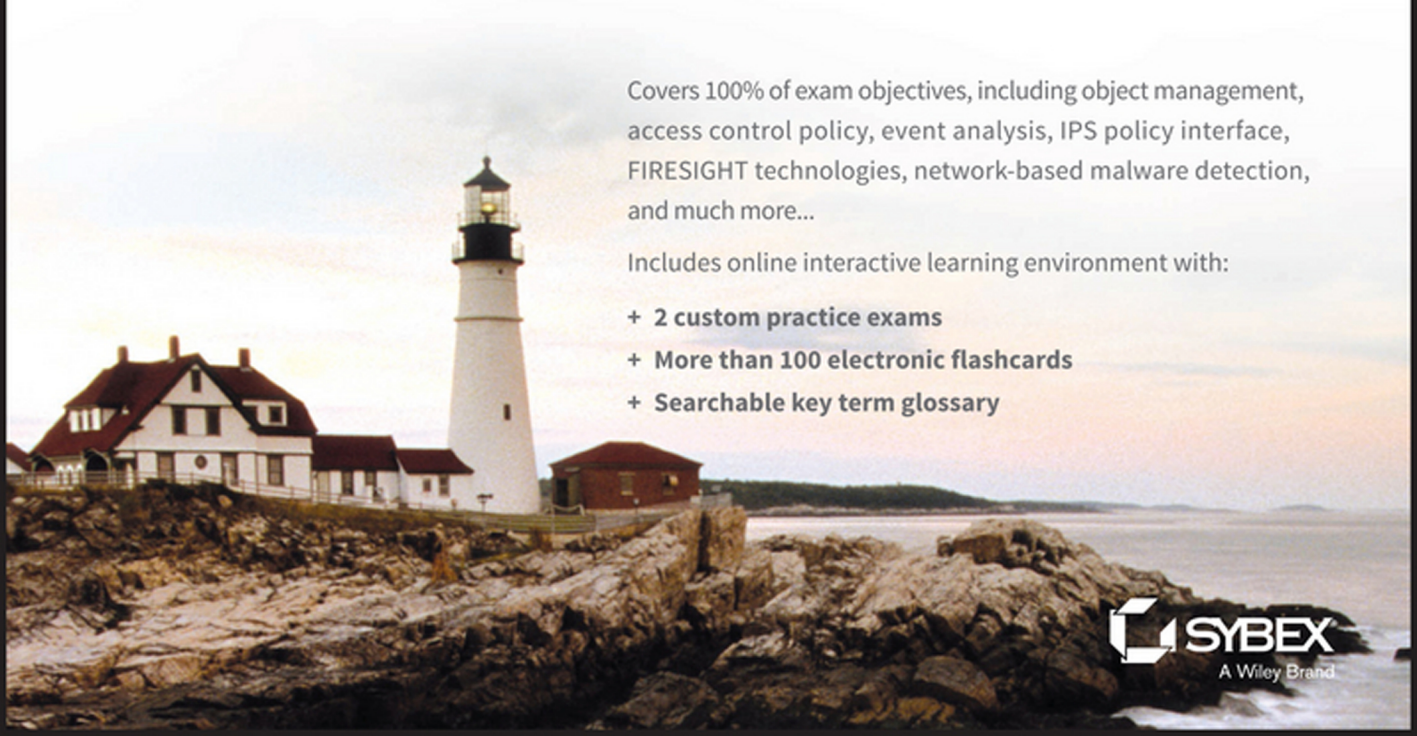
Todd Lammle , John Gay, and Alexis B. Tatistcheff

SSFIPS

Securing Cisco Networks with Sourcefire Intrusion Prevention System

STUDY GUIDE

EXAM 500-285



Covers 100% of exam objectives, including object management, access control policy, event analysis, IPS policy interface, FIRESIGHT technologies, network-based malware detection, and much more...

