

BCCPA v 3.0.3 Chapter Summaries

This document gives brief summaries of the chapters in the Blue Coat Certified Proxy Administrator(BCCPA) textbook.

Chapter 1: Understanding Proxy Servers

This chapter explains what a proxy server is and how it is an important part of securing your private network. You will learn how a proxy server complements a firewall to fully secure your internal network. Also discussed in this chapter are various features of the ProxySG, such as caching, content filtering, WAN acceleration and SSL interception. Features that aid the ProxySG in acting both as a gateway proxy and a WAN acceleration proxy are also covered in this chapter.

Chapter 2: Blue Coat Product Family

This chapter provides an overview of all of Blue Coat's hardware and software products and how they work together to enable organizations to protect and enhance the performance of their networks. Specifically, the chapter introduces the ProxySG, ProxyAV, Blue Coat Director, and Blue Coat RA, the company's new SSL VPN appliance. The chapter also introduces Blue Coat Reporter and Web-filtering applications.

Chapter 3: WAN Optimization Features

IT managers work to achieve a complex goal: increasing efficiency while providing better control and security — while minimizing costs. Organizations can reach that goal by taking advantage of the MACH5 application-acceleration features in the Blue Coat SGOS. The chapter provides an introduction to the rest of the course by outlining the key elements of MACH5: bandwidth management, protocol optimization, object caching, byte caching, and compression.

Chapter 4: SG Deployment

This chapter describes what a proxy is, what it does, and how a proxy, particularly the ProxySG, can be deployed. Various deployment methods are examined: forward proxy, reverse proxy, configuring a transparent proxy and an explicit proxy. The chapter also discusses configuring the ProxySG transparently using the default gateway, bridging mode, WCCP and layer 4 switch. Details on configuring the ProxySG explicitly using the proxy auto config file and the Web proxy auto discovery methods are also discussed.

Chapter 5: Licensing and Upgrading the SG

This chapter focuses on what a customer must do to license their Blue Coat products and what behavior they should expect from their Blue Coat products in regards to the license. An overview of the basic information that each customer should know about the Blue Coat licensing system is provided. You will learn what types of licenses Blue Coat offers, which products have what type of license, and how each type of license is acquired. Additionally, you will learn what happens when the limitations of a license is exceeded and what happens when a license expires.

Chapter 6: SG Initial Setup

This chapter walks you through the steps you need to complete when setting up the ProxySG for the first time. Some of the concepts of initial configuration also apply to reconfiguring an existing ProxySG, or one that has been restored to factory-default settings.

Chapter 7: SG Management Console

This chapter introduces the ProxySG graphical user interface, which is how users most commonly work with their appliances. It focuses on the Management Console and its various features, which students use extensively during lab exercises.

Chapter 8: Policy Management

This chapter expands on the concepts presented in the ProxySG Graphical User Interface chapter. It explains how policies are created to enforce an organization's rules for acceptable Web use. This chapter also illustrates why only a secure proxy with an object-handling operating system can offer the framework needed to identify and enforce policies across an entire enterprise.

Chapter 9: Services

This chapter introduces the Service feature, which determines which traffic is allowed or restricted through the ProxySG. It focuses on the Console Services and the Proxy Services, available through the Management Console. The chapter also discusses the service ports, service port actions and proxy service attributes in detail.

Chapter 10: Hypertext Transfer Protocol (HTTP)

This chapter describes HTTP and how it is used to transport information across the Internet. It provides an introduction to HTTP concepts and terminology and describes how it is used to deliver content across the Web.

Chapter 11: Authentication Introduction

This chapter details the kind of authentication challenges handled by the ProxySG in explicit proxy mode. You will learn how you can control access to the ProxySG, how the ProxySG challenges users before forwarding their requests, and how it passes challenges and credentials between the OCS and user agent.

Chapter 12: Authentication Realms

The ProxySG supports a wide, and constantly growing, number of authentication realms. This chapter focuses on the most commonly used realms — NTLM, LDAP, and Local — and introduces sequence authentication, the method for searching multiple realms for a specific user's credentials.

Chapter 13: Content Filtering

This chapter introduces the fundamentals of content filtering, both onbox and offbox. It also discusses Blue Coat Web Filter, which takes a hybrid approach to content filtering. It maintains a local database of categorized sites but also requests updates from a network of servers if it does not find the categorization locally.

