Internetwork Expert's CCIE™ Security Workbook (IEWB-SC) Volume 1

Internetwork Expert, Inc.
www.InternetworkExpert.com
Toll Free: 877-224-8987

Copyright Information

Disclaimer

The following publication, ***CCIE™ Security Lab Workbook***, is designed to assist candidates in the preparation for Cisco® Systems' CCIE™ Security Lab Exam. While every effort has been made to ensure that all material is as complete and accurate as possible, the enclosed material is presented on an "as is" basis. Neither the authors nor Internetwork Expert, Inc. assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in this workbook.

This workbook was developed by Internetwork Expert, Inc. and is an original work of the aforementioned authors. Any similarities between material presented in this workbook and actual CCIE™ lab material is completely coincidental.

Table of Contents

About IEWB-SC

The CCIE™ Security is one of the most in-demand technical certifications in the world. Over the past several years, governmental requirements regarding mandatory intrusion detection systems, along with the ongoing task of ensuring that corporate networks are safe from ever-evolving security risks has placed advanced security technologies and, in particular, the CCIE Security track in the spotlight.

Internetwork Expert's CCIE™ Security Lab Workbook (IEWB-SC) is the follow-up to our highly acclaimed CCIE™ Routing and Switching Lab Workbook (IEWB-RS), which has assisted networking professionals throughout the world achieve their CCIE™ R&S certification. Like the R&S Workbook, IEWB-SC is designed to be used as a supplement to self study and instructor-led training in preparation for Cisco® Systems' CCIE™ Security Lab Exam.

IEWB-SC consists of ten lab scenarios designed from the ground up, based on Cisco Systems'® recently revised specifications for the CCIE™ Security Lab Exam. These labs are designed to both simulate the actual CCIE™ Security Lab Exam and teach the principles behind the technologies which they cover.

Each of these ten lab scenarios is divided into the following nine technology sections:

1. Catalyst 3550
2. ISDN/PPP
3. Routing Protocols
4. VPN
5. IP Services
6. General Security
7. Advanced PIX Firewall
8. AAA
9. IDS

Each of the above sections is then further subdivided into particular tasks. For each lab scenario, you must configure the presented tasks while conforming to various predefined restrictions.

Restrictions

Each lab scenario contains explicit general restrictions that you must conform to while configuring the lab. These restrictions are defined in the *Lab Do's and Don'ts* introductory section for each scenario. Examples of these restrictions include, but are not limited to, not using static routes, not using default routes, not adding additional IP addressing, etc.

> **Caution**
>
> Ensure that you always read the *Lab Do's and Don'ts* section carefully, as the restrictions may vary from lab to lab.

There may also be certain restrictions for particular tasks within a lab scenario. Examples of these restrictions include, but are not limited to, not issuing a particular configuration command, not creating a certain type of interface, not using the legacy configuration for a technology, etc.

> **Note**
>
> You may do whatever is necessary to complete a task unless the general requirements for the lab scenario or the specific requirements for the task explicitly prohibit you from doing so. This may include using policy routing, redistributing IGPs or BGP, configuring GRE tunnels, etc.

If NTP clock synchronization is needed to complete a particular task, use any of the BB routers as NTP servers. The Windows® 2000 Server can be configured to synchronize its clock to any router by using the **net time /setsntp:X.X.X.X** at the command prompt. When synchronizing any device with one of the BB routers, first ensure that the device has reachability to the BB router and that NTP traffic is not being filtered between the device and the BB router.

Difficulty Rating

Each lab scenarios has been assigned a difficulty rating. Ratings are on a scale of one (1) to ten (10), with ten being the most difficult.

> **Note**
>
> The IEWB-SC lab scenarios are designed to be more technically challenging than the actual CCIE™ Security Lab Exam. Do not be discouraged if you score low or do not understand a particular set of technologies. If you are having trouble with a certain area, do not hesitate to read the explanation contained within the solutions guide. Remember, these labs are designed to teach you *new* technologies and skills as much as they are designed to test your current capabilities.

Point Values

As in the actual CCIE™ Lab Exam, each task within a lab is assigned a specific point value. Points are only awarded if the presented solution meets all the given requirements, and does not violate any preset restrictions. *No partial credit is awarded for any task*. A minimum score of 80 points is required to 'pass' a particular scenario.

