

Blue Coat Systems, Inc.

800 Series Security Appliance

Proxy Cache Competitive Benchmark versus
Cisco Systems Content Engine 560, Inktomi Traffic Server Engine
and Network Appliance NetCache C1105

Test Summary

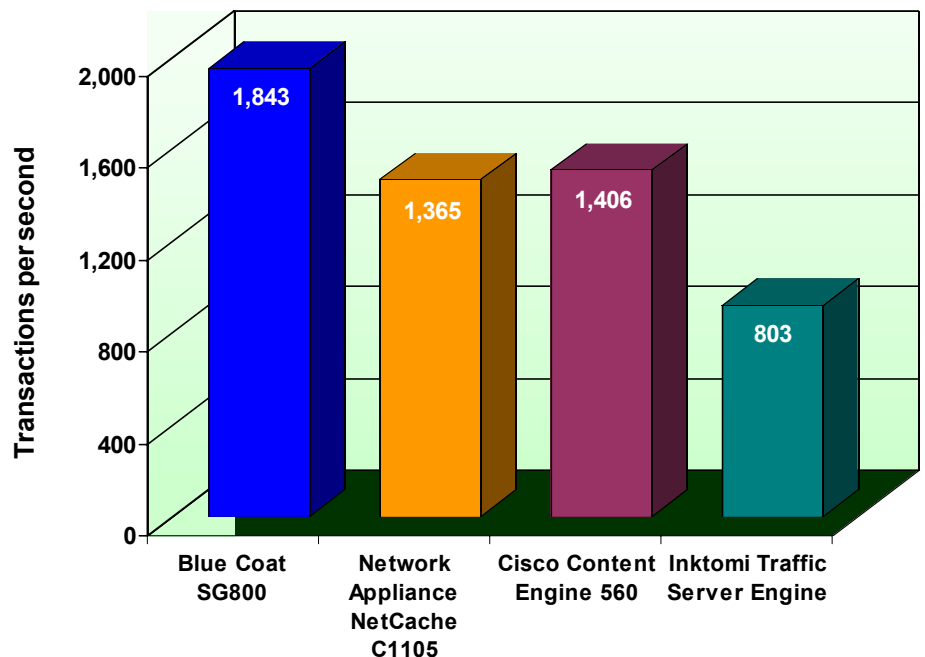
Premise: Government and corporate organizations are interested in comprehensive, content-level security for Web transactions along with a high level of performance. They require complete control over user access to the Web and demand granularity and flexibility in enforcing policy decisions on Web content entering the organization's private network via the Internet. These organizations realize that deploying a firewall alone will not achieve these goals. The Tolly Group endeavors to prove that the Blue Coat SG800 Series holds the most comprehensive policy management for security while also providing the best performance for security, proxy and content delivery applications.

Blue Coat Systems, Inc. commissioned The Tolly Group to evaluate its 800 Series Security Appliance (SG800), a security appliance designed to protect against emerging Web-based threats by policing port 80 traffic running across enterprise networks. The Tolly Group tested the SG800 against a trio of competitive products: A Cisco Systems Inc. Content Engine 560, an Inktomi Traffic Server Engine

Test Highlights

- Serves ICAP virus-scanned objects 15 times faster than Network Appliance NetCache C1105 and other products tested
- Achieves consistently fast end-user response times, maintaining sub-70-millisecond client response times during HTTP tests
- Delivers the greatest number of Windows Media and Real Media video streams
- Offers the most granular method of the products tested for applying security and access policies on Web content

**Maximum HTTP Objects per Second
as per Web Avalanche**



Source: The Tolly Group, August 2002

Figure 1

and a Network Appliance NetCache C1105. The Tolly Group also evaluated Microsoft Corp.'s ISA Server on a feature-comparison basis only.

