

**National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme**



**Common Criteria Evaluation and Validation Scheme
Validation Report**

Blue Coat ProxySG Operating System v3.2.4.8

Report Number: CCEVS-VR-05- 0113

Dated: 8 August 2005

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Thomas P. Murphy
Mitretek Systems
Linthicum Maryland

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

Royal Purvis
Mitretek Systems
Falls Church, Virginia

Tim Bergendahl
The Mitre Corporation
Bedford, Massachusetts

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

1	<i>EXECUTIVE SUMMARY</i>	4
2	<i>Identification</i>	5
2.1	<i>Applicable Interpretations</i>	6
3	<i>Security Policy</i>	7
3.5	<i>Security Management</i>	8
3.6	<i>Privacy</i>	9
3.7	<i>Protection of the TSF</i>	9
4	<i>Assumptions</i>	9
5	<i>Clarification of Scope</i>	10
6	<i>Architecture Information</i>	11
7	<i>Product Delivery</i>	13
8	<i>IT Product Testing</i>	15
9	<i>Evaluated Configuration</i>	17
9.1	<i>TOE</i>	17
9.1.1	<i>Physical Boundary of TOE</i>	17
9.1.2	<i>Logical Boundary of TOE</i>	17
9.2	<i>IT Environment</i>	18
10	<i>Results of the Evaluation</i>	18
11	<i>Validator Comments</i>	18
12	<i>Security Target</i>	19
13	<i>Glossary</i>	19
14	<i>Bibliography</i>	20

Table of Figures

<i>Figure 1: TOE Deployment</i>	4
<i>Figure 2 - Architecture Diagram</i>	13
<i>Figure 3 : Test Configuration</i>	16

List of Tables

<i>Table 1: Evaluation Identifiers</i>	5
<i>Table 2 : Product Hardware Platforms</i>	14

1 EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the Blue Coat ProxySG Operating System (SGOS) version 3.2.4.8 at EAL2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on June 30, 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) [10] written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.1, Part 2 extended and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

SGOS is a proprietary operating system developed specifically for use on a hardware appliance that serves as an Internet proxy. The purpose of the appliance is to provide a layer of security between an Internal and External Network, typically an office network and the Internet. Figure 1: TOE Deployment illustrates the intended environment for the TOE. The scope of the evaluation covered the SGOS software that implements the security between the Internal and External Network. Portions of SGOS and the underlying hardware were treated as part of the IT Environment. The evaluation covers specific models from the Blue Coat ProxySG Series 400, Series 800, and Series 8000 Security Appliances. The specific hardware platforms are listed in Table 2 : Product Hardware Platforms on page 14.

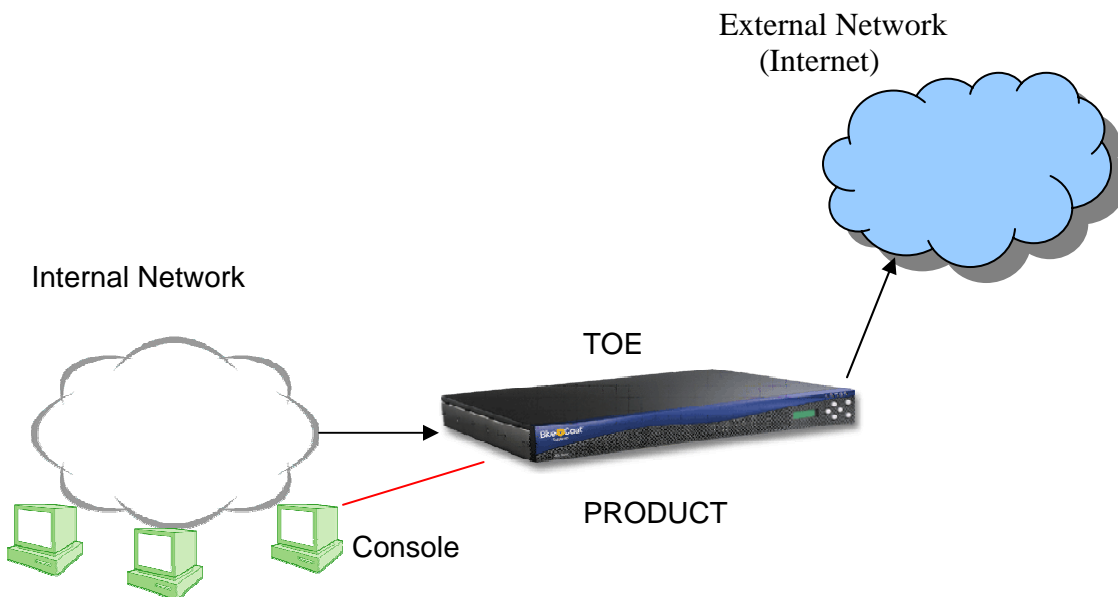


Figure 1: TOE Deployment

The evaluated TOE can be used to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. The controlled protocols are HTTP,

