Study guide by ExamNotes.net

Checkpoint

CCSA 2000 Rev A

Study Guide, written by Yu Chak Tin Michael

Abstract

This ExamNotes Study Guide intends to provide you with information to prepare for the Checkpoint CCSA Exam.

Before you start

This study guide provides you with information on the many different aspects of "Checkpoint CCSA". Before you proceed with this subject, please make sure you are 100% comfortable with the concept of a firewall.

Do NOT rely solely on this study notes for the exam. By all means read more than one book on the subject and make sure you understand the material well enough so that you could be ready for the questions. There is no quick way to succeed for this topic. Ideally you must work things out and gain experience before even trying to sign up for the exam.

Your Study Track for CCSA 2000

1, Know the ins and outs of TCP/IP. Know the protocol architecture. Know TCP, UDP, FTP, HTTP and other related terms.

2, Make sure you are comfortable with the concept of Firewall and network security. You will find the following books useful:

Building Internet Firewalls

Authors: D. Brent Chapman and Elizabeth Zwicky
Publisher: O'Reilly
Edition: 1995
ISBN: 1-56592-124-0

Practical Internet & Unix Security

Authors: Simson Garfinkel and Gene Spafford
Publisher: O'Reilly
Edition: 1996 ISBN: 1-56592-148-8
(discusses primarily host security)

Firewalls and Internet Security: Repelling the Wily Hacker

Authors: Bill Cheswick and Steve Bellovin
Publisher: Addison Wesley
Edition: 1994
ISBN: 0-201-63357-4

For related tutorials on the internet, please visit the following sites:

http://www.tribecaexpress.com/firewallfaq.htm

3, Make sure you know Checkpoint's product offering. Visit www.checkpoint.com and understand the modules offered.

4, Read the WWW Security FAQ to get yourself familiar with the current security issues.

http://www.w3.org/Security/Faq/www-security-faq.html

LEARN CCSA BY SCENARIOS

You are the network administrator of your company. You are asked to plan for and implement a network security solution. You will face a series of questions. You will need to make decisions to maximize the security of your company's network in the most cost effective way.

Your network is connecting to the internet. You want to be sure that the internal networks are protected from outside intrusion. What tool will you use?

Basically you will deploy a firewall. A firewall can be used for enforcing pre-defined security policy on the network communication points. However, keep in mind that it cannot protect against malicious authorized users.

According to pcwebopedia.com, firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Pcwebopedia.com further classify the types of firewall techniques as:

Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

Compare to a firewall, packet filter is a lower cost alternative. It is fast, simple and cheap. However, It is not scalable, not secure, and cannot filter out traffics that are spoofed. Application Layer Gateway is very secure, but is expensive and is CPU power consuming.

Your boss suggests that you consider the firewall software offered by Checkpoint. What is the advantage of Checkpoint's solution?

Stateful Inspection basically uses context information to determine if a request should be allowed. It learns from previous communication sessions and uses dynamic state table to store state information. The operation is completely transparent. And of course, it has ALL the advantages nothing else can offer. Note that the FW-1 module is located between the Network and the Datalink Layers for maximum efficiency.

FW-1 uses a client server architecture for manageability and scalability. Centralized Logging is an advantage if your network is complex. The Customer Log Module is a Management Server with ONLY the logging and alerting functionality. It collects logs and alerts from all the VPN/FireWall Modules but does not maintain the Security Policy.

For security, traffic between the GUI and the Management Server is protected via authentication and encryption (if you are using the Encryption Module).

Your boss suggests that you consider the firewall software offered by Checkpoint. What are the roles in the Checkpoint's solution?

FW-1 uses a client server architecture for manageability and scalability. The FireWalled gateways are controlled and managed by the Management Server. The Management Server in turns is managed by the GUI client. Security policy can be designed via the GUI running on either Windows 9x, Windows NT or X/Motif.

To summarize, we use the Management Module to define the Security Policy. We also use the FireWalled gateway to enforce the Security Policy. The management server is responsible for maintaining all the firewall data.

There are three different GUIs in FW-1. They are: Security Policy Editor, Log Viewer and System Status Viewer. The exam focuses on the use of these GUIs, not the command line tools.

You want to be sure that your internal IPX networks are protected from outside intrusion. How do you do this with FW-1?

In fact you cannot. FW-1 can only handle IP traffics. IP is responsible for moving packet of data from node to node based on a four byte destination address known as the IP number. The Internet authorities assign ranges of numbers to different organizations. The organizations assign groups of their numbers to departments.