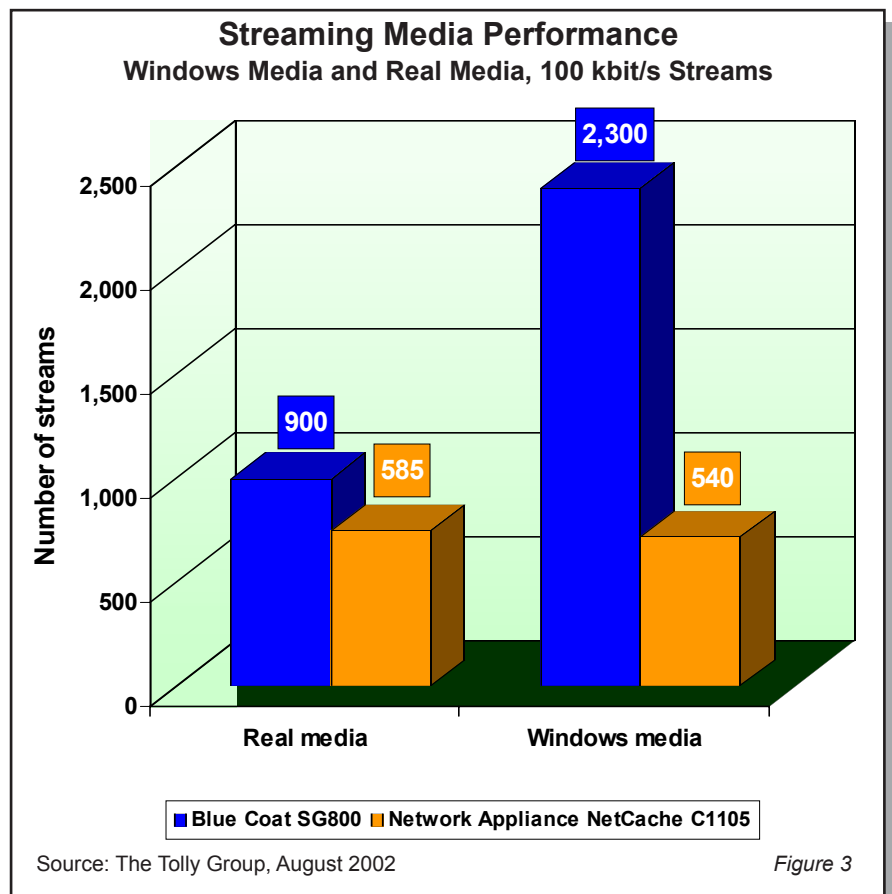
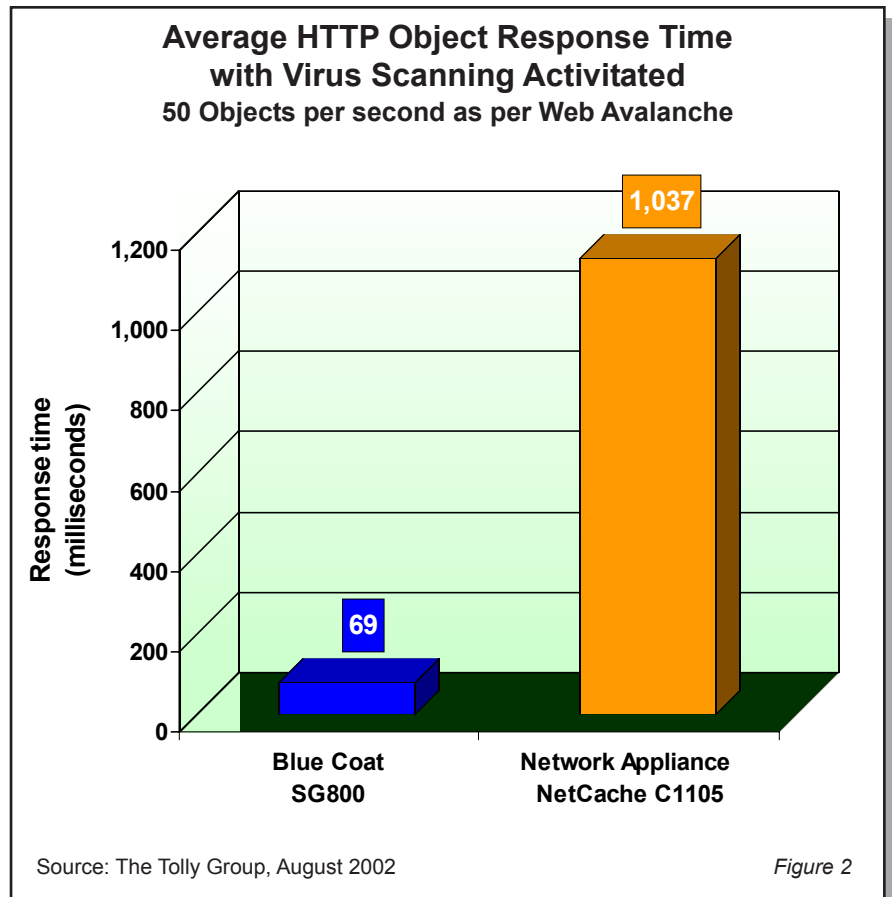
Products from Blue Coat, Cisco, Inktomi and Network Appliance were subjected to a battery of Web performance, system performance and feature verification tests that focused on proxy, security and caching functionality. Both the Blue Coat and Network Appliance devices also were evaluated for their capability to support Windows media streaming and Real media streaming content. Tests were conducted during June and July 2002.

