

BCCPP v 3.1.1 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 caches content. You can use the information in this chapter to better understand ProxySG hardware sizing.

Chapter 2: Caching Architecture

This chapter introduces the concept of caching, where copies of pages and files requested from the web are saved to reduce the time it takes to re-request them. This can reduce latency, provide bandwidth management, and prevent high loads on servers. The chapter also explains how caching is implemented in the ProxySG.

Chapter 3: Services — Advanced Topics

This chapter formalizes what TCP tunnelling is and how you should use with the edge-core deployment scenario in mind. TCP tunneling 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 4: 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 5: 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 6: 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 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: Authentication Agent

Because SGOS is proprietary to Blue Coat, it cannot run authentication software developed specifically for Windows, UNIX, or Linux systems. This chapter introduces the Blue Coat Authentication and Authorization Agent (BCAAA), which is used to pass authentication requests between ProxySG and the authentication database.

Chapter 10: 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 BCAA to support Kerberos authentication.

Chapter 11: Authentication Using LDAP

This chapter discusses Lightweight Directory Access Protocol, used by ProxySG to query realms for authentication. LDAP is flexible and enables software to locate users without knowing the exact location in a network topology. This chapter discusses not only how an LDAP realm is created on the ProxySG, but also how the ProxySG performs LDAP authentication.

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: ProxySG Security

This chapter explores the methods of direct access to the ProxySG, and the relative level of security involved in each: the console account, the console access control list, and the Content Policy Language. Also discussed are restricting access to a single IP, and role-based security.

Chapter 15: 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 16: Policy Tracing

This chapter 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 17: 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 18: 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 19: 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 20: 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 21: Web Cache Communication Protocol

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 22: 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 23: Managing Streaming Media

This chapter introduces the concepts behind streaming media, and describes how using the ProxySG appliance for streaming delivery minimizes bandwidth use. Allowing the ProxySG appliance to handle the broadcast allows for policy enforcement over streaming use. Also discussed are supported clients and formats and how ProxySG handles streaming media according to its delivery method.

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: ProxyClient

This chapter introduces ProxyClient, a thick client whose primary function is to accelerate application traffic over WAN with a ProxySG at the core. Covered in this chapter are the features and benefits of using ProxyClient in implementation for your mobile users or small remote offices.

Chapter 26: ProxyClient Filtering

This chapter goes into more detail about the content filtering options of ProxyClient, since filtering may be required for security and compliance reasons. After covering the benefits of using filtering and logging with ProxyClient, this chapter shows you how to configure for filtering and perform maintenance and troubleshooting.

Chapter 27: ProxyAV Architecture

The ProxyAV enables organizations to detect malware and mobile malicious code at the Web gateway. This chapter discusses the different structural components in ProxyAV and how they interact to scan data, report the presence or absence of viruses, and also upgrade the pattern files for virus scanning.

Chapter 28: ICAP Concepts

This chapter covers the Internet Content Adaptation Protocol (ICAP), the communication mechanism between the ProxySG and ProxyAV. After reviewing the fundamentals behind ICAP, this chapter discusses how an ICAP server is configured, how to use associated tools for scanning and delivering data, and how secure ICAP differs from plain ICAP.

Chapter 29: Introduction to 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.

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: 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.

Appendix C: Hierarchical Token Buckets

This appendix explains the bandwidth management scheme known as hierarchical token buckets, which splits traffic according to category and prevents overuse in one category's traffic from affecting the performance of another.