FTP, SOCKS and AIM, MSN and Yahoo Instant Messenger. This is achieved by enforcing a configurable policy (Proxy SFP) on controlled protocol traffic to and from the Internal Network users. The policy may include authentication, authorization, content filtering, and auditing. Also, internal IP addresses are obfuscated through the proxy, thereby helping to protect internal machines from direct Internet attack.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- the Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated,
- the Security Target (ST), describing the security features, claims, and assurances of the product,
- the conformance result of the evaluation,
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Evaluation Identifiers for Blue Coat Operating System	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Blue Coat ProxySG Operating System v3.2.4.8
Protection Profile	N/A
Security Target	Blue Coat ProxySG Operating System v3.2.4.8 Security Target, dated July 7, 2005 [9]
Evaluation Technical Report	Blue Coat ProxySG Operating System v3.2.4.8 Evaluation Technical Report, Document No. F2-0705-002, Dated August 8, 2005 [10]
Conformance Result	Part 2 extended and EAL2 Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on July 9, 2003.

Evaluation Identifiers for Blue Coat Operating System	
Version of CEM	CEM Version 1.0 [and all applicable NIAP and International Interpretations effective on July 9, 2003]
Sponsor	Blue Coat Systems, Inc. 420 North Mary Ave. Sunnyvale, CA 94085
Developer	Blue Coat Systems, Inc. 420 North Mary Ave. Sunnyvale, CA 94085
Evaluator(s)	COACT Incorporated Bob Roland Jeffrey Burke Anthony Busciglio Nick Krajewski
Validator(s)	NIAP CCEVS Thomas P. Murphy Dr. Jerome Myers Royal Purvis Tim Bergendahl

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

- I-0405 – American English Is an Acceptable Refinement
- I-0422 – Clarification Of ``Audit Records''
- I-0423 – Some Modifications to the Audit Trail Are Authorized
- I-0427 – Identification of Standards

International Interpretations

- RI#003 – Unique identification of configuration items in the configuration list (11 February 2002)
- RI#008 – Augmented and Conformant overlap (31 July 2001)
- RI#016 – Objective for ADO_DEL (11 February 2002)
- RI#019 – Assurance Iterations (11 February 2002)
- RI#031 – Obvious vulnerabilities (25 October 2002)
- RI#049 – Threats met by environment (16 February 2001)
- RI#064 – Apparent higher standard for explicitly stated requirements (16 February 2001)

RI#065 – No component to call out security function management (31 July 2001)

RI#075 – Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1 (15 October 2000)

RI#084 – Aspects of objectives in TOE and environment (31 July 2001)

RI#085 – SOF Claims additional to the overall claim (11 February 2002)

RI#116 – Indistinguishable work units for ADO_DEL (31 July 2001)

RI#127 – Work unit not at the right place (25 October 2002)

3 Security Policy

The TOE is a secure operating system based on LINUX which is delivered installed on a proprietary hardware appliance. The TOE is preloaded onto the appliance by the vendor. When properly installed and set-up by a Console Administrator for a client network, the TOE imposes access constraints on Internet traffic to and from the attached network computers and work stations. The TOE can restrict access to certain protocols, i.e. HTTP, FTP, SOCKS and AIM, MSN and Yahoo Instant Messenger.

The TOE implements specific configurable security policies on network users as set-up by an Administrator. Policies may be associated with all users, groups of users or with each unique user and the user's related device. These policies create access configurations with restrictions on network user access to specific resources, networks and linkages. The security policy also limits the persons authorized to modify the TOE configurations. All access is restricted through the use of Passwords. The TOE implements the following IT security functions: Audit, Information Flow Protection, Identification and Authentication, Security Management, Privacy, and Protection of TSF.

3.1 Audit

The SGOS Audit function generates audit records for all actions related to audit, authentication, administration activities, and communication with external IT devices.

3.2 Administrative Access Control

Using the Command Line Interface (CLI) language, an authorized administrator can craft policies controlling administrative access by users (other than the console administrator, which is not subject to the Administrative Access Control policy). The Administrative Access Control Policy is defined using the Security Gateway Content Policy Language (CPL). The syntax and rules of CPL are defined in the Blue Coat Systems Port80 Security Appliance Content Policy Language Guide [11]. CPL rules allow administrative access to be granted or denied based on the user name, the groups to which the user belongs and the time of day.

