

Web Security for the Enterprise:

How to increase protection against port 80 threats

White Paper

Web Security for the Enterprise

Table of Contents

Summary	3
Introduction	4
Approaches to Web Virus Scanning	5
“On-box” approach	5
“Off-box” approach	6
In Search of a Better Solution	7
The ICAP Cooperation Architecture	7
Policy-based Virus Scanning with Blue Coat Security Gateways	7
Blue Coat Security Gateway Component	8
Partner ICAP Virus Protection Server Component	9
Using Security Gateways to Scale Enterprise Virus Protection	9
Web Caching	9
Scanning Policy Optimization	10
Adding Up Performance Gains with the Security Gateway	10
Additional Scaling Strategies	11
Blue Coat Security Solutions	11
References	11

Summary

The World Wide Web is becoming a critical application for networked businesses worldwide. Valuable as the Web is, it also provides a new way for viruses to enter corporate networks, much the same way that email provided a new entry in the '90's. As enterprises move to tighten security against known viruses entering via floppy disk, CD-ROM, or as email attachments, hackers have begun to exploit the Web as a door that is still being left open by IT departments using firewall technology alone. According to an article published in Business Week [1], "Perimeter defenses such as firewalls are not enough to ward off increasingly sophisticated worms and viruses." It goes on to say that 70% of all intrusion attempts target Port 80 – which is typically left open on corporate firewalls to allow for Web browsing.

As a result, centralized virus scanning and content security at Internet access points is required to control harmful content at the network perimeter – before it gets into the enterprise. But deployment of centralized virus protection services has historically been impeded by the performance, functionality, and scalability limitations of firewall-based solutions. What's worse, many existing virus protection solutions simply aren't designed to monitor Web traffic and find the new types of malicious mobile code being created to exploit Port 80 weaknesses. In order to overcome these technical challenges, a new breed of security device has emerged.

Blue Coat's Port 80 Security Gateway provides an optimized solution for web virus protection and does so extremely efficiently. Using this solution, organizations can afford to provide Web virus protection that can scale to support all of their Web traffic, while also giving them granular policy control for managing Web content.

This paper provides an introduction to the policy-enabled virus protection capabilities of Blue Coat's Port 80 Security Gateway. By combining efficient, standards-based methods of vectoring content to a cooperating virus scanning server with advanced policy enforcement and web object caching capabilities, the Security Gateway provides the optimum solution for the Web virus problem.

"Perimeter defenses such as firewalls are not enough to ward off increasingly sophisticated worms and viruses."

- FROM BUSINESSWEEK [1]

Web Security for the Enterprise

Introduction

The open nature of the Internet is both a blessing and a curse. The same network used to save money and make organizations more efficient is also the entryway for potentially dangerous new threats. As technology evolves, so do computer viruses. Files that were once transported by floppy disk now move as email attachments or Web downloads, and viruses have made the same leaps. The result is that enterprise network administrators are dealing with two issues that are diametrically opposed to each other, increased connectivity and sharing of information on the one hand, and providing increased security on the other.

IS departments, both internal and external to an organization, are aggressively moving to Web-enable their application environments. This includes the use of technologies like ActiveX, JavaScript, Java applets, and other active content components that make the end-user experience more feature-rich and user-friendly.

At the same time, security administrators are faced with the task of securing the network from threats associated with these same technologies. As enterprises move to tighten security against more traditional viruses, hackers have begun to exploit the web protocols typically used for “friendly purposes” – in other words, protocols firewalls are configured to allow. Malicious mobile code viruses, such as Nimda and Code Red, enter networks as executables (e.g. ActiveX, JavaScript, Visual Basic Scripts, etc.) that appear to be part of normal Web content.

In response to this growing threat of virus infection and the difficulties of maintaining security services at the desktop, a managed approach to virus protection has emerged that places virus protection at the edge points of a network where it connects to the Internet. The goal of this approach is to keep harmful content outside the network and protect users behind a security perimeter.

