

# BCCPP v204 Chapter Summaries

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

## Chapter 1: System Architecture

Blue Coat SG architecture is complex and evolves continually to support new and better features. This chapter discusses how the Blue Coat SG handles transactions, analyzes and processes policy and cache content. It also discusses how the Blue Coat SG can enhance Web performance and offers some tips for using older generation firewalls or routers.

## Chapter 2: 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 Blue Coat SG.

## Chapter 3: 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 4: Apparent Data Type

This chapter discusses the advantages of controlling file downloads by a file's apparent data type, thereby preventing the installation of spyware on your network resources. This chapter also focuses on apparent data type triggers and available apparent data type lists.

## Chapter 5: 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 Blue Coat SG manages authentication in transparent proxy mode.

## Chapter 6: HTTP Compression

HTTP compression is an algorithm that reduces the size of the file without causing loss of data, improving network efficiency and performance. In addition to teaching you how to implement HTTP compression, this chapter discusses how compressed objects can be stored in variant forms and how the Blue Coat SG can modify compressed content.

## Chapter 7: 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 8: 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 9: TCP Tunneling

This chapter discusses TCP tunneling, which allows you to configure the Blue Coat SG to terminate connections for any protocol on any TCP port. TCP tunneling - in conjunction with SOCKS compression- allows you to optimize traffic between your remote offices and your headquarters for mission critical applications.

## Chapter 10: Bandwidth Management

Bandwidth Management, one of the key 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 11: Application Delivery Network

This chapter discusses the Application Delivery Network (ADN), which uses byte caching to reduce the amount of TCP traffic across a WAN. ADN accomplishes this by replacing large chunks of repeated data with small tokens representing that data. This chapter also discusses the two-sided deployment that ADN requires.

## Chapter 12: Endpoint Mapper and MAPI Proxies

The Endpoint Mapper proxy is designed to manage Microsoft Remote Procedure Call (RPC) protocol requests and responses. It also used in optimizing Messaging API (MAPI) traffic between Blue Coat SG appliances. This chapter discusses RPC and explains how the Endpoint Mapper service works alone and with MAPI to intercept and accelerate RPC traffic.

MAPI is an RPC-based protocol used by Microsoft Outlook (client) to communicate with Microsoft Exchange (server). It enables the optimization of MAPI traffic between Blue Coat SG appliances at opposite ends of a WAN link. This chapter explains how MAPI works and how organizations can use it to accelerate e-mail across the enterprise.

## Chapter 13: CIFS Proxy

The Common Internet File System (CIFS) is popular in enterprise networks because it allows computers to share files and printers. However, CIFS is inefficient over low-bandwidth links or high-latency links, such as those typically found in enterprise branch offices. This chapter explains how the Blue Coat SG optimizes the CIFS protocol through object caching and pipe lining.

## 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: Managing Instant Messaging

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 16: Managing Peer-to-Peer Traffic

A company that allows employees to access peer-to-peer (P2P) networks may be held liable if its employees use the company's network resources to download and redistribute copyrighted content. This chapter explains how organizations can use the Blue Coat SG to detect and block P2P traffic.

## Chapter 17: 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 Blue Coat SG reverse proxy.

## Chapter 18: 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 Blue Coat SG to the client and headers from the Blue Coat SG to the server. TWURL is an important tool in successfully implementing a reverse proxy deployment.

## Chapter 19: 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 20: Advanced Reporter

This chapter focuses on the advanced features of Blue Coat Reporter such as log processing for v7 and v8 profiles, real time reporting, log filters and report filters. It also explains how reports can be customized through a Web interface.

## Chapter 21: Using Authentication in Transparent Proxy Mode

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

## Chapter 22: Understanding Kerberos Authentication

This chapter 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.

## Chapter 23: Using Kerberos Authentication

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

## Chapter 24: 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 Blue Coat SG. You will learn how the policy substitution realm to identify users under a variety of circumstances.

## Chapter 25: Windows SSO

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

## Chapter 26: Blue Coat SG Security

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

## Chapter 27: Failover

Today's networks require total device availability; downtime is not an option. To guarantee continuity of service, a failover mechanism is required. The Blue Coat SG 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 28: Blue Coat Director

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

## Chapter 29: Spyware Prevention

Spyware is a growing problem: It degrades computer and network performance, impairs productivity, and exposes enterprises to numerous risks. This chapter discusses how Blue Coat, with its proxy-based tools, offers enterprises a network-level, scalable solution for fighting spyware.

## 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.