Practice Tests

Flash Cards

Glossary

Study Planner

Official Cert Guide

Advance your IT career with hands-on learning

CCNP Security

Cisco Secure Firewall and Intrusion Prevention System

ciscopress.com

Nazmul Rajib

Special Offers

Save 70% on Complete Video Course

To enhance your preparation, Cisco Press also sells Complete Video Courses for both streaming and download. Complete Video Courses provide you with hours of expert-level instruction mapped directly to exam objectives.

Save 80% on Premium Edition eBook and Practice Test

The *CCNP Security Cisco Secure Firewall and Intrusion Prevention System Official Cert Guide Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.

```
Result:
input-interface: OUTSIDE_INTERFACE(vrfid:0)
input-status: up
input-line-status: up
Action: allow
```

In addition to the detail trace data (displayed in Example 8-1), you can also save the original packets in the PCAP file format for future reference. Later, for further analysis, you can open the PCAP file in a packet analyzer tool like Wireshark (see Figure 8-11). Additionally, you can replay the captured packets in a PCAP file to emulate the connections in a lab environment. PCAP files are critical to an incident response team for forensic analysis.

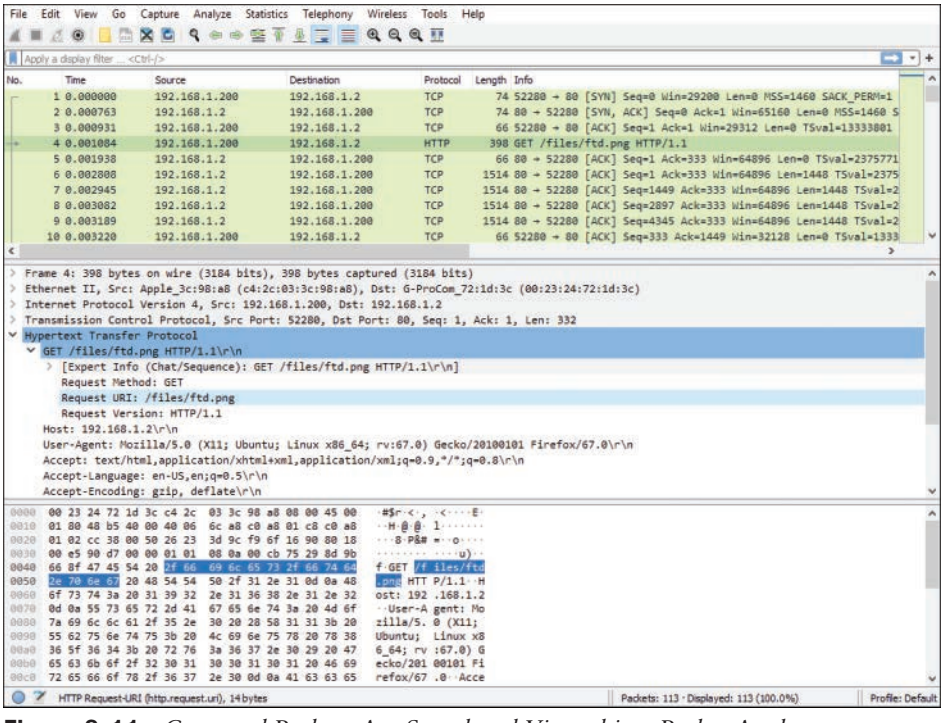

Figure 8-11 *Captured Packets Are Saved and Viewed in a Packet Analyzer*

Packet Capture versus Packet Tracer

The previous sections demonstrate the use of the packet capture tool. The example shows how to capture live traffic and how the trace option provides additional packet flow data. Because capturing live packets can be a CPU-intensive process, running the tool in a production environment requires careful planning. For a quick packet flow analysis, the packet tracer tool can be an easy alternative.

Key Topic

The packet tracer tool enables you to simulate the flow of a packet based on the security policies you deployed on a threat defense. The process is simple: you select an interface and packet type and provide the host detail, as shown in Figure 8-12. The tool uses that information to create a virtual packet. After you start the simulation, the virtual packet is evaluated

8

against the security policies deployed on a threat defense. The verdict on a virtual packet can enable you to predict the potential impact of the security policies on live traffic. You can leverage this tool to investigate any connectivity issues in your real-world network.