Virus scanning of Web objects requires a high-performance system due to the real-time nature of Web browsing.

Adding to the difficulty of securing against virus threats is the real-time nature of the Web. Virus scanning is a very CPU-intensive task and can often take noticeable amounts of time to scan any given object. For applications like email, adding a few seconds or even a few minutes of delay to delivery is acceptable since users are not waiting for information to be displayed in an application screen. However, users accessing Web-enabled applications are expecting immediate responses to their requests, so adding significant delays to Web responses is simply not acceptable. Many organizations have tried to implement real-time Web content virus scanning and have quickly come to the conclusion that while the current class of products are effective at scanning content, they are too slow to be used without a severe negative impact on end-user productivity.

Correcting this inherent performance problem required organizations to deploy extremely expensive virus scanning infrastructures that in most cases still could not provide the performance required. Many organizations have given up trying to solve this problem for now, making them especially susceptible to attack.

Approaches to Web Virus Scanning

Early Web virus protection schemes typically took one of two architectural approaches. The first involved installing a virus scanning application on the same server as the firewall. This is called the “on-box” approach, and was typically seen with application-level firewalls. The second approach, most often seen with packet-level firewalls, was to shuttle content from the firewall to a separate server running a virus scanning application.

This approach typically works only in light traffic environments. Scaling this style of solution has proven to be prohibitively expensive because of architectural limitations. The primary issue is that virus protection applications are very resource intensive, and must vie for the same system resources as the firewall, resulting in unacceptable overall performance.

“On-box” approach

Initially, centralized virus protection solutions were installed as co-resident applications on application-level firewalls (sometimes known as application proxy firewalls). This architecture is still sometimes deployed today. In this model, the application-level firewall inserts a co-resident virus protection application into the traffic flow. Figure 1 illustrates this architecture.

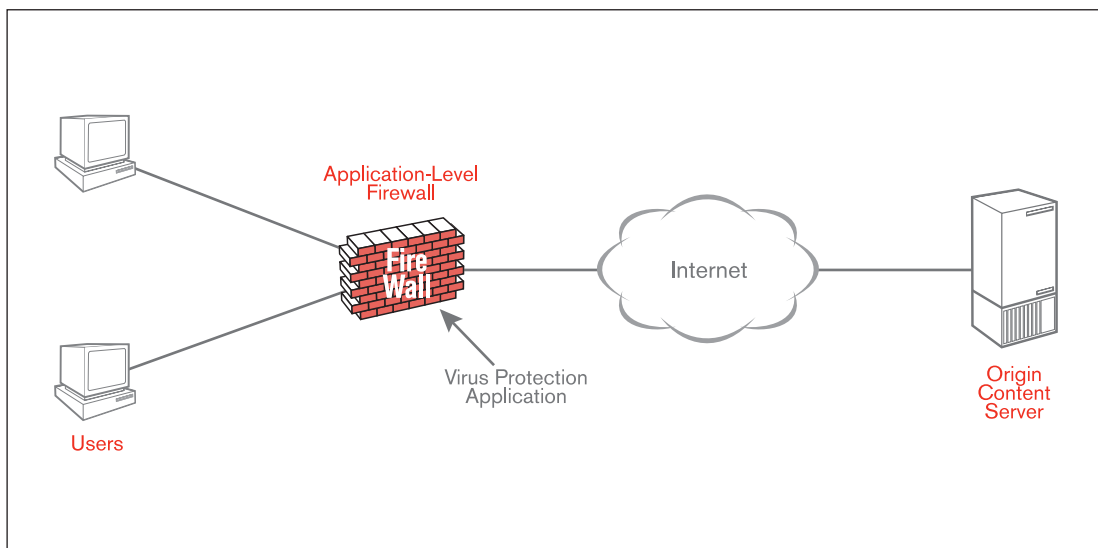


Figure 1 - “On-box” Architecture: An early virus scanning approach for light traffic environments

Web Security for the Enterprise

“Off-box” approach

Packet-level firewalls based on stateful inspection technology have emerged as the clear winner in the overall firewall market. This is due to their superior performance and scalability when compared to application-level firewalls.

