board policies, community standards, and common sense dictate that schools filter applications and Internet traffic that can make its way to students' eyes and ears. But this new class of applications which includes proxies and anonymizers that facilitate evading detection are readily available and students are incredibly adept at using them in K-12 environments. The conventional approach to solving this problem include deploying a URL database in conjunction with a traditional network firewall, but this approach simply can't keep pace with these nimble, network-savvy applications.

The Solution: Application Visibility and Control

The solution is to regain visibility and control of all application traffic going out to the Internet with a Palo Alto Networks next generation firewall. Whether it be browsers going to websites, browsers going to encrypted proxies students have set up, tunneling applications, or a variety of anonymizers, Palo Alto Networks can help K-12 IT departments regain visibility into, and control over the applications traversing the network.

At the heart of the Palo Alto Networks next-generation firewall is App-ID™, a patent-pending traffic classification technology that uses four different techniques to identify and classify applications, going well beyond any other network security technology available. App-ID inspects all of the traffic passing through the firewall, one or more of these techniques – including application protocol detection and decryption, application decoding, application signatures, and heuristic analysis – to quickly identify the specific application associated with each packet stream.



Application Visibility and Control For K-12

When URL Filtering is Insufficient to Control Student Activities



With increased visibility into the actual identity of the application, administrators can deploy comprehensive, policy-based application usage control for both inbound and outbound network traffic. With App-ID, IT can now:

- Improve network visibility by accurately identifying application traffic irrespective of port and protocol.
- Enhance security by dictating access rights based upon the actual application traffic as opposed to simply the port and protocol.
- Enable deployment and enforcement of appropriate application usage policies.
- Increase malware threat detection and prevention effectiveness

Whereas traditional port-based solutions use a single classification technique to identify traffic, App-ID goes well beyond any other network security technology available, to accurately identify the application—even those that use evasive tactics such as SSL encryption, port hopping and emulation.

More About Palo Alto Networks

Starting with a blank slate, Palo Alto Networks produced a next-generation firewall that brings visibility and control over applications, users and content back to the IT department using three unique technologies: App-ID, User-ID and Content-ID. Delivered as a purpose-built platform, Palo Alto Networks next generation firewalls differentiates itself from traditional firewall vendors in the following ways:

- The only firewall that delivers policy-based application visibility and control over more than 600 applications irrespective of port, protocol, SSL encryption or evasive tactic employed.
- The only firewall that enables policy enforcement based on the application, the category or subcategory, the underlying technology and the behavioral characteristic (file transfer capabilities, whether it has had any known vulnerabilities, its ability to evade network security detection, the propensity to consume bandwidth, and capacity to transmit/propagate malware).
- The only firewall that ties policy control seamlessly to user and group information within Microsoft Active Directory (AD).
- The only firewall that melds stream-based scanning, a uniform threat signature format, and a comprehensive URL database with elements of application visibility to limit unauthorized file transfers, detect and block a wide range of threats and control non-work related web surfing.
- The only firewall with function-specific processing for networking, security, content inspection and management, resulting in line-rate, low-latency performance for all services, even under load.

Get the control you need, without slowing down the network – or your instructional technology. Contact your local Palo Alto Networks representative now.

Education Customer Examples