TCP is responsible for verifying the correct delivery of data from client to server. TCP can detect errors or lost data and trigger retransmission until the data is correctly and completely received. On the other hand, UDP does not guarantee delivery. Socket is a name given to the package of subroutines that provide access to TCP/IP on most systems. In FW-1, we are more concern about ports than sockets.

Note that there must be a way to open a connection to a specified computer, log into it, tell it what file is needed, and control the transmission of the file. This is done by the "application protocols" that run on top of TCP/IP. FW-1 is capable of processing requests by investigating the application protocols. Examples include HTTP, FTP, SMTP …etc.

Note that in any case, the protection device cannot control any connection that don't go through the firewall.

You are about to deploy Checkpoint's solution. What server must you get ready for running FW-1?

FW-1 can be run under Windows NT 4.0 with SP4 or above, Windows 2000, Solaris 2.6 or above, HP-UX 10.20 or above, IBM AIX 4.2.1 or above, as well as Red Hat Linux 6.1 with kernel version 2.2.x or above.

Note that the server with FW-1 running should have at least 2 NICs. For security reason, the machine's IP forwarding function should be controlled by FW-1 to ensure that the gateway is forwarding packets only when FW-1 is running.

The suggested order for installing FW-1 on the NT Server:

- Install NT
- Remove any protocols or services that are not needed
- Enable IP forwarding
- Install Service pack
- Install the NT hotfixes if necessary
- Install FW-1
- Install the latest FW-1 patch if available

Note that if you add/remove services from the NT CD and then install any service pack, you may need to re-install all of the hotfixes, the FW-1 server software and then the latest FW-1 patch.

Your boss has a legacy version of FW-1 installed on an old PC. Is an upgrade possible?

Version upgrade can be done only from FW-1 Version 3.0 and higher. If you really want to upgrade a version prior to 3.0, you will have to first upgrade from that version to Version 3.0, then upgrade from Version 3.0 to Check Point 2000. This can be troublesome. The upgrade version will not overwrite the previous versions. That means, if you uninstall the new version, the previous version will be restored. However, you should pay attention to the hardware. Your old PC may not have the processing power to fully utilize FW-1.

You are about to deploy Checkpoint's solution. What is the FW-1 licensing requirement for your network?

Keep in mind that the license restrictions are based on the number of protected hosts. For example, FireWall-1/25 is restricted to protecting 25 nodes. Also, should encryption be required (in case you need to build VPN), the corresponding VPN-1 products are required. However, license for running the GUI Client is not required. Additionally, you may want to use FW-1 to control your Cisco router. In this case, you will need the Open Security Extension/1.

You need to configure an administrator (yourself) for FW-1. Which of the following should you consider?

FW-1 administrator password should have 8 characters or less. For security purpose, you want it to contain both alphabetic and numeric characters. There can be multiple administrators, each with different access privilege levels. You use the GUI (NT) or the cpconfig application (Unix) to change the administrator's privileges. In the Add Administrator dialog box, you can fine tune the privileges of a new administrator.

Remember, there is no relationship between this administrator account and the OS administrator account. In fact, for security reasons, they should be different. To set up FW-1 properly, you MUST define at least one administrator.

As an administrator, when you want to log in from the GUI client, have the following information handy: username, password and the management server name.

You want to configure firewall rules. What is the first step to take?

Before configuring the rules, you should set up the various network objects first. To do so, use the Network Object Manager. This tool can be invoked from within the Security Policy editor GUI. The objects will later on be included in the rules. You do not need to define all the objects in your network. Instead, define only those that will be used in the Rule Base. Possible objects you can define include Workstations, Gateways, Routers, Networks, Switches, Logical Servers, Gateway clusters and Domains.

You get confused by the "directions" of packet flow. Your security rule should be deployed based on what direction?

When you enforce a rule inbound, you enforce the Security Policy only on packets that enter the object. On the other hand, an outbound rule will enforce the Security Policy only on packets that leaves the object. Eitherbound is the default setting, meaning packets are examined twice during the in and out. This is secure but costly, and should be avoided.

Another concept that is related – spoofing. Think about this: Should you allow a packet with an internal address to come in from the outside world? Of course not!

This can fool a packet filter, but not the FW-1. Anti spoofing means that packets with internal IP addresses arriving on the external interface should be blocked. A rule for handling this situation should be defined before any other rules on the external interface. In fact, you should understand the concept of valid addresses - packet with source IP address that belongs to Valid Addresses is allowed to enter the network object, and vice versa.

You get confused by the "position" of the network objects. What is the difference between an External and an Internal object?

On a workstation with VPN/FireWall Module installed, its object is internal to its own Management Station, and is external to other Management Stations. Security Policy can only be installed on an internal host. External host is not under your control.