Includes online interactive learning environment with:

+ **2 custom practice exams**
+ **More than 100 electronic flashcards**
+ **Searchable key term glossary**

SYBEX
A Wiley Brand

SSFIPS

Securing Cisco® Networks with Sourcefire® Intrusion Prevention System

Study Guide

Todd Lammle

John Gay

Alex Tatistcheff

SYBEX®
A Wiley Brand

Senior Acquisitions Editor: Kenyon Brown
Development Editor: Kathi Duggan
Technical Editor: Richard Clendenning
Production Editor: Christine O'Connor
Copy Editor: Judy Flynn
Editorial Manager: Mary Beth Wakefield
Production Manager: Kathleen Wisor
Associate Publisher: Jim Minatel
Book Designers: Judy Fung and Bill Gibson
Proofreader: Josh Chase, Word One New York
Indexer: Robert Swanson
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: © Getty Images Inc./Jeremy Woodhouse

Published by John Wiley & Sons, Inc. Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-15503-4

ISBN: 978-1-119-15505-8 (ebk.)

ISBN: 978-1-119-15504-1 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2015951789

10 9 8 7 6 5 4 3 2 1

To my wife Shelly who has learned to live all these years with a computer nerd.
—Alex

To Jennifer and Paul Gay: Without your support through the late nights, I never would have made it! Thank you for the wonderful years, and I look forward to many more.
—John

Acknowledgments

There are many people who work to put a book together, and although as authors we dedicate an enormous amount of time to write the book, it would never be published without the dedicated, hard work of many other people.

First, Kenyon Brown, my acquisitions editor, is instrumental to my success in the Cisco world. I look forward to our continued progress together in this crazy certification world we call Cisco!

Big thanks to Kathryn Duggan, my developmental editor, who helped keep this project together, and on time. No easy feat! Thank you, Kathryn, once again!

Christine O'Connor, my production editor, and Judy Flynn, my copy editor, are my rock and foundation for formatting and intense editing of every page in this book. This amazing team gives me the confidence to help me keep moving during the difficult and very long days, week after week. I could never imagine writing a single page of a book if I didn't know that the amazing duo of Christine and Judy was behind me all the way! Thank you from the bottom of my heart.

Last listed, but certainly not least, is Richard Clendenning. Phenomenal tech editing at its best and amazing eye on details allowed the authoring team to really shine in this book. Thank you Richard!

—From Todd

Thanks to Todd for driving this entire project. If you ever meet him, you will understand right away how he could write over 60 books. Todd, you're a wild man!

And I would be remiss not to thank my Lord Jesus Christ, to whom I owe literally everything.

—From Alex

Karen Paulson, my former boss who brought me to the Sourcefire team and supported my career development and growth: I cannot thank her enough for her support over the years.

And to Ed Mendez, a co-worker who has fostered my development and been a great learning partner: thanks, man, for all the help!

—From John

About the Authors

Alex Tatistcheff is currently a network consulting engineer for Cisco Security Solutions specializing in FireSIGHT. Alex came to Cisco via the acquisition of Sourcefire, Inc., in 2013. At Sourcefire, he worked for over five years as a senior security instructor teaching the Sourcefire System, Snort, and rule writing classes. During this time, he also completed consulting engagements with several dozen customers.

Prior to coming to Sourcefire, Alex worked on the security team for a large electric utility as a Sourcefire customer and before that as a network/security consultant for numerous organizations.

Alex calls Boise, Idaho, home, where he lives with his wife, Shelly, and two Australian shepherds, Molly and Boomer. He enjoys mountain biking, traveling, and Raspberry Pi.

John Gay is a field security enablement lead with Cisco Systems. He is responsible for facilitating the learning of internal customers. Prior to Cisco's acquisition of Sourcefire, John served as director of instructional delivery, where he managed the instructor team and assisted in the creation and delivery of learning material. Since 1999, John has been in the security industry, training students around the world in IDS/IPS/NGFW/vulnerability assessment. This includes Fortune 500 companies, government agencies, and even military units in theater. Prior to beginning his career in security, John was teaching networking, routing, and back-office applications for a world-class training company. He was also tasked with giving technology presentations for high-profile partners at customer sites and conferences. John has been involved with computers and technology for over 30 years and has had over 20 years in the industry. He also holds a BS in Communication Arts and an MS in Instructional Technology.