3.3 Information Flow Protection

The TOE enforces administrator defined traffic flow policies. The policy that defines the traffic flow policy is referred to as the Proxy SFP. Privileged Administrators craft the Proxy SFP using CPL. The syntax and rules of the CPL are defined in the Blue Coat Proxy SG Content Policy Language Guide [11]. CPL permits the administrator to specify Proxy SFP controls based upon the user name, the users group membership, the source IP address, the destination IP address, the destination port, the protocol, the URL, the time of day, the date, the originating application, the MIME type, the Request Method, other HTTP request header fields, HTTP response header fields, and the HTTP response body.

3.4 Identification and Authentication

The TOE implements two different types of authentication. The first level is for the Administrator logging onto the SGOS to perform system administration via the CLI over a serial connection. Administrative and Configuration functions require a user identity and Password-authentication to access TOE functions.

The second type of authentication is for network users. All network users must undergo a log-in authorization when attempting to access any network or internet resources that have been configured to require authentication in the access control policy. Users trying to access such resources require Password-Authentication to access the specified resources. These users do not have access to change TOE functions or configurations.

3.5 Security Management

The TOE implements two types of administrative roles for managing the TOE. Those roles are Ordinary Administrator and Privileged Administrator. An Ordinary Administrator must re-authenticate and pass access control checks specified by the Administrative Access Control Policy to take on the role of a Privileged Administrator. The TOE distinguishes between the Console Administrator and other users that are authorized as administrators. The Console Administrator is a special role that is not further restricted by the Administrative Access Control Policy. Any person having physical access to the console terminal and knowledge of the Console Administrator user name and password may perform the role of Console Administrator. Just as any other Ordinary Administrator, the Console Administrator must take an action to assume the Privileged Administrator role, but the Console Administrator is not subject to any Administrative Access Control Policies that would potentially limit the capability to assume privileges.

The Console Administrator has full authority to administer all aspects of the TOE including the review and modification of any part of the configuration of the SGOS, including credentials, audit settings, network settings, and system time. Privileged Administrators have the authority to define the information flow control Proxy SFP that is imposed upon network traffic.

3.6 Privacy

SGOS protects the identities of those network devices on the internal network by ensuring that the real source IP address that the user is coming from on the internal network is not available to anyone receiving traffic on the external side of the network.

3.7 Protection of the TSF

The TOE provides self-protection through its interfaces that are available to general users. The TOE relies upon the underlying IT environment to complete the protection of the TOE from tampering. It is assumed that the SGOS appliance will remain physically connected to the network so that the appliance cannot be bypassed. The TOE protects its management functions by isolating them through authentication.

4 Assumptions

The evaluation made the following assumption concerning product usage:

- The Administrator is non-hostile and follows all administrator guidance when using the TOE. Administration is competent and on-going.
- The TOE will be located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware.
- The platform used to host the TOE is one of the platforms listed in Table 2 and functions as documented for SGOS.
- The hardware, operating systems, and software required by the TOE have been installed and configured according to the appropriate installation guides. The internal and external networks are not connected in any way other than the SGOS device.
- The environment must have the ability to authenticate the Administrator and upload a trusted user password file.
- The environment will provide a reliable timestamp.
- The platform used to host the TOE will forward all network traffic directly to the TOE. The platform will be dedicated to supporting the TOE and supports no other systems or processes.
- The environment will provide an audit log of security relevant events.
- Passwords used for both administrator and user accounts will be at least five characters in length.
- All network access is exclusively through the Proxy device. No other access method such as telephone dial-up connection is permitted for any network computer or other device.

5 Clarification of Scope

The TOE only covers a subset of the entire SGOS product that comes preinstalled on the appliance platform. In particular, the underlying hardware was not included in the evaluation.