In contrast to the co-resident virus scanning approach of application-level firewalls, packet-level firewall vendors have used a different strategy for centralized virus protection. The packet-level firewall vectors suspicious content to a cooperating application server (i.e., “off-box”). Figure 2 illustrates this approach.

Checkpoint introduced a solution that utilizes cooperating application servers to host the resource-intensive virus protection software. This utilizes Checkpoint's Content Vectoring Protocol (CVP) [2] to route email and Web content through a cooperating application server for virus scanning and scrubbing before letting it pass through the firewall. This offloading frees the firewall to perform its core screening duties and utilize the cooperating application server for parallel processing of virus scanning. However, this “off-box” approach still causes the firewall to become bottlenecked when it has to wait for a typically slower virus scanning server to finish reviewing traffic.

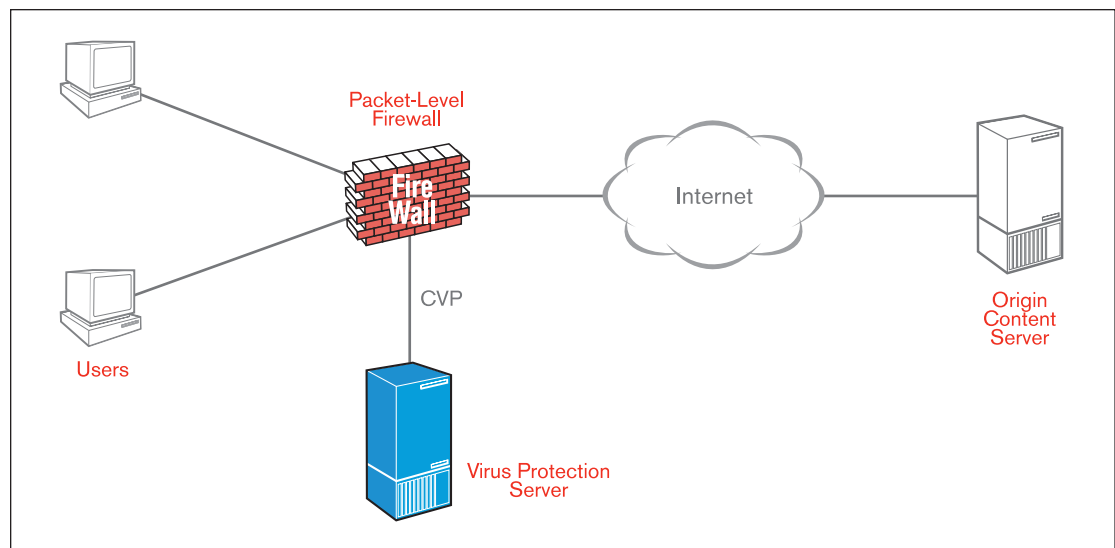


Figure 2 - Off-box Cooperation Architecture: Offers increased firewall performance but limited virus protection scalability

One of the most common packet-level firewalls is offered by Checkpoint Software Technologies, Ltd. Checkpoint realized that hosting a co-resident virus protection application would destroy their performance and scale advantages versus application-level firewalls by requiring the firewall to look deeply into every packet. Instead,

Since the performance advantages of stateful-inspection firewalls relies on not performing Layer 7 functions on the firewall, the typical approach taken is to configure the firewall to forward all content to the virus scanning server – even file types that typically do not require virus scanning (such as .jpg or .gif images). This avoids the need

to make application- and content-level decisions on the firewall. But then the virus scanning server is required to determine what content to scan, in addition to the frequently overwhelming burden of actually scanning the content. This “vector everything” approach has proven to scale poorly as traffic levels increase.