RESULTS

HTTP PERFORMANCE

Tolly Group engineers measured the end-user response times for HTTP requests and recorded the number of objects per second handled by each of the devices tested. Devices were tested under both a moderate traffic load and a maximum traffic load. Transaction rates are reported as "maximum transactions per second," which is a value reported by the CAW Networks test tool as opposed to a transaction rate that is averaged over the course of the test.

The Blue Coat SG800 yielded the greatest transaction per second (tps) rate, processing 1,843 transactions while returning Web objects in just



60 milliseconds in a test with maximum Web traffic loads. By comparison, the SG800's next nearest rival, the Cisco Content Engine 560, delivered 26% fewer transactions with an object response time of 178 milliseconds, or nearly 3X slower than the SG800 object response time rate (see Figure 1). While the Network Appliance NetCache C1105 yielded a Web transaction rate of 1,365 tps, its object response time was 11X slower than the SG800. Inktomi's Traffic Server Engine delivered the poorest Web transaction rate, with 803 tps, although it yielded an object response time of 30 milliseconds.

Web performance tests using a moderate load of Web traffic yielded a more even Web transaction rate among competing products, with Blue Coat's SG800 again outperforming all products tested. The SG800 and Inktomi's Traffic Server Engine posted rates of 523 tps and 504 tps, respectively. Both products also yielded the lowest object response times, with 60 milliseconds for the SG800 and 27 milliseconds for the Inktomi product.

HTTP PERFORMANCE WITH VIRUS SCAN

Engineers repeated the HTTP performance test, this time adding an ICAP virus scan server access routine as a variable. Virus scanning was implemented using the Internet Content Adaptation Protocol

(ICAP), a standards-based architecture used for communicating between a proxy cache and an HTTP virus-scanning server. The Blue Coat SG800 and the Network Appliance NetCache C110 participated in this test, since none of the other products offered this feature. At a set transaction rate of 50 tps, the SG800 delivered a rate of 46 tps and delivered the best object response time, averaging 69 milliseconds (see Figure 2). Although the NetCache C1105 managed to match the SG800's tps rate, the NetCache C1105 was 15 times slower in returning objects, averaging a delay of 1,037 milliseconds. Moreover, the SG800 was able to continue serving virus-scanned files up to at least 700 tps, compared to the NetCache C110, which could not perform error-free tests above a 75 tps level.

FEATURE VERIFICATION

Engineers evaluated the presence of policy management and policy action features based upon a pass/fail metric.

The ability to implement granular, flexible security policy is dependent upon triggers (i.e., events which can initiate an action) and specific actions that can be invoked by the trigger. Policies were checked to function at four levels of granularity: source, destination, service, and time (see Figure 4). Results of this verification test show that the

Blue Coat Systems, Inc.

800 Series Security Appliance

Proxy Cache Benchmark



Blue Coat Systems, Inc. 800 Series Security Appliance Product Specifications*

- Supports up to four (4) 73-GB Ultra 160 SCSI disk drives
- Up to 2 GB RAM and three (3) 10/100 network interface cards
- Configuration restoration allows archiving of system settings, filtering and policy configurations
- Removable, hot-swappable disk drives for true fault tolerance
- Patent-pending policy engine enables sophisticated security policies based on over 30 network, user, content type, and time-based attributes
- Visual Policy Manager application (Java-based) provides intuitive graphical user interface for defining and managing security policies
- Support for proxied and transparent user authentication to multiple, diverse back-end authentication directories including RADIUS, LDAP and NTLM
- Comprehensive URL filtering allows organizations to restrict access to inappropriate Web content
- Caches HTTP and multimedia content that requires authentication at origin servers
- ICAP (Internet Content Adaptation Protocol)-based virus scanning support allows for scanning of Web-based viruses delivered over HTTP
- Integrated MIME-type filtering allows organizations to implement policies for both uploaded and downloaded content by MIME type
- Real-time logging and event notification enables logging and reporting on all events
- Bandwidth management features enable organizations to define limits for the total amount of network capacity available for streaming media and HTTP content