The TOE included the following security services functionality:

- Policy architecture triggers: define control through multiple triggers, such as user/group, time, protocol, application, file/MIME type, request method
- Policy architecture actions: Multiple actions including allow, deny, rewrite, redirect, email management, log request, authenticate and set authentication mode.
- Proxy or transparent installation: Intercepts non-proxied requests and applies policy.
- HTTP port listen: Define non-8080 port for HTTP traffic
- On box content filtering: Restrict access to sites, supporting subscription-based filtering from Websense, SmartFilter, SurfControl and locally defined lists
- Active content control: Disallow active HTML content (Java, ActiveX controls, etc.)
- Filter List (deny): Restrict access to certain sites
- Header transformation: Referrer headers and other headers can be removed or replaced
- Accept/Deny inbound connections separately for each interface: TOE can be configured in parallel with a firewall
- Source IP access restriction: Restrict access based on client IP address
- Custom error messages: End user error messages can be defined by administrator
- FTP Proxy: full FTP proxy functionality
- SOCKS v4/v5 proxy: Additional proxy service for IM and other SOCKS proxy applications
- Instant Messenger traffic control: Allow/disallow IM text, allow/disallow file transfer/voice/video (by file type, size or global), allow/disallow chat room, log and action (kill message, email management) on keywords in IM stream.
- Automatic Account Lockout: user accounts are automatically disabled after the number of wrong password attempts reaches a threshold.

The following capabilities of SGOS are present in the appliance, but were explicitly excluded from the evaluation:

- Streaming
- QuickTime Proxy
- DNS Proxy
- Telnet Proxy
- Off box content filtering
- Off box virus scanning
- SSL termination
- Remote management (browser, ssh, telnet)
- Bridging (hardware or software)
- Dynamic or Static Bypass
- Refresh and Pipelining
- ICP and WCCP
- Visual Policy Manager
- Attack-detection

- Authentication realms other than “local”
- Clusters, fail-over, chained proxies
- RADIUS or TACACS+ splash pages
- Content-management commands
- Syslog, Health checks, SNMP, Heartbeats and Diagnostics
- <forward> policy
- authenticate.mode() settings other than as described in the ST
- Encrypted access logs

The TOE is designed to protect the user’s network by restricting external access from certain specified sources (URLs) and protocols, i.e. HTTP, FTP, SOCKS and AIM, MSN and Yahoo Instant Messenger. Conversely the TOE is also designed to prevent internal user access to certain specified external sources (URLs) and the same protocols. Both internal and external source restrictions are specified by the Console Administrator during set-up. Likewise the Console Administrator can specify the internal and external protocol restrictions. The TOE can only ensure these functions if the connectivity between the Internal and External networks is configured to direct all the traffic for those protocols through the network appliance on which the TOE resides. The TOE does not make claims about other protocols. Any potential filtering of those protocols must be done by other means. Moreover, the TOE might not be involved with and hence does not ensure the protection of internal user identities/ IP addresses through those other protocols.

6 Architecture Information

The TOE is software that is part of an operating system that is delivered on a proprietary hardware device. The TOE relies upon features within the operating system to pass network traffic to the TOE, to provide the system time for auditing, and to provide protection of the TOE from tampering other than through the TOE interfaces that are presented to the end users. The TOE implements its own self protection for the interfaces that it presents to the end users.

The TOE is architected into subsystems and groups of subsystems. There are four subsystems groups: Proxy, Administration, Policy, and Support. The first three of these subsystem groups are implemented by single subsystems that bare similar names: Proxy Subsystem, Administrator Subsystem, and Policy Subsystem. The Support subsystem group is further decomposed into four subsystems: the Authentication Subsystem, the Content Filtering Subsystem, the Logging Subsystem, and the Registry Subsystem. Further details about the system architecture are proprietary to the vendor and will not be provided in the report.

In order to act as a proxy and control restricted protocol traffic from the Internal Network to the External Network, all restricted protocol traffic must flow through the appliance. Arranging for controlled protocol traffic to flow through the appliance requires proper configuration of the organization’s network environment to ensure that there are no other access modes to any network device. There are two kinds of network deployments: explicit and transparent. In an explicit deployment the users’ client software is configured to access the External Network via the proxy. The client software presents

the traffic to the Internal Network port of the proxy for service. In a transparent deployment the network and proxy are configured so that the proxy can intercept controlled protocol traffic intended for the External Network. This traffic is presented to the Internal Network port on the proxy. The users' software is not changed and the user may be unaware that controlled protocol traffic is traversing the proxy.

After initial configuration via the Setup Console, the TOE is operational and behaves as a proxy that denies all traffic as the default. To enable controlled protocol traffic flow, an administrator defines information flow policy rules, which comprise the Proxy SFP. The policy rules that define the Proxy SFP and Administrative Access SFP are expressed using the syntax and rules of the CPL.

The assets of the TOE are the local user list, the Proxy SFP Rules, the Administrative Access SFP Rules, the audit logs, and the system configuration. The two primary security capabilities of the TOE are restricting controlled protocol traffic between the networks and managing the SGOS. The tangible assets and management functions are protected by restricting access to administrators. Only administrators can log into the TOE CLI, access its configuration and configure policies.