Chapter 14: Instant Messaging Filtering

Instant Messaging (IM) has become a useful tool in the enterprise, enabling co-workers to communicate quickly and easily. However, IM also raises security concerns. This chapter discusses how the Blue Coat SG helps an organization maintain control over the communication through instant messaging (IM).

Chapter 15: Creating Notifications and Exceptions

This chapter outlines how administrators can create custom Web pages to inform network users about the organization's acceptable user policy (AUP). Notifying users why they cannot access a resource can reduce the number of unnecessary calls to the organization's help desk from users.

Chapter 16: Access Logging

This chapter explains what access logs are, how they are used, and describes the various access logging features on the ProxySG. It also provides an overview of access logging and explains some common log file terminology.

Chapter 17: Introduction to Blue Coat Reporter

This chapter presents an overview of the Blue Coat Reporter, a powerful reporting tool that provides fast and easy log file importation from the ProxySG with more than 150 pre-defined reports. Reporter's identity-based reporting on Web communications enables enterprises to evaluate Web policies and manage network resources more effectively.

Chapter 18: Blue Coat Reporter Installation

Blue Coat Reporter installation can be done in many ways depending on the version you plan to install. This chapter presents an overview of installing Reporter, Reporter Sizing Guide; a tool you can use while deploying Reporter in your organization, hardware guidelines and first time access to Reporter. This chapter also talks about accessing Reporter over HTTP and HTTPS, creating and managing data profiles and how to upgrade your existing version of Reporter to the most current version of 8.3.2.2.

Chapter 19: Blue Coat Reporter Graphical User Interface

The Administrative menu is the graphical user interface for setting up various parameters in Reporter. This chapter walks you through the various sub menus available under the Administrative menu. Detailed sections on Data Profiles, Scheduler option, Configuring Users and Settings and finally Licensing Reporter are discussed here.

Chapter 20: Introduction to ProxyAV

This chapter introduces the Blue Coat AV, Blue Coat's virus-scanning appliance. Traditional, Web antivirus gateways often lack scalability and performance for HTTP and FTP scanning, which leaves desktops vulnerable. The Blue Coat AV, combined with the Blue Coat SG, provides scalability for virus scanning, plus complete visibility and control of enterprise Web communications.

Chapter 21: ICAP Fundamentals

This chapter provides a brief introduction to ICAP, explains what ICAP means to the future of Internet content handling, and discusses how ProxySG is ideally suited to handle these ICAP enabled value-added services. In other words, ICAP allows its clients to pass HTTP based (HTML) messages (Content) to ICAP servers for adaptation. Also discussed in the chapter are ICAP REQMOD, ICAP RESMOD, Patience page and Trickling features of the ICAP client.

Chapter 22: Service and Support

This chapter provides a high-level overview of the support options that are available to Blue Coat customers worldwide. It outlines the different levels and types of service, including online access to open, review, and comment on technical support cases.

Appendix A: Deployment Planning

Planning and designing the most efficient deployment is the most important decision you have to make, second only to the one of actually buying the ProxySG. This appendix gives detailed information about different kinds of ProxySG deployments.

Appendix B: Conditional Probability — Bayes Theorem

Modern content-filtering technology, as well as spam e-mail detection, relies on some fundamental theorems of statistical analysis. This appendix discusses, at a very high level, the Bayes Theorem, which enables you to determine the probability of a future event based on knowledge that a different event already occurred.

BCCPP v 3.0.3 Chapter Summaries

This document gives brief summaries of the chapters in the Blue Coat Certified Proxy Professional(BCCPP) textbook.

Chapter 1: System Architecture

ProxySG architecture is complex and evolves continually to support new and better features. This chapter discusses how the ProxySG handles transactions, analyzes and processes policy and cache content. You can use the information in this chapter to better understand ProxySG sizing.

Chapter 2: Advanced Services — TCP Tunnelling

This chapter formalizes what TCP tunnelling is and how you should use with the edge-core deployment scenario in mind. TCP tunneling, which already existed in several previous releases, is now more effective because it can be combined with byte caching and gzip compression to reduce bandwidth and increase performance. It is useful for detecting peer-to-peer connections going over open ports on the firewall.