Todd Lammle is the authority on Cisco certification and internetworking and is Cisco certified in most Cisco certification categories. He is a world-renowned author, speaker, trainer, and consultant. Todd has three decades of experience working with LANs, WANs, and large enterprise licensed and unlicensed wireless networks, and lately he's been implementing large Cisco data centers worldwide as well as FirePOWER technologies. His years of real-world experience are evident in his writing; he is not just an author but an experienced networking engineer with very practical experience working on the largest networks in the world at such companies as Xerox, Hughes Aircraft, Texaco, AAA, Cisco, and Toshiba, among many others. Todd has published over 60 books, including the very popular *CCNA: Cisco Certified Network Associate Study Guide, CCNA Wireless Study Guide*, and *CCNA Data Center Study Guide* as well as this FirePOWER study guide, all from Sybex. He runs an international consulting and training company based in Colorado, Texas, and San Francisco.

You can reach Todd through his website at `www.lammle.com/firepower`.

Contents at a Glance

Contents

Introduction

Welcome to the exciting world of Cisco certification! If you've picked up this book because you want to improve yourself and your life with a better, more satisfying, and secure job, you've done the right thing. Whether you're striving to enter the thriving, dynamic IT sector or seeking to enhance your skill set and advance your position within it, being Cisco certified can seriously stack the odds in your favor to help you attain your goals!

Cisco certifications are powerful instruments of success that also markedly improve your grasp of all things internetworking. As you progress through this book, you'll gain a complete understanding of security that reaches far beyond Cisco devices. By the end of this book, you'll comprehensively know how Sourcefire technologies work together in your network, which is vital to today's very way of life in the developed world. The knowledge and expertise you'll gain here is essential for and relevant to every networking job and is why Cisco certifications are in such high demand—even at companies with few Cisco devices!

Although it's now common knowledge that Cisco rules routing and switching, the fact that it also rocks the voice, data center, and security worlds is also well recognized. And Cisco certifications reach way beyond the popular but less extensive certifications like those offered by CompTIA and Microsoft to equip you with indispensable insight into today's vastly complex networking realm. Essentially, by deciding to become Cisco certified, you're proudly announcing that you want to become an unrivaled networking expert—a goal that this book will get you well on your way to achieving. Congratulations in advance on the beginning of your brilliant future!

For up-to-the-minute updates covering additions or modifications to the Cisco certification exams, as well as additional study tools, videos, practice questions, and bonus material, be sure to visit the Todd Lammle website and forum at `www.lammle.com/firepower`.

Why Should You Become Certified in the SSFIPS Securing Cisco Networks with Sourcefire Intrusion Prevention System?

Cisco, like Microsoft and other vendors that provide certification, has created the certification process to give administrators a set of skills and to equip prospective employers with a way to measure those skills or match certain criteria.

The SSFIPS Securing Cisco Networks with Sourcefire Intrusion Prevention System (500-285) exam is designed for technical professionals who need to demonstrate their expertise and skills in deployment and management of Cisco NGIPS solutions, including Cisco FirePOWER appliances and the Cisco FireSIGHT management system.

Rest assured that if you make it through the SSFIPS and are still interested in Cisco and security, you're headed down a path to certain success!

What Does This Book Cover?

This book covers everything you need to know to pass the SSFIPS 500-285 exam.

You will learn the following information in this book:

Chapter 1: Getting Started with FireSIGHT What is FirePOWER? What is FireSIGHT? What is Sourcefire? Understand Sourcefire by building a solid foundation in defining key, industry-wide, and Cisco-specific terms that we'll be using throughout this book. Various FireSIGHT appliance models will be discussed as well as licensing, policies, and initial system setup.

Chapter 2: Object Management This chapter will provide you with the understanding of object types that are used by the FireSIGHT System. And as with the other chapters, this chapter includes review questions and a hands-on lab to help you build a strong foundation.

Chapter 3: IPS Policy Management This chapter provides you with the background necessary for success on the exam as well as in the real world with a thorough presentation of IPS policy management. This in-depth chapter covers IPS policies, which precisely describe the suspicious and/or malicious traffic that the system must watch out for, and they also control how evil traffic is dealt with when it's discovered.