Some tasks have multiple solutions. As long as the presented solution meets the given requirements, points will be awarded for that task. However, certain solutions may negatively impact previous or future tasks. Make sure you carefully read all presented requirements, and try your best to come up with an appropriate solution.

> **Caution**
>
> Points will never be awarded for a task in which you have violated the requirements. However, keep in mind the relative point value of the task in question as compared to future tasks. If you cannot come up with an appropriate solution for a particular task, it is advisable to solve the task by whatever means necessary in order to complete the future tasks which depend on it.

Initial Configurations

Internetwork Expert's CCIE™ Security Lab Workbook includes initial configuration scripts for all devices in each lab scenario. These configuration scripts include basic Layer 2 and Layer 3 routing connectivity, and must be loaded on your equipment before beginning the configuration of the scenario.

For the most recent copy of these initial configuration scripts, see Internetwork Expert on the web at http://www.internetworkexpert.com

In addition to these initial configuration scripts, it is necessary to load the provided configuration files for the backbone devices. However, if you are configuring this scenario on Internetwork Expert's racks, the backbone devices will be preconfigured.

For more detail on the hardware requirements for the internal and external devices in IEWB-SC, see the accompanying *Hardware Specification* section of this document.

Although the newest CCIE™ Security Lab specification states that candidates are not required to configure basic Layer 2 and Layer 3 connectivity, you should have working knowledge of these topics before attempting the CCIE™ Security Lab exam. For individuals without a foundation of the Routing & Switching topics, we recommend using Internetwork Expert's CCIE™ Routing & Switching Lab Workbook (IEWB-RS).

For more information on Internetwork Expert's CCIE™ Routing & Switching Lab Workbook, visit Internetwork Expert on the web at http://www.internetworkexpert.com

Solutions Guide

In addition to this workbook, a detailed solutions guide for Internetwork Expert's CCIE™ Security Lab Workbook is available. The solutions guide includes the final configurations for each lab scenario, accompanied by a thorough explanation of each task. The final configurations for IEWB-SC are broken down on a task-by-task basis. Therefore, you will know exactly which commands correspond to which particular task. There is no need to sort through a long configuration file to guess which commands correspond to which question. The solutions guide for IEWB-SC is as much of an integral part of this product as the workbook itself.

For more information on the IEWB-SC solutions guide visit Internetwork Expert on the web at http://www.internetworkexpert.com.

Rack Rentals

Internetwork Expert has designed the CCIE™ Security Lab Workbook to the publicly stated hardware specification used in the actual CCIE™ Lab Exam. Internetwork Expert offers cost-effective equipment rentals specifically designed to be used with our self-paced training product lines, in order to eliminate the cost of buying all the equipment used in IEWB-SC.

These rack rentals not only minimize your investment in training, but also enable you to utilize Internetwork Expert's value-added services, such as grading.

Grading

Throughout their many years of teaching CCIE™ preparation programs, our trainers have found that many CCIE™ candidates fail the lab without understanding why. Although Cisco® provides a score report for unsuccessful lab exam attempts, this report fails to provide an accurate picture of what was wrong with a CCIE candidate's configurations. In order to eliminate this guesswork, the Internetwork Expert authors have devised a detailed grading and feedback process for these lab scenarios which enables you to quickly determine the areas you need to work on.

Grading for the lab scenarios contained within IEWB-SC is available once the scenarios are configured on our racks or the racks of our preferred vendors. Grading includes a detailed score report that illustrates which sections were configured correctly and which sections were configured incorrectly.

Incorrectly configured sections include a detailed description of what was incorrect, why it was incorrect, as well as an explanation of the intended solution. Correctly configured areas may also include hints and pointers to improve your configurations in the future. At the end of each score report, we provide a recommendation as to what areas need improvement, which may include links to recommended readings.

Internetwork Expert's grading services is one of the best methods available on the market today for truly gauging your level of understanding of CCIE™ -level technologies and topics. Utilizing this service will provide the student with a clear and focused portrait of their technological strengths and weaknesses, and an excellent yardstick for measuring their level of preparation for the CCIE™ Security Lab Exam.