Chapter 3: Content Policy Language

This chapter covers the structure and syntax of Content Policy Language (CPL). Numerous examples will help you will learn proper usage and best practices. The chapter also discusses policy files used by the ProxySG.

Chapter 4: Regular Expressions

After giving a brief history of regular expressions, this chapter discusses the syntax of the Blue Coat implementation of Perl Compatible Regular Expressions (PCRE). The chapter gives many examples and discusses performance issues arising from their use.

Chapter 5: Managing Downloads and Apparent Data Type

As users download seemingly safe content such as music files, they may unknowingly download viruses, Trojans, or malware. This chapter describes how you can protect your network from these hidden dangers. Details on the possible tampering of MIME types and its consequences are also discussed. To overcome this tampering of the MIME types, a unique technique called Apparent Data Types is used. ProxySG allows you to create policies based on the actual file signature and thereby eliminating the abovesaid issue.

Chapter 6: Policy Tracing

This chapter expands on the concepts presented in the VPM chapter. It explains how policies are created to enforce an organization's rules for acceptable Web use. This chapter also illustrates why only a secure proxy with an object-handling operating system can offer the framework needed to identify and enforce policies across an entire enterprise.

Chapter 7: HTTP Details

This chapter looks at HTTP in detail to show how you can use HTTP to perform special redirection. It shows practical examples of how administrators use redirection, authentication, and cookies to accomplish their business goals. This chapter is fundamental to understanding how ProxySG manages authentication in transparent proxy mode.

Chapter 8: Using Authentication in Transparent Proxy Mode

Authentication in transparent proxy deployments is a challenge. This chapter discusses how the ProxySG authenticates users in a scenario where HTTP 407 is not available, without the user receiving multiple authentication requests.

Chapter 9: Using Kerberos Authentication

In this chapter, you will explore the system requirements and configuration necessary to support Kerberos authentication with the ProxySG. This chapter also focuses on configuring the ProxySG and Blue Coat Authorization and Authentication Agent (BCAAA) to support Kerberos authentication.

Chapter 10: Substitution Realm

This chapter discusses the policy substitution realm, a best- effort method for identifying users based on information available in the request that a client makes to the ProxySG. You will learn how the policy substitution realm to identify users under a variety of circumstances.

Chapter 11: Windows SSO

Authentication in transparent proxy deployments is a challenge. This chapter discusses how the ProxySG authenticates users in a scenario where HTTP 407 is not available, without the user receiving multiple authentication requests.

Chapter 12: Advanced Authentication

This chapter is designed to both dive into the details on how ProxySG handles the authentication process and as a primer for the Guest Authentication feature. The complexity pertaining to authentication is that ProxySG is a multi protocol device. A single user can be using a web browser, have an ftp download going, chatting through IM, and streaming a video all from the same desktop. The chapter guides the student to understand how the proxy deals with the different scenarios. Also discussed in the chapter are details on surrogate credentials , inactivity timer during authentication and the authentication model that ProxySG is based on.

Chapter 13: Guest Authentication

This chapter discusses the ability of ProxySG appliance to allow access to unauthenticated or unauthorized (or both) users even when there are authentication policies in place. The chapter walks the students through a detailed understanding of the features and functionalities that the ProxySG appliance makes available to the administrator. The chapter also discusses persistent connection , best practices to be followed while authenticating and a possible troubleshooting scenario.

Chapter 14: SSL Proxy

This chapter provides an introduction to the Blue Coat SSL proxy. HTTPS, which is HTTP over SSL, offers secure communication between a client and a server. Unfortunately, malicious internal users and Web sites can retrieve or distribute inappropriate content over HTTPS. This chapter discusses how SSL proxy overcomes these security challenges.

Chapter 15: Bandwidth Management

Bandwidth Management, one of the elements of MACH5, allows you to give users access to resources while limiting the total amount of bandwidth that they use. It also allows you to set priorities for those resources. This chapter explains how bandwidth management works and how to implement it to improve network performance.

Chapter 16: Introduction to Streaming Media

Streaming has become fairly broad in definition and now generally refers to media, such as video and audio, that is delivered over a network. The data associated with multimedia applications can be, and usually is, quite complex. This chapter looks into the fundamental concepts of streaming media, streaming media model, ProxySG supported clients and formats. Also discussed in this chapter is the way the streaming content gets processed into unicast and multicast modes.