For more information contact:

Blue Coat Systems, Inc.
650 Almanor Ave, Sunnyvale, CA 94085
Phone: (408) 220-2200
Fax: (408) 220-2250
URL: <http://www.bluecoat.com>
E-mail: info@bluecoat.com

**Vendor-supplied information not verified by The Tolly Group*

SG800 offered comprehensive authentication (NTLM, LDAP, RADIUS, local password list) and the greatest capabilities in the features verified over any other product in the test.

Test engineers found the SG800's user interface – called the Visual Policy Manager (VPM) – intuitive for users that are familiar with configuration of security devices. It simplified policy management and allowed for rapid creation of complex policies. For example, 40 different security actions can be initiated from a single trigger, or from combinations of approximately 30 different triggers – this unique capability enables organizations to create almost any Web security or proxy policy required for their business.

STREAMING PERFORMANCE

Tolly Group engineers measured the maximum number of streams supported by the Blue Coat SG800 and

the Network Appliance NetCache C1105. Engineers measured the streaming rate when handling either Real media files, or Windows media streaming files.

Tests – using the common 100 Kbit/s stream size – show that the Blue Coat SG800 supported 900 Real media streams and 2,300 Windows media streams, which equates to 54% and 426% greater streaming capacity than the Network Appliance NetCache C1105 device, which delivered 585 Real media streams and 540 Windows media streams respectively (see Figure 3).

SYSTEM RESTART TIME

Engineers measured the system restart time for both a console reset and a simulated power outage. In both situations, the SG800 proved that it is capable of restarting and passing traffic within 91 seconds or less, which is significantly less than the three other rival products, which required from 111 seconds to 227 seconds.

ANALYSIS

The Blue Coat Systems SG800 has demonstrated it is a device not only capable of content caching/delivery, but also content security. Results show that the SG800 can outperform the Network Appliance C1105, Cisco Content Engine 560, and Inktomi Traffic Server Engine in a maximum transaction-per-second test while still maintaining low object response times.

With regards to HTTP performance, the SG800 achieved a 35% higher transaction-per-second rate than the Network Appliance NetCache C1105, while still maintaining a sub-100-millisecond response time. For streaming media, the SG800 served more than 4X more streams than the NetCache C1105 when servicing Windows media files at a 100 Kbit/s rate.

In the HTTP performance tests with virus scan, the SG800 further demonstrated that its

Factoring in Microsoft's ISA Server

Despite Blue Coat's desire to test its SG800 head-to-head in Web and system performance benchmarks against Microsoft's ISA Server, The Tolly Group was unable to test the Microsoft product due to the software giant's licensing restrictions, which restrict publishing of competitive benchmarks.

The Tolly Group did, however, compare ISA Server against other products in the feature verification examination. Here, we begin to see that the SG800 offers a greater depth of granularity with regard to support for policy triggers than the Microsoft ISA Server. While the SG800 supported each of five triggers inspected, the ISA Server lacked support for user attribute and MIME triggers.