Class-on-Demand

In addition to grading, Internetwork Expert offers online virtual breakdown sessions for each lab scenario contained within IEWB-SC.

These sessions, known as Class-on-Demand, are taught by the authors of the IEWB-SC workbook, Brian Dennis (CCIE #2210) and Brian McGahan (CCIE #8593), and feature explanations and configurations of each lab scenario from the ground up. By attending these Class-on-Demand sessions, you will obtain an in-depth insight into the principles behind the networking technologies covered in IEWB-SC. In addition, you will understand the reasoning behind each question and its accompanying solution, be shown configuration best practices, and learn valuable test-taking strategies.

IEWB-SC Class-on-Demand sessions are delivered on-demand, and utilize Internetwork Expert's state-of-the-art virtual classroom software. Best of all, the Class-on-Demand sessions are available at any time, allowing you to utilize our CCIE training materials around your schedule. You may view an individual Class-on-Demand session multiple times in order to completely understand the topics covered.

Note

Rack Rentals, grading, and Class-on-Demand sessions are available for purchase on an individual basis, as well as through discounted combination packages. For more information, see Internetwork Expert on the web at http://www.internetworkexpert.com.

Mock Lab Exams

After completion of Internetwork Expert's CCIE™ Security Lab Workbook the last step in your preparation should be to schedule a CCIE™ Security Mock Lab exam with Internetwork Expert to evaluate your readiness for the real thing.

Internetwork Expert's CCIE™ Security Mock Lab is a simulation of the conditions you will face in the actual CCIE Security Lab exam. In our CCIE Security Mock Lab exam you will be presented with a highly complex security lab scenario to configure. You will be allotted eight hours to configure the exam, plus an additional half hour for a lunch break (eight-and-a-half hours total).

Once the exam time has expired, your configurations will be manually graded by one of our highly skilled CCIE™ instructors, and you will be emailed a detailed score report outlining your performance. The following day you will join one of our instructors in our online classroom for a one hour one-on-one breakdown session to discuss your performance. This online session will allow you to receive live feedback from the actual instructor that graded your exam, not just a cookie-cutter response from a grading script.

Based on the results of this evaluation, our CCIE™ instructors will give you an honest recommendation of whether you are ready to take and pass the CCIE™ Security Lab exam, or if more preparation is in order. If more preparation is required, you will have a clear picture of your topical strengths and weaknesses. Based on this you will be able to maximize the remaining preparation time you have before the real lab exam.

For more information on Internetwork Expert's CCIE™ Security Mock Lab exams visit Internetwork Expert on the web at http://www.internetworkexpert.com

Support

Support for Internetwork Expert's CCIE™ Security Lab Workbook is provided free of charge via the Internetwork Expert Forum. The Internetwork Expert Forum is actively monitored and supported by the actual authors of the workbook, along with various other CCIE™ certified engineers and internetworking experts.

To get the most out of this product, join the IEWB-SC discussion on the Internetwork Expert Forum at http://forum.internetworkexpert.com.

Live Chat

In addition to the Internetwork Expert Forum, Internetwork Expert hosts a real-time text chat server where you can interact with other networking professionals to discuss this and other Internetwork Expert products. This server is hosted via Internet Relay Chat (IRC) at irc.internetworkexpert.com. To connect to this server go to http://www.internetworkexpert.com/chat/ or download a standalone IRC client such as http://www.mIRC.com.

Feedback

We are committed to your satisfaction. If you find any errors in this product, or have comments on how we can make our products better in the future, please submit them to us via email to iewb-sc@internetworkexpert.com.

Hardware Specification

Internetwork Expert's CCIE™ Security Lab Workbook uses the same hardware specification used in the actual CCIE™ Security Lab exam. This includes six routers with Ethernet, FastEthernet, Serial, ISDN, and ATM. All routers run 12.2T IOS with the Firewall Feature Set. In addition to the six routers, two Catalyst 3550 series switches running the enhanced multilayer software image (EMI) are included. Specific security-related hardware is also included, which consists of a PIX firewall running 6.3 PIX OS, an IDS 4210 running 4.x software, a VPN 3005 concentrator running 4.x software, and a Windows 2000 server for AAA, CA, and Cisco® VPN Client support, as well as GUI access to the IDS 4210 via IDS Event Viewer and the VPN 3005 via HTTP/HTTPS.