Chapter 4: Access Control Policy Chapter 4 covers the heart of the FireSIGHT system. An Access Control policy acts kind of like the central traffic cop for FireSIGHT because all traffic passing through a device is processed through it. And you'll find plenty of help in this chapter as long as you don't skip the review questions and hands-on lab at the end.

Chapter 5: FireSIGHT Technologies FireSIGHT is the name given to a technology built into the Cisco FirePOWER NGIPS to provide us with contextual awareness regarding events, IP addresses, users on the network, and even background about the hosts in the system. As with Chapter 4, plenty of help is there for you if don't skip the review questions and hands-on labs at the end.

Chapter 6: Intrusion Event Analysis In this chapter, we'll review using the FireSIGHT System to analyze intrusion event data. We'll explore some of the workflows available when analyzing events and show you examples of how to drill into relevant event data. We'll also cover how to use the Dashboards and Context Explorer. As always, before tackling the hands-on lab in this chapter, complete the review questions.

Chapter 7: Network-Based Malware Detection A nickname derived from the term *malicious software*, malware comes in a variety of vile flavors, from coded weapons fashioned to damage, control, or disable a computer system to reconnaissance tools for stealing data or identity theft. FireSIGHT's Advanced Malware Protection (AMP) is designed to tackle one of the worst and arguably most prevalent threat vectors today—malware! As always, don't skip the review questions and hands-on lab at the end.

Chapter 8: System Settings This chapter will cover how to apply settings on the systems to control user preferences, time zones, and other key factors plus configuring health checks to alert you to conditions within your devices. Remember the review questions and hands-on labs at the end.

Chapter 9: Account Management In this chapter, we're going to cover a variety of administrative functions for user account management. We'll discuss creating and managing both internal and external users. The hands-on labs and review questions will help you master this chapter.

Chapter 10: Device Management In this chapter we'll discuss and demonstrate registering the device with the Defense Center as well as touring each of the device's properties. You'll discover the different settings for the interfaces and switch and router configurations, plus, we'll survey the different VPN and NAT types available to managed devices as well.

Chapter 11: Correlation Policy Correlation Policy is an often overlooked but useful feature of the FireSIGHT System. The features available in this area concentrate on detection of unusual activity rather than specific intrusion or malware events. By using correlation rules, white lists, and traffic profiles, we can detect network or host behaviors that may be an indication of malicious activity.

Chapter 12: Advanced IPS Policy Settings This chapter is the perfect time to introduce you to some essential advanced IPS policy settings, and we'll also survey important application layer preprocessor settings, network and transport layer preprocessors, and specific threat detection preprocessors. We'll also talk about the significant advantages gained via detection enhancements and performance settings.

Chapter 13: Creating Snort Rules In this chapter, we're going to focus exclusively on the fundamentals of Snort rules, detailing their structure, syntax, and options. We'll also explore how Snort performs rule optimization for better performance and show you how rule matching takes place internally.

Chapter 14: FireSIGHT version 5.4 Facts and Features Last, but definitely not least, this key chapter covers all the great new features in FireSIGHT Version 5.4 that launched in February 2015. Don't be fooled when you hear people refer to this release as a "point" upgrade because that's a serious understatement. Version 5.4 is a major-league upgrade with substantial new capabilities. In addition to all the bright new features, the user interface has been updated, changing the location of some configuration settings. The settings remain largely unchanged from previous versions, but they've been moved in the user interface.

Appendix A: Answers to Chapter Review Questions This appendix contains the answers to the book's review questions.

Be sure to check the announcements section of my forum to find out how to download bonus material I created specifically for this book.

Interactive Online Learning Environment and Test Bank

We've worked hard to provide some really great tools to help you with your certification process. The interactive online learning environment that accompanies the *SSFIPS Securing Cisco Networks with Sourcefire Intrusion Prevention System Study Guide, Exam 500-285*, provides a test bank with study tools to help you prepare for the certification exam—and increase your chances of passing it the first time! The test bank includes the following:

Sample Tests All of the questions in this book are provided, including the assessment test, which you'll find at the end of this introduction, and the chapter tests that include the review questions at the end of each chapter. In addition, there are two *exclusive* practice exams with 50 questions each. Use these questions to test your knowledge of the study guide material. The online test bank runs on multiple devices.