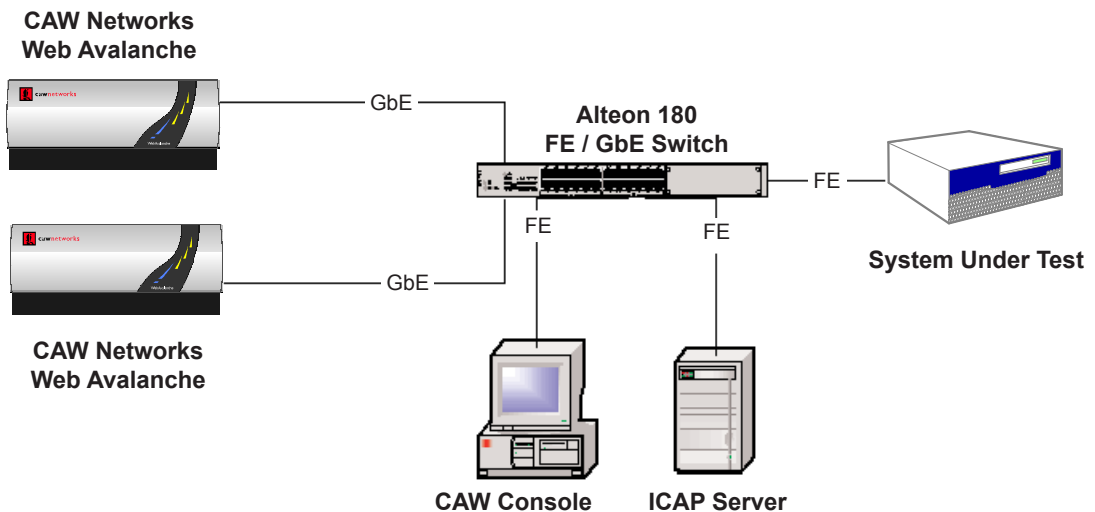
Tolly Group engineers saw a wider disparity between the two products when they examined the Actions capabilities of the products. Here, again, the SG800 exhibited broader support than did the ISA Server (see Figure 3). Moreover, the ISA Server failed to match the debugging capabilities of the SG800.

Feature Verification Comparison

	Blue Coat SG800	Cisco Content Engine 560	Inktomi Traffic Server Engine	Microsoft ISA Server	Network Appliance NetCache C1105	SunOne iPlanet Proxy Server
Policy Management						
Central policy architecture	Yes	Partial	No	Yes	No	Yes
Graphical policy editor interface	Yes	No	No	Yes	No	No
Policy Triggers						
User group memberships	Yes	No support	No	Yes	Yes	Yes
User Attributes	Yes	No support	No	No	No	No
MIME	Yes	Yes	No	No	No	Yes
File Type	Yes	Yes	No	Yes	No	Yes
Time of day	Yes	No	Yes	Yes	Yes	Yes
Policy Actions						
Authentication override	Src, Dst, Svc, Tm	Src, Dst, Svc	Src, Dst, Svc, Tm	No Support	Not noted	Srv, Dst, Svc, Tm
Content filtering	Src, Dst, Svc, Tm	Dst	Dst	Src, Dst	Src, Dst, Svc, Tm	Srv, Dst, Svc, Tm
Customizable error page	Src, Dst, Svc, Tm	Content filtering only	Dst	Dst	Dst	Src, Dst
Limit bandwidth	Src, Dst, Svc, Tm	No support	No support	No Support (just prioritization)	Src, Dst, Svc, Tm	No Support
Replace active content	Src, Dst, Svc, Tm	No support	No support	No Support	No support	Src, Dst, Svc, Tm
Rewrite URL (two-way)	Src, Dst, Svc, Tm	No support	Dst	No Support	Not noted	No Support
Set TTL (time to live)	Src, Dst, Svc, Tm	Protocol only	No support	No Support (global only)	Dst	No Support
Splash page	Src, Dst, Svc, Tm	No support	No support	No Support	No support	No Support
Virus scan	Src, Dst, Svc, Tm	No support	No support	No Support	Src, Dst, Svc, Tm	Src, Dst, Svc, Tm
Warn	Src, Dst, Svc, Tm	No support	No support	No Support	No support	No Support
Debugging Tools						
Packet capture	Yes	No	Yes (OS)	Yes (OS)	Yes	Yes (OS)
Policy Rules						
Trace policy rules	Yes	No	No	No	No	No
Write to event log	Yes	No	No	No	No	No
Logging						
Formats						
Common log format	Yes	No	Yes	Yes	Yes	Yes
Extended log format	Yes	Yes	Yes	Yes	Yes	Yes
Squid log format	Yes	Yes	Yes	No	Yes	No
Customizable format	Yes	No	Yes	Yes	Yes	Yes

Policy settings: Src = source address, Dst = destination address,
Svc = service type, Tm = time of day

Web Performance Test Bed



Source: The Tolly Group, August 2002

Figure 5

high-performance HTTP performance characteristics are easily extended to HTTP virus-scanning environments. In fact, the product showed little degradation in response time performance when delivering HTTP objects without virus scanning (60 ms) or with virus scanning (69 ms). This is a critical metric to consider when making a vendor selection – the real-time nature of Web applications requires a solution that can perform "real time" scanning against Web-based threats.