As per the actual CCIE™ lab hardware specification, IEWB-SC also includes various external devices that are not within the control of the candidate. These devices include a Frame Relay switch, an ISDN switch, and an ATM switch. In addition, three backbone routers are included to inject routes and facilitate in the testing of security related features.

The physical topology of IEWB-SC remains the same throughout the entire workbook. Therefore, once your lab has been physically cabled to meet the workbook's specification, there is no need to change the cabling in order to complete each lab.

The generic devices used in IEWB-SC include the following:

Device	Software Version	Software Feature Set	Interfaces
R1	12.2(15)T13	IP/FW/IDS PLUS IPSEC 3DES BASIC	1 - Ethernet 2 - Serial
R2	12.2(15)T13	IP/FW/IDS PLUS IPSEC 3DES BASIC	1 - Ethernet 2 - Serial
R3	12.2(15)T13	IP/FW/IDS PLUS IPSEC 3DES BASIC	2 - Ethernet 4 - Serial
R4	12.2(15)T13	IP/FW/IDS PLUS IPSEC 3DES BASIC	2 - Ethernet 1 - Serial 1 - ISDN 2 - FXS
R5	12.2(15)T13	IP/FW/IDS PLUS IPSEC 3DES BASIC	2 - Ethernet 1 - Serial 1 - ISDN
R6	12.2(11)T11	ENTERPRISE/FW/IDS IPSEC 3DES	1 - FastEthernet 1 - ATM
SW1	12.1(19)EA1	EMI Crypto	24 - FastEthernet 2 - GigEthernet
SW2	12.1(19)EA1	EMI Crypto	24 - FastEthernet 2 - GigEthernet
PIX	6.3(3)	N/A	1 - Inside 1 - Outside
VPN	4.x	N/A	1 - Public 1 - Private
IDS	4.x	N/A	1 – C&C 1 - Sensing
AAA	Windows 2000 Server	See AAA Server Section of Intro	2 - Ethernet

