

BCWAP v 3.0.3 Chapter Summaries

This document gives brief summaries of the chapters in the Blue Coat WAN Acceleration Professional (BCWAP) Course.

Chapter 1: Device Authentication

This chapter describes device authentication and how it is used in the Blue Coat implementation. Device authentication allows devices to identify one another, creating more secure communication and interaction. Device authentication helps to secure the network and the various protocols involved in them. The chapter also discusses the processes involved in certificate signing, obtaining an appliance certificate and the authorization procedure involved.

Chapter 2: ADN Connection Types

Blue Coat implementation of an Application Delivery Network (ADN) requires two-sided deployments, with an ProxySG appliance (a *peer*) at each end of the WAN link featuring byte caching and acceleration techniques. This chapter provides conceptual information regarding various deployments that employ WAN optimization. The various types of ADN connection tunnels — explicit, translucent and transparent tunnels, are also discussed in detail in this chapter.

Chapter 3: 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 4: Secure ADN

This chapter describes the concepts behind Secure ADN and how it is used. It explains how and why it is advantageous to the user to implement a secure ADN. This feature give customers the ability to enable SSL security for all ADN tunnel connections and routing connections, regardless of what traffic is being accelerated or tunneled by the ADN. Secure tunnels, admission control, possible configurations, and secure ADN for SSL traffic are discussed in this chapter.

Chapter 5: Asymmetric Routing

This chapter describes how to use the ProxySG TCP Connection Forwarding feature to resolve issues posed by asymmetric routing. Depending on the enterprise network configuration, asymmetric routing may occur on the outbound or inbound connections. Connection forwarding can resolve issues where TCP connections are dropped or timed-out because a device is not aware of connection state. Connection Forwarding allows ProxySG appliances to act as peers in a cluster that share TCP connection state information. The chapter discusses network scenarios where asymmetric routing may cause TCP connection issues, how these issues are resolved with ProxySG and where to find statistics on Connection Forwarding configurations on each ProxySG.

Chapter 6: ADN Load Balancing

Load balancing is a method of spreading work out over multiple devices. This is useful because it allows a network to deal with loss from latency. When a network is backed because there is too many users trying to use the same application, productivity goes down. With load balancing enabled, client requests are redirected to other routes and preventing this latency. The user request takes another path, relieving the load that would usually be handled by only one device and allowing that client request to reach the origin content server (OCS) in a quicker fashion.

Chapter 7: 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 8: Advanced Services — TCP Tunnelling

This chapter formalizes what TCP tunnelling is and how you should use it with the edge-core deployment scenario in mind. TCP tunnelling, 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 9: ADN — Advanced Topics

The core of the chapter is designed about the concept of dynamic dictionary sizing; in fact the early part of the chapter are designed mostly to prep the audience with the information necessary to better understand why this is an important modus operandi for the ProxySG and how it is implemented so effectively in the SGOS.

Chapter 10: Troubleshooting ADN

This chapter details how to define symptoms, identify problems, and implement solutions in generic ADN troubleshooting scenarios. There are many causes that can compromise ADN performances. For example, network connection failed, firewall session timer, routing loop, subnets not advertised, VPN tunnel fragmentation, etc. This chapter also talks about the various utilities an administrator can use to troubleshoot an ADN scenario. The `test adn` CLI command helps you to identify the ADN connection routes, modes, decisions, failures, and etc. in your ADN network.

Chapter 11: CIFS — Advanced Topics

ProxySG appliances utilizing MACH5 WAN Optimization allows IT organizations to secure and accelerate the delivery of business applications for all users across the distributed enterprise - including those in or near Internet gateways, branch offices, data centers, and even individual end points. As an integral part of the MACH5 WAN Optimization framework, CIFS Protocol Optimization can be implemented across the network to increase productivity and profits by improving user performance while reducing costs.

Chapter 12: Troubleshooting CIFS Proxy

This chapter details how to define symptoms, identify problems, and implement solutions in generic CIFS troubleshooting scenarios. CIFS is a very chatty protocol. A single user operation (for e.g., file open) can result in multiple CIFS transactions. Therefore, it is necessary to establish context in the trace to identify user operation and drill into the specific transaction that may be an issue with the protocol proxy. Some of the common troubleshooting scenarios include system integration problems, CIFS misconfiguration, network connectivity issues, oplock is not granted to user for concurrent access, SMB signing is enabled, etc.

Chapter 13: MAPI Proxy — Advanced Topics

MAPI Protocol Optimization is the use of in-depth knowledge of the Messaging Application Programming Interface (MAPI) protocol to accelerate user response time. By acting as a proxy between the client and server, and having a detailed understanding of how the MAPI protocol functions, ProxySG appliances can anticipate user requests, resulting in data retrieval before clients have even requested it. Due to the traditionally “chatty” nature of MAPI, the performance improvement can be considerable.

Chapter 14: VLAN Support

A Virtual Local Area Network (VLAN) is a logical broadcast domain that spans multiple physical LAN segments. Unlike the routers which split the network based on its geographical location, VLANs can logically group switch ports and their connected users by functions, departments, or applications. The details that go into VLAN tags, trunking, asymmetric trunking and some possible deployment situations are covered in this chapter.

Chapter 15: 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 16 : Quality of Service

Quality of Service (QoS) is a technique used to prioritize network traffic. Blue Coat’s MACH5 technology supports the QoS prioritization technique used by network devices that works by setting Type of Service (ToS) bits in the IP header of packets. By preserving or manipulating ToS information and using Bandwidth Management classes, administrators can use specific triggers and actions to set priority and assign resources to different types of traffic flow.

Chapter 17: 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 18: Managing Content Delivery Networks

This chapter describes the various processes that go behind managing a content delivery network (CDN). A content delivery network uses a combination of many networking technologies to effectively deliver content between geographically dispersed networks. An attempt to correlate the terminologies with various Blue Coat products and understand the basic processes behind each component of the CDN is made. This chapter also describes the differences before and after the advent of CDN technologies and the advantages of subscribing to or implementing a CDN in a corporate set up.

Chapter 19: WAN Optimization Deployment Scenarios

The purpose of this chapter is to provide students with a sense of how versatile the ProxySG appliance really is. The case studies described in the chapter show how the ProxySG appliance can solve a variety of problems that can arise from an even wider variety of other issues, such as network topology, WAN limitations, and geography. In all the scenarios presented, Blue Coat was able to provide the customer exactly what they needed and more. WAN acceleration happened in all cases, with significant gains in bandwidth capacity being seen. This happened on many different internal and external, business-critical applications.

Appendix A: Understanding Byte Caching

This appendix describes in detail what byte caching is. Regardless of name, byte caching is a technique for replacing repetitive streams of raw application data with shorter “tokens” prior to transmission over the network. Because byte caching is not protocol specific, it can be performed on all TCP traffic completely transparent to the client and servers..