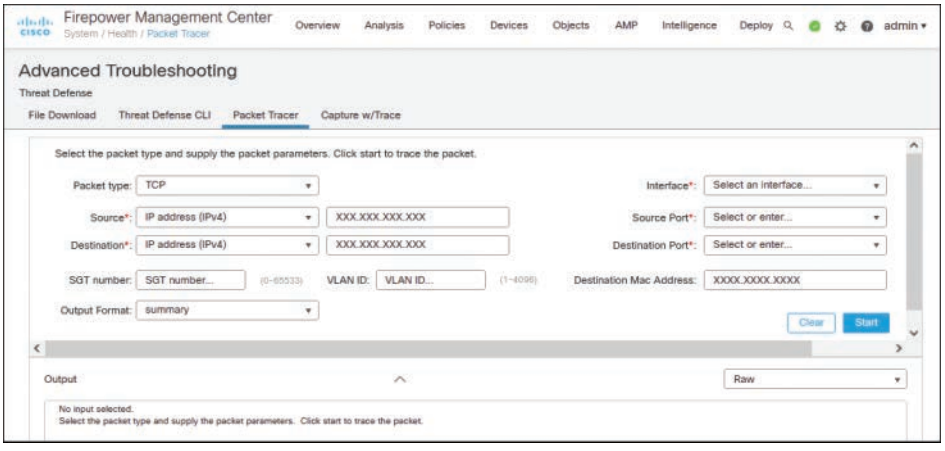

Figure 8-12 *User Interface for the Packet Tracer Tool*

Summary

This chapter demonstrates the generation of live traffic between a web server and a client, provides detailed steps for capturing traffic between them using the management center, and then describes how to use a packet analyzer tool for further analysis. The chapter also illustrates the possible reasons for a packet drop and delineates the packet flow through different components of a threat defense. It empowers you to prepare for the next chapters because they will describe various security policies.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 22, "Final Preparation," and the exam simulation questions in the Pearson Test Prep practice test software.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 8-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 8-2 Key Topics for Chapter 8

Key Topic Element	Description	Page
Paragraph	Benefit of the packet capture tool	158
List	Optimal performance during packet capture	160
Paragraph	Packet tracer	169

Memory Tables and Lists

There are no Memory Tables or Lists for this chapter.

Define Key Terms

Define the following key terms from this chapter, and check your answers in the Glossary:

PCAP file, packet analyzer

CHAPTER 9

Network Discovery Policy

This chapter provides an overview of the following topics:

Network Discovery Essentials: This section describes different types of application detectors and explains the operation of network discovery components on a threat defense.

Best Practices for Network Discovery: In this section, you learn important best practices to improve the effectiveness of network discovery.

Fulfilling Prerequisites: This section discusses the settings that you should not overlook before configuring a network discovery policy.

Configurations: This section describes the reusable objects on Secure Firewall and then uses objects to configure discovery rule conditions.

Verification: In this section, you find different ways to view network discovery data on a management center GUI.

The objectives of this chapter are to learn about

- Network discovery policy operation and configuration
- Application detectors
- Reusable object management
- Dashboard and event viewer
- Discovery data analysis

Secure Firewall can automatically discover the applications and services running in a network. It can dynamically identify the hosts and users who are running an application. It also can discover applications with or without the help of any active scanner. Secure Firewall allows you to monitor or block traffic solely based on the type of application a user might be running. This chapter describes how to enable application visibility and control (AVC) on Secure Firewall using the network discovery policy.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 9-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 9-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Network Discovery Essentials	1–2
Best Practices for Network Discovery	3–5
Fulfilling Prerequisites	6
Configurations	7
Verification	8

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following statements about application detectors is true?
   - **a.** Internal detectors are always on; they are built in the software.
   - **b.** The management center leverages OpenAppID to create custom detectors.
   - **c.** Secure Firewall software comes with a set of application detectors, by default.
   - **d.** All of these answers are correct.
2. Which of the following databases contain the fingerprint information?
   - **a.** Snort rule database
   - **b.** URL filtering database
   - **c.** Vulnerability Database
   - **d.** Discovery event database
3. What does a network discovery policy allow Secure Firewall to discover?
   - **a.** Hosts
   - **b.** Users
   - **c.** Applications
   - **d.** All of these answers are correct.
4. For accurate discovery of the latest applications, which of the following should you consider?
   - **a.** Ensure that the network discovery policy is set to monitor the load-balancer devices.
   - **b.** Use the network addresses instead of network objects.
   - **c.** Generate Rule Recommendations in an intrusion policy.
   - **d.** Keep the Vulnerability Database (VDB) version up to date.

5. Which of the following is considered a best practice when deploying network discovery policy?
   a. Deploy the threat defense as close as possible to the gateway.
   b. Add the addresses 0.0.0.0/0 and ::/0 in the rule for an accurate host profile.
   c. Exclude the IP addresses of any NAT and load-balancing devices from the list of monitored networks.
   d. For precise detection of the latest application, create a rule to discover private IP addresses.
6. Which of the following statements is not true?
   a. To discover applications, hosts, or users from certain subnets, you can trust the traffic from that subnet to expedite the discovery process.
   b. Secure Firewall uses the Adaptive Profiles option to perform application control.
   c. The Adaptive Profiles option should be always enabled to ensure superior detection.
   d. Trusted connections are not subject to deep inspection or discovery.
7. Which of the following statements is false?
   a. If you forgot to create an object using the Object Management page, you can still create one on the fly directly from the Add Rule window.
   b. Creating objects for the network resources and reusing them in the discovery rules are optional; however, it helps with rule management in the long term.
   c. You can create objects only for three elements: network addresses, port numbers, and interfaces.
   d. You can group multiple objects into a single configuration.
8. What is the reason that some operating systems appear as pending?
   a. The network discovery policy deployment is not complete.
   b. The threat defense is currently waiting on further packets to conclude analysis.
   c. The management center has reached its license limit.
   d. The operating system is currently being updated by the host.

Foundation Topics

Network Discovery Essentials

When you access a website, you interact with at least three types of applications: a browser on a client computer that originates the web communication, an underlying protocol that establishes the communication channel to the web, and the web contents from a server with which you are communicating. When a threat defense is deployed between the client and server, it can discover all three of these applications in a network. Moreover, it can categorize applications based on risk level, business relevance, content category, and so on.