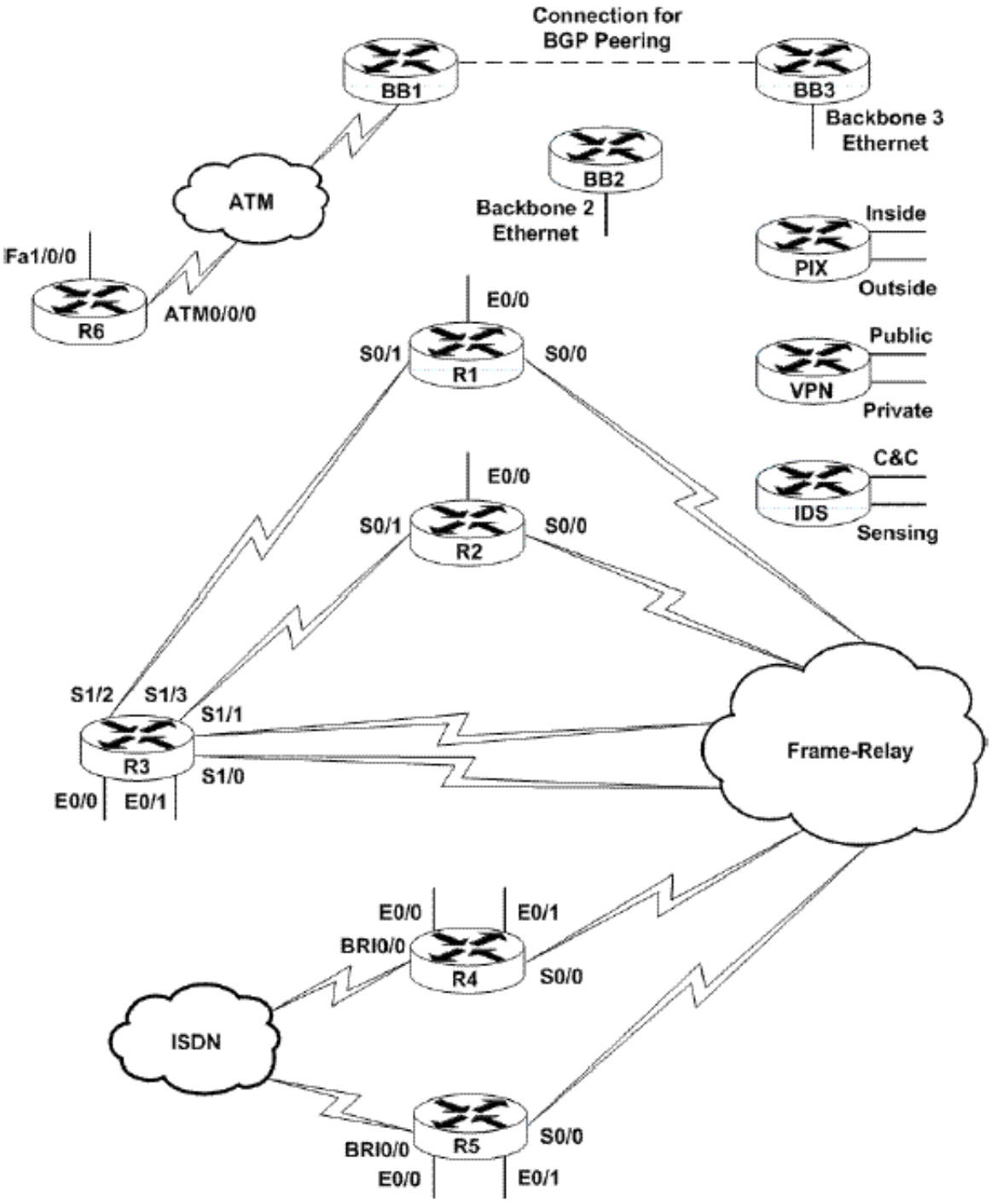
The specific devices used in design of IEWB-SC were the following

Device	Platform	DRAM	Flash	Installed WICs / Modules
R1	2610	64	16	2 - WIC-1T
R2	2610	64	16	2 - WIC-1T
R3	2611	64	16	1 - NM-4A/S
R4	2611	64	16	1 - WIC-1T 1 - WIC-1B-U 1 - NM-1V 1 - VIC-2FXS
R5	3620	64	16	1 - NM-2E2W 1 - WIC-1T 1 - WIC-1B-U
R6	7505	128	20	1 - RSP2 2 - VIP2-40 1 - PA-FE-FX 1 - PA-A1-OC3MM
SW1	3550-24-EMI	Default	Default	N/A
SW2	3550-24-EMI	Default	Default	N/A
PIX	501	Default	Default	N/A
VPN	3005	32	Default	N/A
IDS	4210	Default	Default	N/A
AAA	Windows 2000 Server	256	N/A	2 - Ethernet

The external core devices used in IEWB-SC include the following

Device	Software Version	Software Feature Set	Interfaces
BB1*	12.1(15)	Enterprise Basic	1 - ATM
BB2	12.1(15)	IP Plus	1 - Ethernet
BB3*	12.1(15)	IP Plus	1 - Ethernet
Frame Relay Switch	N/A	N/A	6 - Serial
ATM Switch	N/A	N/A	2 - ATM OC3
ISDN Switch	N/A	N/A	2 - ISDN BRI U Interfaces
* BB1 and BB3 will need to peer via iBGP with each other. This can be done over any interface, such as Ethernet, Serial, or even an AUX port to AUX port connection			