While the “off-box” approach has proven to be more effective than “on-box”, simply moving all content level decisions to the virus scanning server has simply moved the bottleneck from one machine to another, with only marginal improvements in overall throughput. What most organizations are still looking for is a way to truly deliver virus scanning of Web content at the performance level their users demand.

In Search of a Better Solution

Given that the majority (70%+) of the traffic flowing through the firewall is Web-based, it stands to reason Web caching could help solve this problem. Mindful of the benefits Web caching can offer for virus protection when combined with a CVP-style architecture, several proxy caching vendors collaborated on the development of a new off-box virus scanning solution. This work [3] began in 1999 and has resulted in the Internet Content Adaptation Protocol (ICAP) standard[4]. Initially, Checkpoint’s CVP protocol was considered, however upon further investigation, it was determined that this protocol didn’t integrate well with the semantics of the primary web protocols – HTTP and FTP. Thus, the group designed the new ICAP protocol to efficiently provide a generalized off-box solution for several Web applications, with virus protection being one of the most important.

The ICAP Cooperation Architecture

The ICAP cooperation architecture is conceptually similar to the CVP design introduced by Checkpoint Software Technology Ltd. However, it differs in two fundamental ways. First, ICAP is optimized to encapsulate HTTP with maximum efficiency. Second, the architecture calls for four distinct modes of operation that are modeled upon the operational characteristics of proxy caches. The interested reader is advised to consult the ICAP specification [4] for in-depth information on ICAP modes. While virus protection was one of the applications specifically targeted by the designers of the ICAP protocol, control policy that determines what content is to be vectored out to the virus scanning server is an essential component that has yet to be addressed by the ICAP specification. In order to provide an optimized solution, this control policy should be managed by the proxy cache. Again, an alternative would be to vector all content to the virus server and let it determine what content requires scanning. However, this approach only serves to further burden the virus scanning server and results in the frequent unnecessary routing of benign content to the anti virus server.

Policy-based Virus Scanning with the Blue Coat Security Gateway

The Blue Coat Security Gateway supports the ICAP specification to interoperate with a range of virus scanning applications. The virus protection application is hosted on a “out of box” server known as the ICAP server. The combination of the ICAP server and its application are known as an ICAP service. This service is registered with the Security Gateway, which in this case is referred to as the ICAP client. Figure 3 illustrates the ICAP architecture for a virus protection application with a Blue Coat Security Gateway.

The ICAP cooperation architecture is conceptually similar to Checkpoint’s CVP protocol, but has been optimized for Web protocols.