Flashcards The online text banks includes 100 flashcards specifically written to hit you hard, so don't get discouraged if you don't ace your way through them at first! They're there to ensure that you're really ready for the exam. And no worries—armed with the review questions, practice exams, and flashcards, you'll be more than prepared when exam day comes! Questions are provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning and provide last-minute test prep before the exam.

Other Study Tools A glossary of key terms from this book and their definitions are available as a fully searchable PDF.

In addition to the online test bank, the authors have provided additional study material that'll help you get the most out of your exam preparation:

Todd Lammle Bonus Material and Labs Be sure to check the `www.lammle.com/firepower` web page for directions on how to download all the latest bonus material created specifically to help you study for your Securing Cisco Networks with Sourcefire Intrusion Prevention System (SSFIPS) exam.

Online Videos Check out the online videos available at `www.lammle.com/firepower`.

Go to `http://sybextestbanks.wiley.com` to register and gain access to this interactive online learning environment and test bank with study tools.

How to Use This Book

If you want a solid foundation for the serious effort of preparing for the Securing Cisco Networks with Sourcefire Intrusion Prevention System (SSFIPS) exam, then look no further. We've spent hundreds of hours putting together this book with the sole intention of helping you to pass the exam as well as really learn how to correctly configure and manage Firepower!

This book is loaded with valuable information, and you will get the most out of your study time if you understand why the book is organized the way it is.

So to maximize your benefit from this book, I recommend the following study method:

1. Take the assessment test that's provided at the end of this introduction. (The answers are at the end of the test.) It's okay if you don't know any of the answers; that's why you bought this book! Carefully read over the explanations for any question you get wrong and note the chapters in which the material relevant to them is covered. This information should help you plan your study strategy.
2. Study each chapter carefully, making sure you fully understand the information and the test objectives listed at the beginning of each one. Pay extra-close attention to any chapter that includes material covered in questions you missed.
3. Complete all hands-on labs in each chapter, referring to the text of the chapter so that you understand the reason for each step you take. Try to get your hands on some real equipment, or rent ASA/FirePOWER pods at `www.lammle.com/firepower`, which you can use for the hands-on labs found only in this book. These labs will equip you with everything you need for your SSFIPS certification goals.
4. Answer all of the review questions related to each chapter. (The answers appear in Appendix A.) Note the questions that confuse you, and study the topics they cover again until the concepts are crystal clear. And again—do not just skim these questions! Make sure you fully comprehend the reason for each correct answer. Remember that these will not be the exact questions you will find on the exam, but they're written to help you understand the chapter material and ultimately pass the exam!
5. Try your hand at the practice questions that are exclusive to this book. The questions can be found at `www.sybex.com/go/firepower`. And be sure to check out `www.lammle.com/firepower` for the most up-to-date exam prep questions, bonus material, videos, Todd Lammle bootcamps, and more.
6. Test yourself using all the flashcards, which are also found on the download link. These are brand-new and updated flashcards to help you prepare for the SSFIPS exam and a wonderful study tool!

To learn every bit of the material covered in this book, you'll have to apply yourself regularly, and with discipline. Try to set aside the same time period every day to study, and select a comfortable and quiet place to do so. I'm confident that if you work hard, you'll be surprised at how quickly you learn this material!

If you follow these steps and really study—*doing hands-on labs every single day* in addition to using the review questions, the practice exams, and the electronic flashcards—it would actually be hard to fail the Cisco exam. But understand that studying for the Cisco exams is a lot like getting in shape—if you do not go to the gym every day, it's not going to happen!

Where Do You Take the Exams?

You may take the Securing Cisco Networks with Sourcefire Intrusion Prevention System (SSFIPS) exam, or any Cisco exam, at any of the Pearson VUE authorized testing centers. For information, check `www.vue.com` or call 877-404-EXAM (3926).

To register for a Cisco exam, follow these steps:

1. Determine the number of the exam you want to take. (The SSFIPS exam number is 500-285.)
2. Register with the nearest Pearson VUE testing center. At this point, you will be asked to pay in advance for the exam. At the time of this writing, the exam is $250 and must be taken within one year of payment. You can schedule exams up to six weeks in advance or as late as the day you want to take it—but if you fail a Cisco exam, you must wait five days before you will be allowed to retake it. If something comes up and you need to cancel or reschedule your exam appointment, contact Pearson VUE at least 24 hours in advance.
3. When you schedule the exam, you'll get instructions regarding all appointment and cancellation procedures, the ID requirements, and information about the testing-center location.