IEWB-SC Physical Cabling Connections



IEWB-SC Physical Interface Connections

ISDN	
Switch Type	basic-ni
R4 BRI0/0 SPID1	52720X4
R5 BRI0/0 SPID1	52720X5

Frame Relay Switch Configuration					
Local Router	Local Interface	Local DLCI	Remote Router	Remote Interface	Remote DLCI
R1	S0/0	102	R2	S0/0	201
R1	S0/0	103	R3	S1/0	301
R1	S0/0	113	R3	S1/1	311
R1	S0/0	104	R4	S0/0	401
R1	S0/0	105	R5	S0/0	501
R2	S0/0	201	R1	S0/0	102
R2	S0/0	203	R3	S1/0	302
R2	S0/0	213	R3	S1/1	312
R2	S0/0	204	R4	S0/0	402
R2	S0/0	205	R5	S0/0	502
R3	S1/0	301	R1	S0/0	103
R3	S1/0	302	R2	S0/0	203
R3	S1/0	304	R4	S0/0	403
R3	S1/0	305	R5	S0/0	503
R3	S1/1	311	R1	S0/0	113
R3	S1/1	312	R2	S0/0	213
R3	S1/1	314	R4	S0/0	413
R3	S1/1	315	R5	S0/0	513
R4	S0/0	401	R1	S0/0	104
R4	S0/0	402	R2	S0/0	204
R4	S0/0	403	R3	S1/0	304
R4	S0/0	413	R3	S1/1	314
R4	S0/0	405	R5	S0/0	504
R5	S0/0	501	R1	S0/0	105
R5	S0/0	502	R2	S0/0	205
R5	S0/0	503	R3	S1/0	305
R5	S0/0	513	R3	S1/1	315
R5	S0/0	504	R4	S0/0	405

Ethernet Connections			
Local Router	Local Interface	Remote Router	Remote Interface
R1	E0/0	SW1	Fa0/1
R2	E0/0	SW1	Fa0/2
R3	E0/0	SW1	Fa0/3
R3	E0/1	SW2	Fa0/3
R4	E0/0	SW1	Fa0/4
R4	E0/1	SW2	Fa0/4
R5	E0/0	SW1	Fa0/5
R5	E0/1	SW2	Fa0/5
R6	Fa1/0/0	SW1	Fa0/6
IDS	C&C	SW1	Fa0/10
IDS	Sensing	SW2	Fa0/10
PIX	Inside	SW1	Fa0/11
PIX	Outside	SW2	Fa0/11
VPN	Private	SW1	Fa0/12
VPN	Public	SW2	Fa0/12
AAA	Inside	SW1	Fa0/20
SW1	Fa0/13	SW2	Fa0/13
SW1	Fa0/14	SW2	Fa0/14
SW1	Fa0/15	SW2	Fa0/15

AAA Server

In addition to the six routers, two switches, and three security devices, a Windows® 2000 Server is required to run CiscoSecure ACS Server (AAA), IDS Event Viewer, Cisco VPN Client, and a web browser for GUI access to the IDS 4210 and VPN 3005.

Although the PC is listed to have two Ethernet interfaces, only one is required if the PC is being accessed locally with a keyword and monitor. Two interfaces are used on Internetwork Expert's racks in order to allow remote access to the Windows® GUI via Remote Desktop Connection and VNC.

An evaluation version of CiscoSecure ACS Server, the IDS Event Viewer, and the Cisco VPN Client can be obtained from cisco.com with a valid service contract. Use the following links to download these software packages.

CiscoSecure ACS:
http://www.cisco.com/kobayashi/sw-center/cw2000/crypto/90dayeval/

IDS Event Viewer:
http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto/

Cisco VPN Client:
http://www.cisco.com/kobayashi/sw-center/vpn/client/

Note

As of the publishing of this workbook IDS Event Viewer will not run on Windows® 2003 Server. Although Windows® 2000 Server evaluation software can no longer be downloaded directly from microsoft.com, it can still be obtained through the purchase of many MSCE 2000 publications, such as "MCSA/MCSE Self-Paced Training Kit (Exam 70-215): Microsoft® Windows® 2000 Server, Second Edition" ISBN 0-7356-1767-8. For more information on which Microsoft® publications include Windows® 2000 Server evaluations visit Microsoft® Press on the web at http://www.microsoft.com/mspress/

IE's Security Workbook Lab 1

Difficulty Rating (10 highest): 6

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	7
ISDN/PPP	12
Routing Protocols	15
VPN	15
IP Services	2
General Security	11
Advanced PIX Firewall	15
AAA	12
IDS	11

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain CCIE_SECURITY between SW1 and SW2.
1.2. Authenticate the VTP domain with the password CISCO.