The TOE protects the IP addresses of Internal Network machines and protects these machines from malicious content delivered via controlled protocols. An End User's Internal Network IP address is obfuscated by SGOS when their controlled protocol traffic is sent to the External Network. Also, malicious content carried by controlled protocols from the External Network can be blocked by the Proxy SFP.

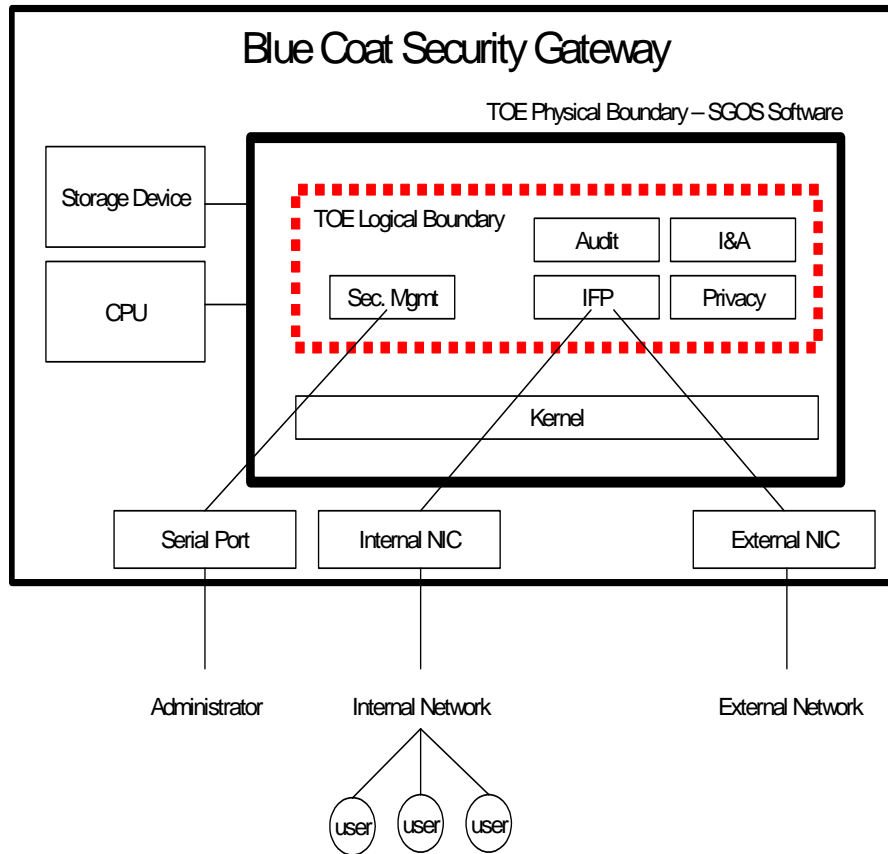


Figure 2 - Architecture Diagram

SGOS is delivered on one of several appliances manufactured by Blue Coat Systems. These included the SG400 line, SG800 line and the SG8000 line of products. Every appliance runs the same software, the TOE. All access to the appliance via internal ports and NIC ports passes through the TOE portion of the appliance operating system.

7 Product Delivery

The TOE is a software product that is delivered preinstalled on a Hardware Appliance along with some hard-copy documentation and a CD-ROM. The purpose of the appliance is to operate the TOE and act as an Internet proxy for the network and its users. Table 2 below lists the valid hardware options for the evaluated TOE. To obtain the SGOS product from Blue Coat, the customer must specify both the hardware platform and the version of SGOS that they want to have preconfigured onto the platform. To obtain the evaluated version of the TOE, the customer must specify one of the platforms listed in Table 2 and they must specify that they want the evaluated version of Blue Coat ProxySG Operating System, i.e. version 3.2.4.8 installed on the appliance.

Table 2 : Product Hardware Platforms

Model	WAN bandwidth	Disk	RAM	Interfaces	Number of users	Size
400-0	1.5 MBit/s	40 GB	256 MB	2 10/100 Base T	100	1U
400-1	1.5 MBit/s	80 GB	512 MB	2 10/100 Base T	100	1U
800-0	1.5 MBit/s	18 GB	512 MB	2 10/100 Base T	100	1U
800-0B	3 MBit/s	36 GB	768 MB	2 10/100 Base T	200	1U
800-1	4 MBit/s	72 GB	1 GB	2 10/100 Base T	400	1U
800-2	8 MBit/s	144 GB	1.5 GB	2 10/100 Base T	700	1U
800-3	10 MBit/s	288 GB	2 GB	2 10/100 Base T	1500	1U
8000-1	35 MBit/s	146 GB	1 GB	4 integrated 10/100/1000 on board ports, optional fiber available	1500	4U
8000-2	45 MBit/s	288 GB	2 GB	4 integrated 10/100/1000 on board ports, optional fiber available	3000	4U
8000-3	80 MBit/s	434 GB	3 GB	4 integrated 10/100/1000 on board ports, optional fiber available	5000	4U
8000-4	90 MBit/s	576 GB	4 GB	4 integrated 10/100/1000 on board ports, optional fiber available	8000	4U