Tips for Taking Your Cisco Exams

The Cisco exams contain about 50 to 60 questions and must be completed in about 90 minutes or less. This information can change per exam. You must get a score of about 80 percent to pass this exam, but again, each exam can be different.

Many questions on the exam have answer choices that at first glance look identical—especially the syntax questions! So remember to read through the choices carefully because close just doesn't cut it. If you get commands in the wrong order or forget one measly character, you'll get the question wrong. So, to practice, do the hands-on exercises at the end of this book's chapters over and over again until they feel natural to you.

Also, never forget that the right answer is the Cisco answer. In many cases, more than one appropriate answer is presented, but the *correct* answer is the one that Cisco recommends. On the exam, you will always be told to pick one, two, or three options; never "choose all that apply." The Cisco exam may include the following test formats:

- Multiple-choice single answer
- Multiple-choice multiple answer

- Drag-and-drop
- Router simulations

However, be advised that the current SSFIPS exam is listed as all multiple choice questions for now, but understand that this can change at any time.

Here are some general tips for exam success:

- Arrive early at the exam center so you can relax and review your study materials.
- Read the questions *carefully*. Don't jump to conclusions. Make sure you're clear about *exactly* what each question asks. "Read twice, answer once" is what I always tell my students.
- When answering multiple-choice questions that you're not sure about, use the process of elimination to get rid of the obviously incorrect answers first. Doing this greatly improves your odds if you need to make an educated guess.
- You can no longer move forward and backward through the Cisco exams, so double-check your answer before clicking Next since you can't change your mind.

After you complete an exam, you'll get immediate, online notification of your pass or fail status, a printed examination score report that indicates your pass or fail status, and your exam results by section. (The test administrator will give you the printed score report.) Test scores are automatically forwarded to Cisco within five working days after you take the test, so you don't need to send your score to them. If you pass the exam, you'll receive confirmation from Cisco, typically within two to four weeks, sometimes a bit longer.

SSFIPS Exam Objectives

Candidates will demonstrate knowledge of in-depth event analysis, IPS tuning, and configuration in addition to the Snort rules language. Exam takers will show their skills in using and configuring Cisco NGIPS technology, including application control, firewalls, and routing and switching capabilities.

This study guide has been written to cover the SSFIPS exam objectives at a level appropriate to their exam weightings. The following table provides a breakdown of this book's exam coverage, showing you the weight of each section and the chapter where each objective or subobjective is covered:

Objective/Subobjective	Percentage of Exam	Chapters
1.0 Object Management	**6%**	
1.1 Understand the types of objects that may be created and configured in object management		2
1.2 Describe the implementation of security intelligence feeds		2, 4

Objective/Subobjective	Percentage of Exam	Chapters
2.0 Access Control Policy	**10%**	
2.1 Describe the purpose, features, and configuration of access control policy rules		4
2.2 Describe the purpose and configuration of an access control policy		4
3.0 Event Analysis	**5%**	
3.1 Understand the role that geolocation can play in analysis		6
3.2 Be familiar with the interfaces for analysis, including the Dashboard, Work Flows and Context Explorer		6
4.0 IPS Policy Basics	**5%**	
4.1 Understand and describe the operation of the IPS policy interface		3
4.2 Describe the use of the rule management user interface in the IPS policy editor		3
4.3 Be able to implement Cisco FireSIGHT recommendations		3
5.0 FireSIGHT Technologies	**12%**	
5.1 Understand the discovery component inside FireSIGHT, including the policy configuration and the data collected		5
5.2 Understand the type of data collected by connection events with FireSIGHT		5
5.3 Understand the user information that is discovered with FireSIGHT		5
6.0 Network-Based Malware Detection	**10%**	
6.1 Describe the interface components used for analyzing malware events		7
6.2 Understand the different techniques used to identify malware		7
6.3 Describe the features of malware detection as used by the Cisco NGIPS, including communication, actions, and protocols		7