1 Point

1.3. Recently, your manager read a horror story on the Internet about someone plugging a rogue switch into the network with a high configuration revision number and crashing the network. Immediately afterwards your manager tasked you with preventing this problem from occurring. Configure the network to reflect your manager's request.

2 Points

1.4. In order to improve security in the access layer of the network, your security team has suggested that hosts connecting to the network should use username and password authentication. In order to test out this setup before deploying it network-wide, a Windows® XP host has been connected to port Fa0/17 of SW1.
1.5. The Windows® XP host will be sending the username HOST and a password of CISCO.
1.6. Configure SW1 to forward this authentication request on to the RADIUS server at 10.0.0.100. If authentication is successful, the host should be allowed access to the network. If authentication fails, the host should be denied access to the network.
1.7. SW1 should authenticate to the RADIUS server using the password CISCO.
1.8. SW1 should send the authentication request to the RADIUS server using the source IP address 150.X.7.7.

4 Points

2. ISDN/PPP

2.1. Configure ISDN DDR between R4 and R5 using dialer profiles.
2.2. R4 should initiate a call to R5 irrespective of interesting traffic. R5 should not drop the call due to the lack of interesting traffic or initiate a call based on interesting traffic.
2.3. Do not use dialer watch for this task.

2 Points

2.4. Configure PPP authentication on R4 and R5 to meet the following requirements:
- R4 should only challenge the remote end if the call direction is outbound
- R4 should challenge using the hostname ROUTER4
- R5 should challenge for both inbound and outbound calls, but should allow the remote end to refuse authentication
- R5 should challenge using the hostname ROUTER5
- R5 should authenticate R4 using the AAA server using TACACS+

2.5. Apply the appropriate configuration to the AAA server for this task.

3 Points

2.6. The primary purpose of the ISDN connection between R4 and R5 is to back up the Frame Relay connection between them. Whenever the Frame Relay connection is up, R4's dialer interface should be in standby state. Upon R4's subinterface S0/0.345 going down, R4 should initiate the ISDN connection to R5.
2.7. For cost control and added security, when R5 receives the call from R4, R5 should drop the call and retrieve a callback string from the AAA server. R5 should then call back R4 using the callback string provided by the AAA server.
2.8. Apply the appropriate configuration to the AAA server for this task.

4 Points

2.9. An ATM PVC using AAL5SNAP encapsulation has been provisioned between R6 and BB1. The VPI for this PVC is 0 and the VCI is 20X.
2.10. Use the IP address 54.X.7.6/24 for this interface.
2.11. For added security, the circuit will require CHAP authentication. Configure R6 to respond to CHAP challenges from BB1 with the hostname of ROUTER6 and a hash value that represents the password of CISCO. R6 should not authenticate BB1.
2.12. R6 should be able to ping BB1 (54.X.7.254) and its own IP address of 54.X.7.6.

3 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.3. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.4. Create three static routes on the PIX with a next hop of 183.X.119.11. The first static should point to 192.10.X.0/24, the second to 10.8.8.0/24, and the last to 150.X.8.0/24.
3.5. Configure RackXPIX as the PIX's hostname.

2 Point

3.6. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.7. The IDS should use R1 as its default gateway.
3.8. Configure RackXIDS as the IDS's hostname.

1 Point

3.9. Configure OSPF area 51 between SW2, the VPN3005, and BB2.
3.10. The VPN3005 should advertise reachability information about the rest of the network to SW2 and BB2.
3.11. You are allowed to configure static routes on the VPN3005 to accomplish this.

2 Points

3.12. Configure OSPF area 100 on the PIX to connect to R1.
3.13. Configure the PIX to advertise a default route to the rest of the OSPF routing domain.

2 Points

3.14. Authenticate all OSPF adjacencies within area 0 using a secure hash value of the password CISCO.

2 Points

3.15. The OSPF adjacency between R3 and R5 should use a hash value based off the password CISCO35.
3.16. The OSPF adjacency between R4 and R5 should use a hash value based off the password CISCO45.