In addition to the stronger performance and scalability of the Blue Coat SG800, engineers confirmed the unique policy capabilities of the SG800 that apply to Windows and Real streams in the same way they apply to HTTP. This allows administrators a common tool and methodology for configuring policies such as time-based rules (to allow access to a specific event) and

bandwidth management across all applications – whether they are operating over HTTP or natively over Microsoft Media Stream (MMS) or the Real-Time Streaming Protocol (RTSP).

In summary, the SG800 demonstrated that its optimized approach to handling Web traffic and HTTP content yielded the highest performance for transactions across both moderate load and maximum load tests – combined with some of the lowest response times. The tests demonstrate that the SG800 is best suited to scale to the needs of the largest deployments while still meeting user performance expectations.

TEST CONFIGURATION AND METHODOLOGY

For performance tests, The Tolly Group tested a Blue Coat

Systems SG800 running software version SG 2.1.00. The device was configured with an 866-MHz Pentium III with 512 Mbytes of RAM and two 10/100 Fast Ethernet NICs. Engineers tested the SG800 against three devices: a Cisco Systems Content Engine 560 running software version CE560-4.0.3 and configured with a Pentium III with 512 Mbytes of RAM and two 10/100 Fast Ethernet NICs. The SG800 also was tested against an Inktomi Traffic Server Engine running software version 4.0.15 and configured with two Pentium III processors with 1 Gbyte of RAM and two 10/100 Fast Ethernet NICs. Lastly the SG800 tested against a Network Appliance NetCache C1105 running software version 5.2 and configured with a 433-MHz Pentium III processor with 512 Mbytes of RAM and two 10/100 Fast Ethernet NICs.

For Web performance tests, the devices under test connected via Fast Ethernet to an Alteon Web Systems 180E Fast Ethernet/Gigabit Ethernet switch, which, in turn, supported Gigabit Ethernet connections to a CAW Networks Web Reflector (version 4.0.9), a Web server simulator, and a CAW Networks Web Avalanche (version 4.0.9), an HTTP test tool (see Figure 5). Those latter devices generated real-world Web traffic for the HTTP performance tests. The Alteon 180E switch also supported Fast Ethernet links to a CAW Console and to an ICAP server used for virus scanning during Web performance tests.

For the HTTP performance tests, engineers installed and configured the Web Avalanche and Web Reflector products for HTTP delivery. Each system first ran through a quick baseline test to determine roughly how many objects could be served without failure. Then the system cache was cleared and a slow ramp up was begun. Once the system reached peak load it had to maintain such, without any failures, for three minutes. Results were recorded by the Web Avalanche.

For the HTTP performance with virus scan test, engineers configured the test devices to access a Symantec AV Server Scan Engine version 3.0.0.24 via ICAP. For this test each system ramped up to 50 object requests every second and an

average was recorded from the Web Avalanche for this three-minute test. The same object distribution and attributes as used in the first HTTP Performance Test were also reused for this test.

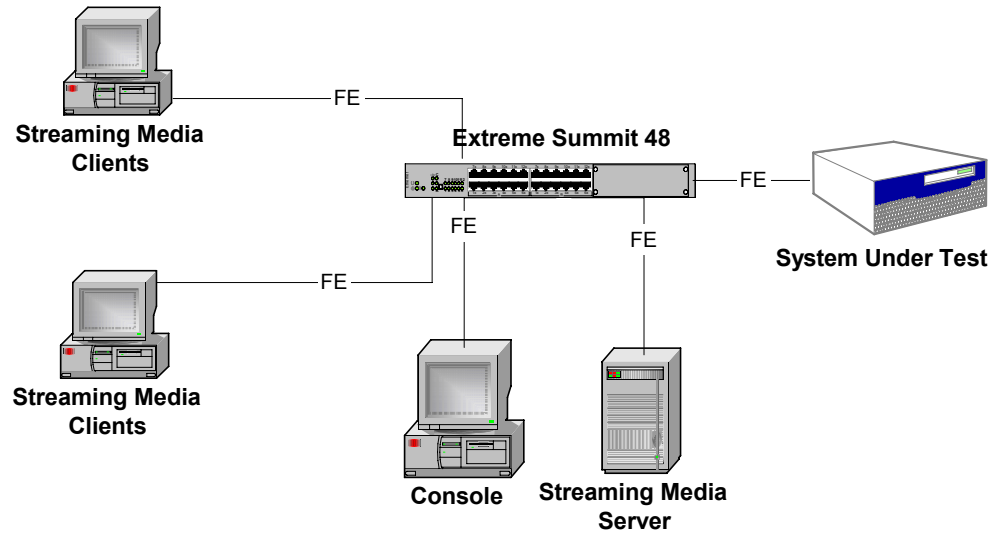
For streaming media performance tests, the devices under test maintained their Fast Ethernet connections to an Extreme Networks Summit 48 switch, which supported Fast Ethernet links to streaming media clients, a streaming media server and a console.