Objective/Subobjective	Percentage of Exam	Chapters
7.0 Basic Administration	**12%**	
7.1 Describe the settings contained in the system polices		8
7.2 Understand the general user preferences and system settings of the Cisco NGIPS		8
7.3 Describe the settings available for the health monitoring features of the Cisco NGIPS		8
8.0 Account Management	**5%**	
8.1 Understand the permissions available to different account roles		9
8.2 Describe the features that can use external authentication		9
9.0 Creating Snort Rules	**5%**	
9.1 Be familiar with the options used to create Snort rules inside the Cisco NGIPS		13
10.0 Device Management	**10%**	
10.1 Describe the VPN types supported and the configuration of those VPNs		10
10.2 Define the different NAT types		10
10.3 Understand the properties of the managed devices and the settings that may be configured		10
10.4 Describe the settings for configuring the virtual interface and virtual router switch types		10
11.0 Correlation Policies	**10%**	
11.1 Describe the components of a correlation policy		11
11.2 Understand the process for creating a white list		11
11.3 Describe the purpose and creation of traffic profiles		11
11.4 Be familiar with the types of responses available when dealing with correlation policies		11

Objective/Subobjective	Percentage of Exam	Chapters
12.0 Advanced IPS Policy Configuration	**10%**	
12.1 Describe the features and settings of application layer preprocessors		12
12.2 Describe the features and settings of network and transport layer preprocessors		12
12.3 Describe the features and settings for specific threat detections in the advanced section of IPS polices		12
12.4 Understand the benefits of the detection enhancements and performance settings in the intrusion policy editor		12

Exam objectives are subject to change at any time without prior notice and at Cisco's sole discretion. Please visit Cisco's certification website (`www.cisco.com/web/learning/exams/list/500-285p.html`) for the latest information on the SSFIPS exam (you'll be prompted to login to your CCO account).

Assessment Test

1. You want to install a Next Generation Firewall (NGFW) and you need to license the product correctly. Which of the following license(s) will you choose?
   - **A.** Protect
   - **B.** Control
   - **C.** Malware
   - **D.** URL Filtering

2. There is a default set configured for the variable set. Which of the following is true regarding this variable set?
   - **A.** This set is provided by Cisco.
   - **B.** Variables in this set determine the default value for any additional variable sets.
   - **C.** Once a variable value is edited, future Cisco updates to that variable will not be applied.
   - **D.** All of the above.

3. You need to export a policy and provide it to your security admin. They ask you what format you'll be sending the policy in. Which of the following is your answer?
   - **A.** Ccsv
   - **B.** Binary
   - **C.** Text
   - **D.** `.xls`

4. You want to block the URLs for Facebook in your company; however, you want to make sure that the users understand why they were blocked so they don't bother you. How should you configure the AC rule?
   - **A.** Create a Block rule, specify the website, and enable logging.
   - **B.** Create an Allow rule and specify an IPS policy that contains a Snort rule blocking the website.
   - **C.** Create an Interactive Block rule for the site, and specify an HTTP response on the HTTP Responses tab.
   - **D.** Create a Block rule for the site, and specify an HTTP response on the HTTP Responses tab.

5. You want to view summary information of your network traffic. How would you do this?
   - **A.** Analysis ➢ Connections ➢ Events
   - **B.** Overview ➢ Dashboard ➢ Connection Summary
   - **C.** Analysis ➢ Connections ➢ Hosts ➢ Network Map
   - **D.** Overview ➢ Dashboard ➢ URL Statistics

6. You have configured the Dashboard as your default page and have also configured widgets to help you analyze your network. Which of the following are characteristics of the Dashboard? (Choose three.)
   - **A.** Customizable widgets
   - **B.** Flexible searching and dynamic pivoting of data
   - **C.** Multiple searches and various event views all on one page
   - **D.** The ability for users to add personal dashboards

7. You need to define Spero analysis to your manager. Which of the following will you use to help you define Spero?
   - **A.** It's used to analyze a SHA-256 to determine if a file is malicious.
   - **B.** It's a form of analysis that involves executing the file in a sandbox environment.
   - **C.** It's a manual analysis that cannot be performed automatically.
   - **D.** It's a method of analyzing static file attributes such as headers and metadata.