Web Security for the Enterprise

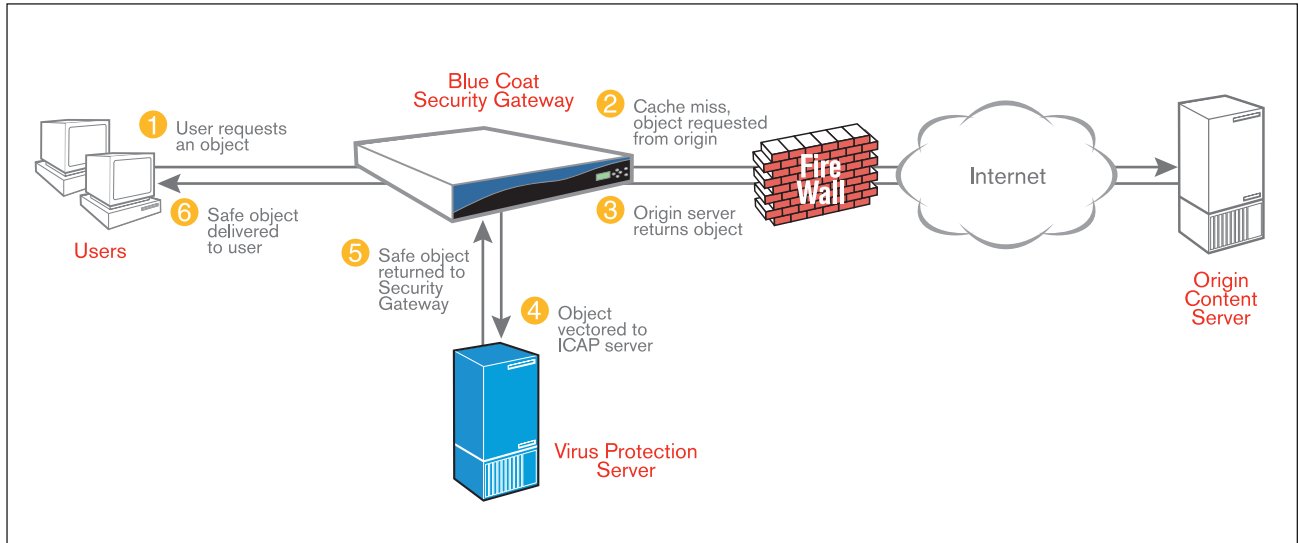


Figure 3 - Implementing ICAP for Virus Protection with the Blue Coat Security Gateway

The virus protection service operates as follows. In step 1, the user agent sends an object request to the Security Gateway (ICAP client). If the object is in cache, it is returned immediately in step 6; otherwise the request is forwarded on to origin server in step 2. The origin server responds to the ICAP client with an object in step 3. In step 4, the Security Gateway ICAP Client, based on its scanning policy, vectors the response out to a virus protection server (ICAP server). The ICAP server processes the object and proceeds to step 5, in which it returns a safe object to the ICAP client. The Security Gateway caches the safe object and proceeds to step 6 where it returns the object to the user agent. Any additional requests for the same content are handled by the Security Gateway without a rescan of the content – thus avoiding additional load on already overloaded virus protection servers.

Blue Coat Security Gateway Component

The Blue Coat Security Gateway provides the underlying policy framework and language used in defining, provisioning and enforcing web security policies. Security Gateways provide a state-of-the-art policy framework

and Policy Processing Engine (PPE). Blue Coat Visual Policy Manager defines control policy, which is provisioned to an enterprise's Security Gateways. Utilizing the Visual Policy Manager, powerful security policies for virus protection can be executed on the Security Gateways from a central management location. For example, in order to conserve virus scanning resources, network operators could set a policy to scan all Visual Basic scripts except those originating from a known, trusted source (e.g. an internal server). Further, Security Gateways enable these kinds of policies to be applied on a per-user and per protocol basis, allowing the flexibility required to adapt to changing security threats.

In addition to policy and content vectoring capability, the Security Gateway allows for load balancing across virus scanning servers and performs periodic health checks to ensure virus scanning servers are up and available to respond to requests. These capabilities allow network engineers to scale the backend virus protection infrastructure and ensure service reliability and overall throughput.

Finally, the Security Gateway also allows specific content to be sent to specialized devices that are better equipped to handle that type of content, for instance sending active content to a specialized behavioral-based inspection application while sending documents to a traditional virus pattern matching server.

Partner ICAP Virus Protection Server Component

Blue Coat's Security Gateway works with a range of partners' ICAP virus protection servers. To enable this capability, the Security Gateway is configured for use with the cooperating ICAP server and policy rules are defined for the types of content to be sent to the ICAP server.

Blue Coat has partnered with Symantec and Trend Micro, among others, who provide ICAP certified servers that interoperate seamlessly with the Security Gateways.

Symantec AntiVirus ScanEngine 3.0

The Symantec AntiVirus ScanEngine 3.0 [6] provides ICAP integration capability with Blue Coat's Security Gateway. For more information, contact Symantec Corporation at www.symantec.com.