Differences in each model are to allow for different performance and scalability requirements in each customer site. All models use motherboards with Intel processors. Differences in throughput are driven by processor speed, number of processors, amount of memory, and number and size of disks within each product. In addition, the SG8000 product line offers redundant power supplies and multiple Gigabit Ethernet network interface cards with optional fiber cards.

The following documentation is delivered in hard-copy form along with the SGOS appliance.

- A Quick Start Guide for the delivered platform. Depending upon the platform chosen one of the following three documents:
 - SG 400 Series Port80 Security Appliance Quick Start Guide, Rev 00A 01/2003 document number 231-02651
 - SG 800 Series Port80 Security Appliance Quick Start Guide, document #231-02589, Revision:00D 04/2004
 - SG 8000 Series Port80 Security Appliance Quick Start Guide, document #231-02710, Revision:00B 05/2004
- License Key

Additional evaluated documentation is provided for Set-up, Administration and User guidance on the delivered CD. The following documentation is available on the CD:

- Blue Coat Systems Port80 Security Appliance Configuration and Management Guide, document #231-02629, Revision:2.1.07 04/28/2003 [12]
- User Guidance Blue Coat Systems ProxySG Operating System 3.2.x, Revision 1.[13]

- Blue Coat Systems Port80 Security Appliance Content Policy Language Guide, document #231-02586, Revision:2.1.07 03/07/2003 [11]

In addition, the following evaluated documentation is also on the delivered CD for the Series 800 hardware platform:

- CacheFlow Security Gateway 800 Series User's Guide, document #231-02587, Revision:1a 05/2002 [14]

8 IT Product Testing

Testing of the evaluated configuration was performed at COACT lab on June 23, 2005. The testing was conducted by CCTL evaluators and observed by 2 Validators. A vendor representative was also present for the testing, but did not participate in any of the actual testing or test analysis. Figure 3 : Test Configuration illustrates the test configuration. The Client was a Windows 2000 Professional PC configured with Microsoft Internet Explorer 6.0 SP1, an FTP Client, and Yahoo IM. The Management workstation a Windows XP Professional PC configured with Microsoft IE 6.0 SP1, Hyperterminal, NMAP, and Ethereal. The Management workstation was connected to the internal network through its Ethernet interface and it was also connected to the TOE through a serial connection that served as the Console connection. The External server was also a Windows XP Professional PC configured with Microsoft IE 6.0 SP1, Bison FTP Server, NMAP, and Yahoo IM. The hardware platform for the tested TOE was a Blue Coat SG400 Series Port80 Security Appliance. Screen captures on the Client and Management workstation were used to record test results for evaluation records.

