



## Executive Summary

As the leader in Wide Area Application Delivery, Blue Coat products accelerate and secure applications within your WAN and across the Internet. Blue Coat provides a robust and flexible solution that controls users and network resources, protects against Web-based threats, and accelerates the broadest range of WAN-based applications. Whether deployed on either end of a WAN, at Internet access points, or in front of business-critical services, Blue Coat ProxySG appliances provide control points that stop the bad and accelerate the good. As part of this solution, ProxySG appliances support Data Tricking of ICAP objects while they are being scanned, providing a flexible mechanism for scanning objects.

## What is Data Tricking?

Blue Coat ProxySG appliances implement Data Tricking to improve the user experience during ICAP scanning. Internet Content Adaptation Protocol (ICAP) is the protocol used by Blue Coat ProxySG and ProxyAV appliances, as well as some third party partner appliances, to perform scanning of objects to detect viruses, worms, spyware, and Trojans. Data Tricking is a mechanism implemented by Blue Coat ProxySG appliances performing ICAP scanning that slowly delivers, or trickles, data to the client as it is being scanned. By trickling data, users do not experience the timeouts sometimes associated with waiting for large objects to be scanned, or when scanning is delayed by high loads on content servers or upstream bandwidth limitations.

## Why should I perform Data Tricking in my network?

Blue Coat ProxySG appliances offer two methods of providing feedback to users when virus scanning of an object is in progress – patience pages and data trickling. Patience pages are user-friendly HTML pages displayed to the user, informing them that a scan is in progress. Patience pages, however, are available only in response to Web browser requests. Because the data is not actually sent to the user until the entire object is scanned, a patience page implementation can sometimes result in client applications timing out while waiting for the scan to complete. Data Tricking provides an alternative to patience pages that is better suited to preventing the timeouts that commonly occur when scanning relatively large objects, when scanning objects retrieved upstream over a smaller bandwidth pipe, or when content servers are overloaded. Data Tricking most closely resembles the user experience when scanning is not taking place, and is also a desirable option for use with applications that are not browser-based. Patience pages require that the user is able to display the patience page, but Data Tricking is not limited to Web browser requests and can therefore be ideal for various FTP and HTTP applications.

## How does Data Tricking work?

Data Tricking is designed to prevent the timeouts that can sometimes be associated with patience pages. To prevent such timeouts, Data Tricking trickles – or transmits at a very slow rate – bytes to the client at the beginning of the scan or near the very end. Because the ProxySG appliance begins serving content without waiting for the ICAP scan result, timeouts do not occur. However, to maintain security, the full object is not delivered until the results of the content scan are complete (and the object is determined to not be infected). Two types of Data Tricking are available on Blue Coat ProxySG appliances – trickle from start and trickle at end.

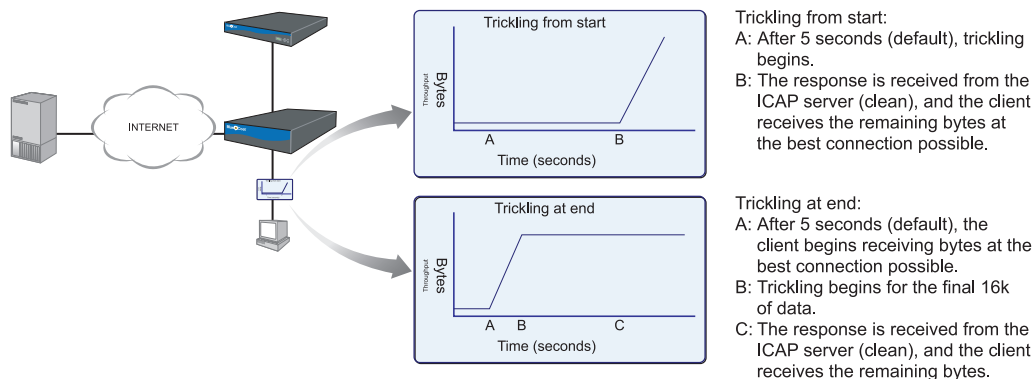


### Trickle from start

In trickle from start mode, the ProxySG appliance buffers a small amount of the beginning of the response body. As the ICAP server continues to scan the response, the ProxySG appliance allows one byte per second to the client. After the ICAP server completes its scan, if the object is deemed to be clean (no response modification is required), the ProxySG appliance sends the rest of the object bytes to the client at the best speed allowed by the connection. If the object is deemed to be malicious, the ProxySG appliance terminates the connection and the remainder of the response object. Trickling from the start is the more secure Data Tricking option because the client receives only a small amount of data pending the outcome of the virus scan.

### Trickle at end

In trickle at end mode, the ProxySG appliance sends the response to the client at the best speed allowed by the connection, except for the last 16KB of data. As the ICAP server performs the content scan, the ProxySG appliance allows one byte per second to the client. After the ICAP server completes its scan, if the object is deemed to be clean (no response modification is required), the ProxySG appliance sends the rest of the object bytes to the client at the best speed allowed by the connection. This method is more user-friendly than trickle at start. This is because users tend to be more patient when they notice that 99% of the object is downloaded versus 1%, and are less likely to perform a connection restart. However, network administrators might perceive this method as the less secure method, as a majority of the object is delivered before the results of the ICAP scan.



*Trickling is available in two types – trickling from start and trickling at end*

## The Blue Coat Difference

### Multi-Vendor Support

Blue Coat ProxySG appliances support multiple Web virus scanning vendors to provide administrators with the flexibility to choose the vendor that best addresses the area(s) of concern of the enterprise. Blue Coat Web virus scanning partners provide protection against viruses, spam, adware, malware, Trojans, and provide intrusion prevention.

### Scanning of Secure Content

Blue Coat Systems provides the only solution able to effectively scan secure (HTTPS) content. Without the ability to scan secure content, a virus scanning solution can only guarantee protection of insecure content, leaving a significant security hole that makes the value of the overall solution questionable.