

# Blue Reef Biz Talk

## Anonymous Proxy – what is it, what are the implications and how can you combat it?

### What is an “Anonymous Proxy” and how can it affect me as a School Principal under my Duty of Care obligations?

#### Bypassing School Browsing Controls

---

Over the past few years schools have moved from operating in simple IT environments to becoming small Internet Service Providers, enabling students to access the internet for educational purposes.

The question of how to prevent students accessing inappropriate, and in some cases, illegal content is of constant concern. The most common solution uses filtering software to try to ensure appropriate internet usage. Filtering software checks all requested websites against a known blacklist of nefarious sites and blocks all requests that are deemed inappropriate.

As increasing numbers of students look for ways to bypass school-mandated filtering policies, unregulated commercial bypass enterprises have begun offering paid services that provide students with a series of constantly changing website addresses that are not on the blacklist.

Once a student pays the fees (many sites are “free” but often contain viruses and malware), all traffic from the student’s computer goes to these so-called “legitimate” websites. From there the web request is tunnelled to restricted sites enabling access to inappropriate content on school premises, in an undetected and anonymous way. This technique is known as filter evasion by “anonymous proxy”.

An interesting conundrum presents itself to the education community:

1. Can we afford not to act when students are using school equipment to bypass our duty of care policy for inappropriate content?
2. How can we educate parents and custodians not to allow students to pay for or subscribe to these services?

#### Challenges

---

The challenges schools face can be divided into three groups: Governance, Policy Management, and Enforcement Technology. Schools need to ask the following important questions:

##### **Governance:**

1. Does the school’s Acceptable Usage Policy cover this new paradigm?
2. Does the school communicate effectively with custodians and parents about the implications of allowing students to pay for these services, including the potential side-effects such as virus infection, disclosure of sensitive information and cyber-stalking?
3. What remedies can the school take in the event of such a bypass?

##### **Policy Management:**

1. How can we track these bypass website services, as they keep on changing?
2. What type of website requests can we consider as a bypass?
3. As many of these sites use encryption methods to hide their traffic, do we need to stop access to all/some encrypted content which may also affect access to other legitimate sites such as banking sites?

## Technology Enforcement:

1. Can we use an external source of information listing all these services and include them in our filter?
2. Can we use a rule-based approach in our filter to determine when such a service is being used, and are there any other more effective technologies available to help stop this happening?

## Blue Reef Solution

---

The most commonly used solution to this challenge has similarities to the never ending cycle of law enforcement and crime. The blacklist provider will keep on trying to record all the new service website names, and the service provider will keep on coming up with new ones. Such a cycle is an inefficient and largely ineffective way of dealing with the Anonymous Proxy threat.

The Blue Reef Solution delves deeper into the problem and is consequently much more effective. In addition to checking that the requesting website address is legitimate it looks at the content of the full web request and response. This often reveals that an inappropriate content request is being concealed in the request or the returned response and allows the school to implement its policies to block and educate the user.

## Blue Reef Best Practice

---

Blue Reef is the first choice Internet Management Provider to over 300 educational institutions throughout Australia. We have been assisting schools achieve solutions to issues like Anonymous Proxies for over a decade. Our extensive experience in the development of tools, policies and technologies to address these types of educational needs is unsurpassed.

Blue Reef's holistic approach provides a solution that is more effective because it concentrates on looking into the requests to verify whether they are inappropriate rather than constantly chasing the bypass service providers. Our approach includes:

1. A Bypass Services Acceptable Usage policy document template and parents communications template
2. The Sonar Internet Management Technology appliance for controlling content using:
  - a. **Deep URL and content inspection** to analyse contents of web requests
  - b. Web traffic reporting per user to identify who has been trying to use a bypass service
  - c. The ability to quarantine and slow down a student who has violated the policies.

More information is available at [www.blureef.com.au](http://www.blureef.com.au)

## About the Author

---

Guy Lupo, VP Products & Services, Blue Reef Pty. Ltd. has 20 years experience in governance, compliance and security in the enterprise and education spaces, and is continuously working with educational organisations to improve their processes and supporting technologies to achieve better educational outcomes.

Guy's career history includes strategic product and management roles with worldwide international leaders such as Check Point, CA, Microsoft, Cisco, BMC Software and other start-ups in the Governance, Compliance and Security space.