Trend Micro InterScan™ WebProtect for iCAP 1.0

The Trend Micro InterScan™ WebProtect iCAP Edition server [7] provides ICAP integration capability with Blue Coat's Security Gateway. For more information, please contact Trend Micro, Inc. at www.trendmicro.com.

Using Security Gateways to Scale Enterprise Virus Protection

Blue Coat Security Gateways provide network operators with a “one-two” punch for immediately scaling virus protection systems. The two key enablers of increased system performance are Web Caching and Scanning Policy Optimization. Each of these functions offloads processing demands on virus scanning applications and allows for better overall system performance. This section explains the individual affect of each as well as the cumulative effects of implementing both features on a Blue Coat Security Gateway participating in a web virus protection solution.

Web Caching

By caching safe, virus-scanned objects, the expensive virus scan operation can be “amortized” across a number of access requests. In other words, users requesting an object that has already been scanned and stored in cache will not trigger a redundant scan of the object. Since Security Gateways are specifically designed to parse Web content responses, this operation does not further burden the Security Gateway as it would a firewall. The result is an effective performance increase for both the virus scanning server (which has to scan fewer objects) and the system as a whole (which can deliver cached, scanned content without waiting on an external scanning operation).

Virus scanning application performance gains are similar to those observed in network bandwidth gain deployments, and are sometimes referred to as “scan gain”. The amount of scan gain observed in a deployment is related to the number of objects that can be served directly from cache without needing to be scanned. In most enterprise deployments, the hit rate for



“When a product receives a Well-Connected award, it is an important endorsement - it is the top in its category and carries through with its promise of excellence.”

PUBLISHER
NETWORK COMPUTING



“Editors' Choice Awards are selected based on a product's usefulness to enterprise end-users...Blue Coat [the] Security Gateway appliance fills a need for secure and reliable enterprise e-business activities.”

EDITOR
COMMUNICATION NEWS

Web Security for the Enterprise

objects that require scanning, but which already have been scanned and cached by the Security Gateway typically ranges from 20% - 60%[8]. The result is that by deploying the Blue Coat Security Gateway into existing firewall-based virus-scanning deployments, organizations can scale system capacity by a factor of 3X[8] or more.

Scanning Policy Optimization

In addition to the performance improvements due to caching, most virus scanning deployments can be improved by optimizing where and how scanning policy is enforced in the network.

The Security Gateway's policy optimization capability improves system performance in two ways:

First, by relocating the object scanning policy from the cooperating virus scanning application servers to the much faster Security Gateway, the application server avoids having to perform these operations.

Second, when the scanning policy is enforced on the Security Gateway, objects that do not need scanning do not have to be vectored to the cooperating application server, avoiding an unnecessary and expensive operation. Since over 70% of web traffic [9,10] isn't susceptible to virus infection, this savings can be quite substantial.

The effects of scanning policy optimization are best measured by examining overall system throughput. In most cases, relocating scanning policy to the Blue Coat Security Gateway has a additional 2X performance improvement versus an existing firewall-based solution [8].

Adding Up Performance Gains with the Security Gateway

While both caching and policy optimization can help scale a virus protection system individually, the true power of the Security Gateway is derived from the fact that the corresponding performance gains are cumulative. The result is that deploying a Security Gateway into an existing virus protection deployment can easily yield an overall performance improvement of 6X [8] or more.

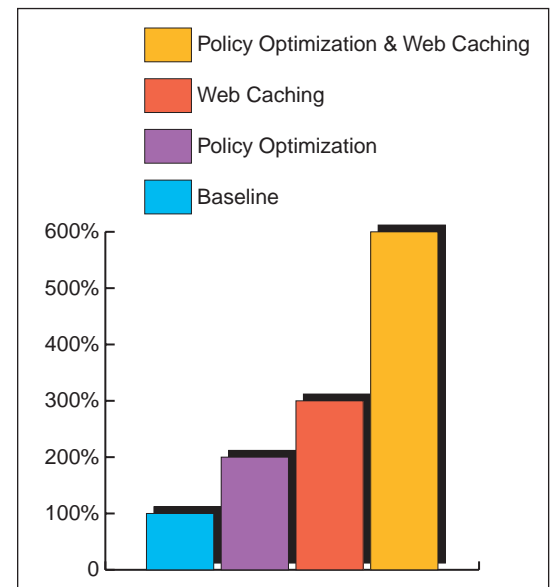


Figure 4 - Virus Protection Performance Improvements with the Blue Coat Security Gateway