For Real media streaming tests, content was served via Real Server 8 from a 733-MHz Pentium III PC with 256 Mbytes of RAM, running Windows 2000, Service Pack 2. For Windows media streaming tests, content was served from a Windows Media Services Server 4.1 from a 733-MHz Pentium III PC with 256 Mbytes of RAM, running Windows 2000, Service Pack 2. Engineers used PyPlayer 1.52 for Real media to load the SUT; this test tool also was used in the Windows media test. Both test tools were installed on a bank of 12 733-MHz Pentium III PCs, each with 256 Mbytes of RAM, running Windows 2000, Service Pack 2. These devices performed the client file viewing actions of normal users. With the SUT inline, when the test tool made a first request for the streaming file, it was first served via an origin server, through the SUT to the

client; the SUT cached this file, and was able to directly serve the file for future request without aid from the origin server. From the test tools, the number of active, non-packet-dropping streams was obtained.

For feature verification, engineers checked each product for feature availability, and conducted appropriate tests (dependent upon feature) to validate functionality. For example, for content filtering, the content filter was configured, and then access to the content was attempted. Once a feature was verified, it was next analyzed to find what kind of triggers could invoke the feature. Specifically, for source triggers, we examined user name, user group, source IP, browser type, etc., for destination triggers, we examined host, domain, IP address, port, etc., for service, we examined MIME type, etc., and for time, we examined work hours (Mondays, 5pm to 7am, etc.).

Streaming Media Test Bed



Source: The Tolly Group, August 2002

Figure 6

The Tolly Group gratefully acknowledges the providers of test equipment used in this project.

Vendor	Product	Web address
Acterna LLC	Domino FastEthernet DA-362	http://www.acterna.com
CAW Networks	Web Avalanche/Reflector 4.0.9	http://www.caw.com
Real Networks	PyPlayer 1.52	http://www.realnetworks.com

TOLLY GROUP SERVICES

With more than a decade of testing experience of leading-edge network technologies, The Tolly Group employs time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy. Plus, unlike narrowly focused testing shops, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure. The company offers an unparalleled array of reports and services including: Test Summaries, Tolly Verifieds, performance certification programs, educational Webcasts, white paper production, proof-of-concept testing, network planning, industry studies, end-user services, strategic consulting and integrated



marketing services. Learn more about The Tolly Group services by calling (732) 528-3300, or send E-mail to info@tolly.com.

For info on the Fair Testing Charter, visit: www.tolly.com/About/ftc.asp

PROJECT PROFILE

Sponsor: Blue Coat Systems, Inc.

Document number: 202148

Product Class: Proxy cache/Web security appliance

Products under test:

- Blue Coat Systems 800 Series Security Appliance ver SG 2.1.00
- Cisco Systems Content Engine 560 ver 4.0.3
- Inktomi Traffic Server Engine ver 4.0.15
- Network Appliance NetCache C1105 ver 5.2

Testing window: June through July 2002

For more information on this document, or other services offered by The Tolly Group, visit our World Wide Web site at <http://www.tolly.com>, send E-mail to info@tolly.com, call (800) 933-1699 or (732) 528-3300.

Internetworking technology is an area of rapid growth and constant change. The Tolly Group conducts engineering-caliber testing in an effort to provide the internetworking industry with valuable information on current products and technology. While great care is taken to assure utmost accuracy, mistakes can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental, and consequential damages which may result from the use of information contained in this document. All trademarks are the property of their respective owners.

The Tolly Group doc. 202148 rev. kco 16 Oct 02