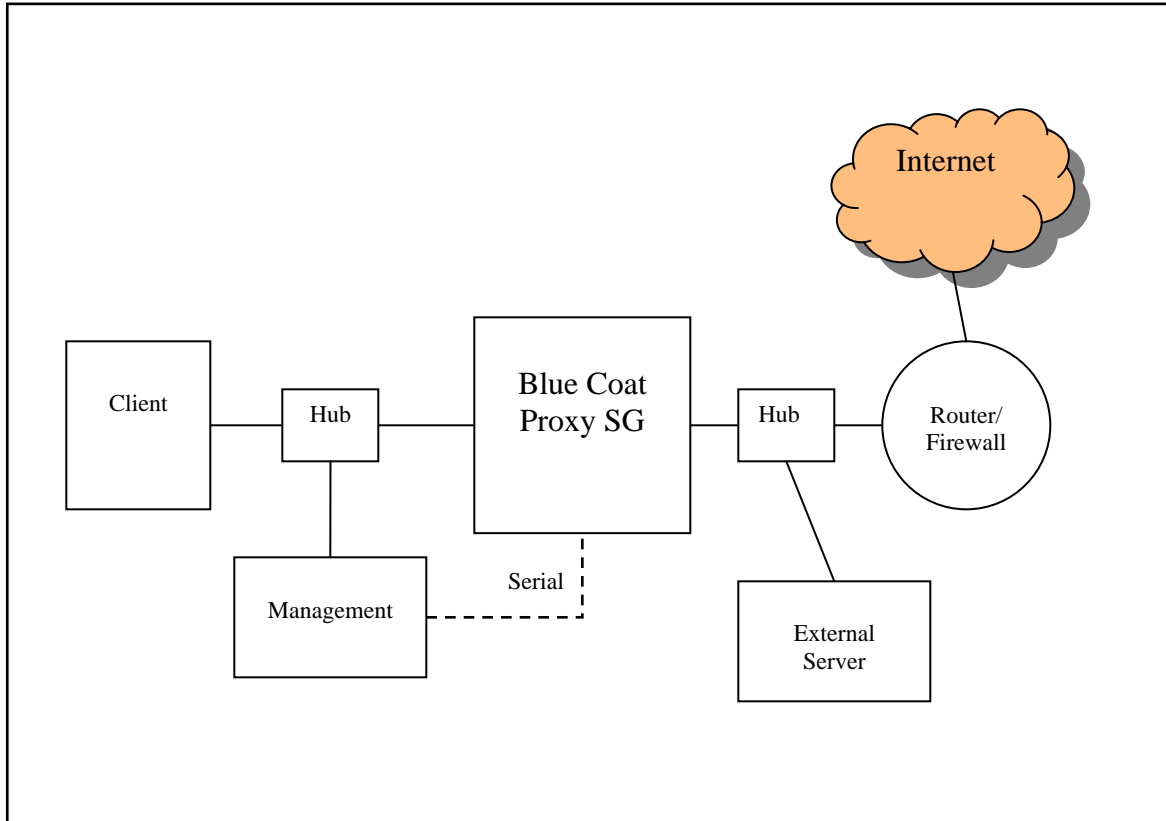


Figure 3 : Test Configuration

Testing of the evaluated configuration was performed at COACT lab on June 23, 2005. The testing was conducted by COACT staff evaluators and observed by two Validators. A vendor representative was also present for the testing, but did not participate in any of the actual testing or test analysis. The evaluators setup a test network and used the Security Console to create a series of restricted access user configurations. Function Tests were made for proper access before access restrictions, while access restrictions were in force and after access restrictions were lifted. Both Security Console access restrictions were tested and Command Line Interface access configurations. The evaluators also performed duplicate developer tests and penetration testing. The tests covered the full spectrum of vendor testing, set-up, operation and functional performance. Test results were confirmed via frequent data extractions and retained screen snapshots and as printed records.

Penetration testing was based on a rigorous evaluation of the developers' Vulnerability Analysis plus an independent search for other vulnerabilities. The evaluation team found most of the developers' Vulnerability Analysis to be satisfactory without any supplemental testing. The evaluators did developed five additional penetration tests. One of those tests, for a buffer overflow technique, was designed to supplement the vendor analysis and the other four tested additional potential penetration attacks that the evaluators identified during their analysis of the other TOE evidence.

The end result of the testing activities was that all tests gave expected (correct) results. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST. The Penetration Test results showed that attempts to overflow buffers did not adversely affect the TOE. In all case the TOE denied access to the network.

9 Evaluated Configuration

9.1 TOE

This section documents the configuration of the IT product during the evaluation. The evaluated configuration consists of the Blue Coat Appliances listed in Table 2 with Blue Coat ProxySG Operating System v3.2.4.8 preinstalled. The security functionality of SGOS that was included in the evaluation is summarized in the Clarification of Scope section (page 10) of this report and is describe in further detail in the ST.

9.1.1 Physical Boundary of TOE

The TOE consists of some software components of the Blue Coat ProxySG Operating System. The TOE resides within the physical boundaries of SGOS on the hardware appliance platform. The physical boundary of the TOE is illustrated in Figure 2 - Architecture Diagram on page 13 That figure illustrates key aspects of the hardware and software that are outside of the scope of the TOE boundary as well as showing that the TOE is confined within the hardware that is acquired with the TOE.

9.1.2 Logical Boundary of TOE

The logical boundary of the TOE is the defined by the security mechanisms that the TOE provides. The logical boundary is also illustrated in Figure 2 - Architecture Diagram on page 13. The ST defines the TOE supplied mechanisms as:

Security Audit: The TOE has two separate auditing capabilities to provide an audit trail of security relevant events. These are System Event Logging and Access Logging

Configurable Security Policies: The TOE provides the administrator with the ability to define security policies using the ProxySG Content Policy Language (CPL). There are two types of policies that are enforced by the TOE: Administrative Access Control Policies and Information Flow Protection (IFP) Polices.