8. How often do health checks on a managed device run?
   - **A.** Every 10 minutes
   - **B.** Every 5 minutes
   - **C.** Every 30 minutes
   - **D.** Every 60 minutes

9. You want to be able to have a user escalate their user permissions if you provide them with a password. How would you accomplish this?
   - **A.** From the System ➢ Local ➢ System Policy and choose User Interface.
   - **B.** By changing the value of the Pluggable Authentication Module (PAM) login attribute for the user.
   - **C.** From the User Management screen, click the User Roles tab and then click Configure Permission Escalation.
   - **D.** From the User Management screen, click the Login Authentication tab and then click Configure Permission Escalation.

10. If an application is taking more than an allotted amount of time to pass traffic through the inline device, what feature allows traffic to pass without inspection?
    - **A.** Automatic Application Bypass
    - **B.** Profiling
    - **C.** Fail-Open
    - **D.** Automatic Application Redirect

11. You've decided to create a new traffic profile and your boss asks what the default PTW and sample rate is going to be. What do you tell him?
    - **A.** 1 week, 1 hour
    - **B.** 1 week, 5 minutes

C. 24 hours, 5 minutes

D. 24 hours, 30 minutes

12. Inline Normalization performs what function, which helps prevent network threats?

A. Inline Normalization–enabled IPS blocking.

B. Inline Normalization sends traffic to the IP and TCP preprocessors.

C. Inline Normalization cannot stop threats.

D. Inline Normalization removes deviations in IP, TCP, and ICMP protocol standards.

13. Which keyword is used to reduce the number of logged alerts for noisy rules?

A. `byte_count`

B. `detection_filter`

C. `metadata`

D. `file_data`

14. What are the three SSL object types added in the 5.4 code?

A. Cipher Suite List

B. TTLS

C. Distinguished Name

D. PKI

E. WPA2

Answers to Assessment Test

1. B. The Control license enables application control functionality, allowing the device to become an NGFW. See Chapter 1, "Getting Started with FireSIGHT," for more information.

2. D. All of the options are true regarding the default set. See Chapter 2, "Object Management," for more information.

3. B. Policies are exported in a binary format. This can be imported into another FSM assuming it is on the same software version. See Chapter 3, "IPS Policy Management," for more information.

4. D. While this could be done with an Interactive Block rule (C), this would also allow the user to override the block if desired. See Chapter 4, "Access Control Policy," for more information.

5. B. To view the summary of your traffic, you can go to Overview ➢ Dashboards ➢ Connection Summary. Alternately, you can go to Overview ➢ Summary ➢ Connection Summary. See Chapter 5, "FireSIGHT Technologies," for more information.

6. A, C, D. Flexible searches with multiple search criteria is a feature of the Context Explorer, not the Dashboard. See Chapter 6, "Intrusion Event Analysis," for more information.

7. D. Spero analysis involves evaluating hundreds of file attributes including headers, DLLs called, and other metadata. See Chapter 7, "Network-Based Malware Detection," for more information.

8. B. Health policies are set to run every 5 minutes by default. This can be changed in the health policy. See Chapter 8, "System Settings," for more information.

9. C. To set up a user so the user can escalate its permissions, from the User Management screen, click the User Roles tab and then click Configure Permission Escalation. Then choose the user role that the user will have its permissions escalated to. See Chapter 9, "Account Management," for more information.

10. A. Automatic Application Bypass (AAB) terminates the IPS inspection process if traffic takes an excessive amount of time to make it through the device (bypass threshold). It will generate a troubleshooting file and a health alert and restart inspection within 10 minutes. See Chapter 10, "Device Management," for more information.

11. B. The default PTW is 1 week, and the sample rate is one sample every 5 minutes. See Chapter 11, "Correlation Policy," for more information.

12. D. The purpose of Inline Normalization is to remove deviations in IP, TCP, and ICMP protocol standards. When this feature is enabled, you can pick and choose what types of normalizations will be used for the specific protocols. See Chapter 12, "Advanced IPS Policy Settings," for more information.