Chapter 17: Managing Streaming Media

This chapter describes how using the ProxySG appliance for streaming delivery minimizes bandwidth use by allowing the ProxySG appliance to handle the broadcast and allows for policy enforcement over streaming use. The delivery method depends on if the content is live or video-on-demand.

Chapter 18: Forwarding

Forwarding is the ability to forward Web requests to other appliances before sending the request to an origin server. This chapter describes how forwarding can be used to provide administrators with the flexibility to define scalable proxy-hierarchy designs. It also shows how students can create forwarding commands.

Chapter 19: Reverse Proxy — Implementation

This chapter expands on the reverse proxy concepts discussed in the Blue Coat Certified Proxy Administrator (BCCPA) course. It explains typical reverse proxy deployments and describes the many benefits of the ProxySG reverse proxy.

Chapter 20: Two-Way URL Rewrite

This chapter discusses two-way URL rewrite (TWURL), a way to ensure the consistency and accuracy of links served by the ProxySG to the client and headers from the ProxySG to the server. TWURL is an important tool in successfully implementing a reverse proxy deployment.

Chapter 21: Failover

Today's networks require total device availability; downtime is not an option. To guarantee continuity of service, a failover mechanism is required. The ProxySG offers the capability to implement a redundant configuration of Blue Coat secure proxy appliances. This chapter describes failover, how it is used, and how it is configured.

Chapter 22: Access Logging-Advanced Topics

This chapter focuses on two important advanced topics in access logging: log formats and security. After reviewing the basics of the access logging, the chapter discusses the various formats available for access logs and explains how to improve security by encrypting and digitally signing access logs.

Chapter 23: Web Cache Communication Protocol(WCCP)

The Web Cache Communication Protocol (WCCP) was developed by Cisco Systems and specifies interactions between one or more routers (or Layer 3 switches) and one or more Web caches. The purpose of the interaction is to establish and maintain a transparent redirection of selected types of traffic flowing through a router. This chapter walks you through how Web traffic can be transparently redirected to the ProxySG from a Cisco router allowing comprehensive Web policies to be implemented for the enterprise.

Chapter 24: Health Checks

The goal of this chapter is to describe the function of Blue Coat's health check, why it is important and useful, and how it works. The main function of health checks is to allow Blue Coat customers to monitor their external resources that work with Blue Coat products. Customers are able to monitor many resources such as SOCKS gateways and Websense off-box services.

Chapter 25: Blue Coat SG Security

This chapter presents a brief introduction to the various methods of securing access to ProxySG. It describes the security benefits of each method and shows you how to use the CPL (Content Policy Language) to achieve maximum security.

Chapter 26: Introduction to Blue Coat Director

This chapter explains how organizations with multiple ProxySG appliances can benefit by using Blue Coat Director. It shows how Director can be deployed and how administrators can use it to manage ProxySG configurations, set policy, distribute and control Web content, and perform backups.

Chapter 27: Introduction to Blue Coat Remote Access(RA)

Blue Coat RA is an on demand SSL VPN that provides secure remote access for employees, partners and customers. With integrated endpoint security and information protection features and no VPN client software or local Admin rights required, Blue Coat RA provides an ideal remote access solution for extending applications and resources to users on unmanaged endpoints that are beyond the reach of IPsec VPNs and traditional SSL VPNs. Blue Coat RA is the industry's only application-independent architecture and utilizes patent-pending on demand Connector technology.

Appendix A: Understanding Digital Certificates

The appendix gives details about asymmetric cipher, Public Key Infrastructure, digital certificates, and certification — topics essential in securing transmission of data over networks.

Appendix B: Blue Coat Authentication and Authorization Agent(BCAAA)

The appendix gives details about the basic components of the BCAA. Also discussed are BCAA's functionality details and authentication realms that are supported.

Appendix C: Understanding Kerberos Authentication

This appendix discusses the basic concepts behind Kerberos authentication. It also explains the differences between NTLM and Kerberos authentication realms. The chapter also focuses on Kerberos ticket structure, ticket granting ticket and ticket granting service in detail.