Identification and Authentication:

The TOE provides mechanisms for the authentication of administrators and end users.

Security Management:

The TOE provides a mechanism to manage the TOE based upon two administrative roles: ordinary administrators and the console administrator.

Privacy:

The TOE includes a mechanism to ensure that the only IP address sent out by the TOE to the External Network is the external interface IP address of the TOE appliance itself. The Internal network IP addresses of users are never transmitted on the External Network.

9.2 IT Environment

The underlying hardware and portions of the operating system for the TOE are part of the IT Environment, but they are included in the appliance products that one must purchase to obtain the TOE. Hence there is no other special equipment that one must separately acquire to install the TOE in its evaluated configuration. The underlying platforms for the evaluated version of the TOE are listed in Table 2 : Product Hardware Platforms

10 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document contains the verdicts of "PASS" for all the work units.

The evaluation determined the product to be conformant with Part 2 extended and, as well, meeting the requirements for Part 3, and EAL 2. The details of the evaluation are recorded in the proprietary Evaluation Technical Report (ETR), [10] which is controlled by COACT Inc.

11 Validator Comments

This evaluated TOE consists of only a portion of the product that is delivered with the network appliance. Much of the evaluation that was performed would have been exactly the same if the same security mechanisms had been evaluated but the entire network appliance had been included in the evaluation. The vendor choose to exclude portions of the platform from the TOE because it gave them more flexibility in adjusting to future changes in the availability of hardware components within the platform.

However, this was at the expense of replacing some standard CC SFRs with some explicitly defined SFRs.

The TOE controls access and protects internal network users from interaction with a limited set of Internet protocols, i.e. HTTP, FTP, SOCKS and AIM, MSN and Yahoo Instant Messenger. Internal network device identification (IP address) is also protected by the TOE. Protection is only assured by this evaluation if all access to the internal network is through the Blue Coat appliance. If additional protocols need to be filtered, then additional filtering devices and possibly other paths to the external network may be necessary. If some devices on the internal network have alternate connections to the External Network, then further analysis of the network architecture and protection mechanisms would be required to ensure that the protections provided by the TOE could not be bypassed through those other network connections.

As listed in Clarification of Scope section on page 10 the Blue Coat ProxySG Operating System, v3.2.4.8 has additional functions but these were not part of the ST and were not evaluated during TOE testing. This evaluation makes no claims about the effectiveness of those mechanisms.

12 Security Target

The Security Target, *Blue Coat ProxySG Operating System, v3.2.4.8 Security Target, dated July 7, 2005* [9] is included here by reference.

13 Glossary

AIM	
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CPL	Content Programming Language
DBMS	Database Management System
DLL	Dynamically Linked Library
DNS	Domain Name System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transport Protocol
I&A	Identification and Authentication
ICP	Internet Cache Protocol
IFP	Information Flow Protection
IP	Internet Protocol
IT	Information Technology
MIME	Multi-Purpose Internet Mail Extension

MSN	Microsoft Network
NIAP	National Information Assurance Program
NIC	Network Interface Card
NIST	National Institute of Science & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
SGOS	Blue Coat ProxySG Operating System
SNMP	Simple Network Management Protocol
SOCKS	Socket Secure (server)
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
ST	Security Target
TACACS	Terminal Access Control Access Control System
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
URL	Universal Request Locator
WCCP	Web Cache Communication Protocol

14 Bibliography

- [1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.
- [2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.
- [3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.
- [4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.
- [5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6
- [6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.
- [7] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.
- [8] Common Criteria Evaluation and Validation Scheme for Information Technology Security Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, February 2002

Blue Coat ProxySG Operating System v3.2.4.8 Validation Report

[9] Blue Coat ProxySG Operating System, v3.2.4.8 Security Target, dated July 7, 2005

[10] Blue Coat ProxySG Operating System v3.2.4.8 Evaluation Technical Report, Document No. F2-0705-002, Dated August 8, 2005

[11] Blue Coat Systems Port80 Security Appliance Content Policy Language Guide, document #231-02586, Revision:2.1.07 03/07/2003

[12] Blue Coat Systems Port80 Security Appliance Configuration and Management Guide, document #231-02629, Revision:2.1.07 04/28/2003

[13] User Guidance Blue Coat Systems ProxySG Operating System 3.2.x, Revision 1.1

[14] CacheFlow Security Gateway 800 Series User's Guide, document #231-02587, Revision: 1a 05/2002