You have defined the network objects. What is the next step to take?

Now you are ready to define a rule in the Rule base. Before doing so, note that there are two types of special rules that worth your attentions. The Implicit Drop Rule is the last rule in the rule base that drops all the communication attempts not described by the rules you defined. This rule drops packets without taking logs. On the other hand, Stealth rule is the first rule in the rule base that prevents traffic from directly accessing the firewall itself.

To define your own rules, you must specify the Source, Destination, Service, Action and Install On (which is the enforcement point) elements.

Keep in mind that FW-1 implements the rules Top Down. Watch out for conflicting rules. The rules at the top take precedence. The real EFFECTIVE security settings is determined by the combination of settings in the Security Policy Properties and the Rule Base. The order of packet matching is: Anti Spoofing - Properties marked FIRST in the Security Policy Properties - Rule base order except for the last rule - Properties marked BEFORE LAST in the Security Policy Properties - Rule Bases last rule - Properties marked LAST in the Security Policy Properties - Implicit Drop Rule.

Note that you are encouraged to verify your rule base settings before installing it onto the firewall module. The verify button on the toolbar can be used for this purpose.

Apart from filtering packets, you also want to authenticate users. How do you do this?

According to pcwebopedia.com, authentication is the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

In FW-1, in order to set up authentication, you need to first define the user, then assign the user to a group, specify the authentication scheme to be used, and finally configure the corresponding authentication rule in the rule base.

Firewall-1 Password is a Fixed scheme. It is not necessary to have an user account in FWl-1 to use this password. This scheme is safe as password is encrypted. However, this is Checkpoint proprietary.

OS Password makes use of the Operating System password, and is considered to be less secure. S/Key uses One time password generated based on seed value, secret key and length. This is VERY secure and VERY complex. SecurID makes use of hardware secured card to generate unique and unpredictable access code every 30 to 90 seconds. AXENT Pathway Defender is a token based scheme that requires separate server software and user token cards. RADIUS requires the use of RADIUS server for centralized authentication and accounting.

If you want to enable internal access to the Internet using user authentication, you will want to:

- Enable the HTTP Security server.
- In the browser, specify the Firewall as the proxy.
- Specify the valid Source / Destinations for the user definition.
- Modify the Properties of User Auth Action and the Allowed Servers from Predefined to Any.

For maximum security, you decided to hide the internal IP structure. How can this be done in FW-1?

You should consider to use NAT. Do not confuse NAT with PAT. They are similar in nature, but NAT is the correct term to use in FW-1. PAT is widely used in MS Proxy Server.

According to pcwebopedia.com, NAT - short for Network Address Translation, it is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations. NAT serves two main purposes: Provides a type of firewall by hiding internal IP addresses; Enables a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations; Allows a company to combine multiple ISDN connections into a single Internet connection.

In FW-1, you can use the Source Static Mode for one to one mapping that translates illegal IP to legal IP. You use this only for outgoing traffic. To make this work, you will also need to publish the legal addresses manually with an ARP entry so that replies can be routed back correctly. That means, once you've setup the internal systems to use static NAT, that you have created the network object and installed it in the rule base, you still have to create a route entry from the command prompt by using the route add -p legal_IP_address mask 255.255.255.255 private_IP_address command. The –p parameter will make the entry permanent.

If you need one to one mapping that translates legal IP to illegal IP for incoming traffic, use Destination Static Mode. To allow multiple hosts to share on legal IP for internet access, use Hide Mode. In hide mode, port numbers are used to distinguish between traffic for the different internal hosts. Again, the legal addresses must be published manually with an ARP entry so that routing of replies is possible.

How do you monitor the status of the FW-1 modules?

To do so you need to use the System Status GUI tool. This tool can be used to show the number of packets dropped, rejected, inspected and logged. It also shows the security policy and the status of the Firewall-1 Daemon.

FW-1 does not use NT Event Viewer to maintain its log. Instead, it provides the Log viewer tool for you to review logs. In FW-1, a log file will have the current date appended to its file name when it is saved. When you start a new log file, the current

log file will be saved automatically. To view the pop up alerts, you do not have to open the log viewer tool.

In Log viewer, if you want to show only the current connections, you may use the Active Connection Mode. If you want to create charge back or progressive billing reports, use the Accounting Mode instead.

The System Status tool indicates that one of your firewall module is DISCONNECTED. What does this mean?

If the daemon is INSTALLED, that means the daemon is running with the security policy installed. If the daemon is NOT INSTALLED, that means the daemon running without any security policy installed. If the status is DISCONNECTED, that means there is no response from the daemon --- may be the daemon has crashed.