Additional Scaling Strategies

The following are some simple guidelines for obtaining the most scalable virus protection solution from a Blue Coat Security Gateway.

- > Partition inspection levels by threat risk: Classify objects by the degree of scrutiny required by the virus protection service; and then associate those classes with the commensurate scan level needed to provide this scrutiny. Remember, the more scrutiny needed, the fewer transactions per second the virus protection service can perform.
- > Sub-partition bypass and inspection levels by trust domains: Further refine the scan policy based first upon the trust relationship between domains and then by inspection level. It is likely the types of objects considered threatening will vary depending upon where they originate.

Blue Coat Security Solutions

It is important to remember that virus protection alone is not a complete security solution. Rather, it is a fundamental element in a larger security strategy. In order for virus protection services to function as integral components of that larger strategy, rather than security islands of their own, it is necessary to integrate them into a comprehensive security policy.

Blue Coat's suite of security products provides customers with application-level security, powerful policy-based control capabilities, comprehensive management, and reporting functionality for authorization management, virus scanning, active content security, web usage monitoring, content (URL)

filtering, and network bandwidth protection. Acting in concert with existing routers, firewalls and servers, Blue Coat's Security Gateways reduce the complexity, management and processing overhead needed for comprehensive Web security.

For more information on optimized Web security with Blue Coat Security Gateways, visit www.BlueCoat.com.

References

- [1] "Cracks in the Firewall", Business Week, April 9, 2002.
- [2] "Content Vectoring Protocol (CVP) API Specification", Checkpoint Software Technologies Ltd, November 1998.
- [3] ICAP Forum, (www.i-cap.org).
- [4] Elson, J., et al. "ICAP the Internet Content Adaptation Protocol", draft-elson-icap-00.txt , June 2001. Available online at: http://www.icap.org/spec/icap_specification.txt
- [6] Symantec Corporation. www.symantec.com
- [7] Trend Micro, Inc. www.trendmicro.com
- [8] Results originate from Blue Coat internal comparative testing of Blue Coat Security Gateways versus Nokia appliances running Checkpoint Firewall-1.
- [9] Arlitt, M., Friedrich, R. and T. Jin. "Workload Characterization of a Web Proxy in a Cable Modem Environment", HP Laboratories Technical Report HTP-1999-48, April 1999.
- [10] T. Kelly. "Thin-Client Web Access Patterns: Measurements from a Cache-Busting Proxy", In proceedings of the Sixth International Workshop on Web Caching and Content Distribution, 20-22 June 2001, Boston University, Boston, MA.

Contact Blue Coat Systems
1.866.30.BCOAT
408.220.2200 Direct
408.220.2250 Fax
www.bluecoat.com



The Web Security Authority.

Copyright ©2002 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Blue Coat Systems, Inc. Specifications are subject to change without notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use, Blue Coat is a registered trademark of Blue Coat Systems, Inc. in the U.S. and worldwide. All other trademarks mentioned in this document are the property of their respective owners. Version 1.0

Blue Coat Systems, a Web security company, has developed the industry's first port 80 security appliance. Safeguarding many of the world's largest corporate networks, this high-performance security appliance intelligently protects against Web-based threats by policing Port 80 – the primary hole in the enterprise security infrastructure. Headquartered in Sunnyvale, California, Blue Coat Systems can be reached at 408.220.2200 or at <http://www.bluecoat.com>.