2 Points

3.17. Authenticate the OSPF area 100 adjacencies between R1, R2, R3, and the PIX using the clear-text password CISCO.
3.18. Do not use the **ip ospf authentication** interface command on R1, R2, or R3's connection to the Frame Relay cloud to accomplish this.
3.19. Do not authenticate the adjacency between R3 and SW1.

3 Points

4. VPN

4.1. The network administrator has requested that the network be configured to allow communication between hosts in VLAN 4 and 41.
4.2. Hosts in VLAN 4 should appear to be in the 10.4.4.0/24 network to hosts in VLAN 41.
4.3. Hosts in VLAN 41 should appear to be in the 10.7.7.0/24 network to hosts in VLAN 4.
4.4. The use of two static routes is permitted for this task.

1 Point

4.5. Create a LAN-to-LAN VPN between VLAN 4 and 41 over the Frame Relay cloud on R3 and R4 using the following parameters:
- ISAKMP Authentication Method: RSA-SIG
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
- ESP Encryption: AES-256
- ESP Authentication: HMAC-MD5

4.6. This configuration should continue to function when the ISDN backup is active between R4 and R5.

5 Points

4.7. After recent security issues in VLAN 2, the network administrator has requested that R2's interface E0/0 be configured to support Cisco's VPN client using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: SHA
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-SHA
- Address Pool: 192.168.0.1-192.168.0.50
- Group Name: IELAB
- Group Password: CISCO
- DNS Server: 183.X.46.100
- WINS Server: 183.X.46.100
- Domain: internetworkexpert.com
- Allow for split tunneling to destinations not in the 183.X.0.0/16 network

4.8. Without using a static route, configure R2 to inject the VPN client's IP address into its routing table to ensure IP reachability.

5 Points

4.9. Create a LAN-to-LAN VPN on the VPN3005 and the PIX between the 10.8.8.0/24 and the 183.X.19.0/24 subnets using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5

4.10. Configure the VPN3005 so that hosts in the 183.X.19.0/24 subnet can not ping hosts in the 10.8.8.0/24 subnet through this VPN tunnel.

4 Points

5. IP Services

5.1. The network administrator has requested that R4 be configured to log all severity 6 and below messages to a syslog server located at 10.0.0.100.

5.2. To help guard against tampering with the syslog messages on the server itself, R4 should include a sequence number for each log message.

2 Points

6. General Security

6.1. Recently, it was discovered that hosts behind BB3 were attempting to gain access to one of the company's main file servers. Your manager has requested that R3 be secured according to the following requirements.

- Treat interface E0/0 as the outside interface and all other interfaces as inside interfaces
- Drop packets that contain their own routing information
- Using CBAC (firewall feature set), permit returning TCP/UDP sessions and ICMP traffic that were initiated from behind R3 inbound on the outside interface
- Permit HTTP and HTTPS access to a web server with the IP address of 183.X.19.100
- Permit traceroute replies inbound on the outside interface
- Log all packets denied by access-lists to a syslog server at 10.0.0.100
- These log messages should include the layer 2 address of the packet that was denied
- Allow for a maximum of 500 unassembled IP packets and twice the default packet state structure timeout
- Close half-open TCP session after 15 seconds
- Start tearing down half-open TCP sessions when the number exceeds 1500, and stop when they fall back down to 750
- Allow users on R3 itself to ping and telnet to BB3
- Permit all necessary routing protocol
- Deny all other traffic

5 Points

6.2. Additionally, in order to reduce the filtering overhead on R3, your manager has requested that all packets destined to TCP port 139 be dropped prior to reaching R3's interface E0/0.
6.3. Do not make changes to R3's configuration to accomplish this task.

2 Points

6.4. A new corporate policy dictates that management through the CLI on R4 and R6 be performed using SSH. Telnet access to R4 and R6 should be disabled.
6.5. Users will be authenticating with the username SSH and the password CISCO.
6.6. Allow SSH connections sourced from any 183.X.0.0/16 IP address.

2 Points

6.7. The network administrator has voiced concerns that R6's ATM connection to BB1 is not secure. The network administrator would like to only allow packets in from BB1 that were initiated from behind R6.
6.8. Configure R6 to monitor TCP and UDP traffic as it flows out its ATM interface to BB1 and dynamically permit the return packets inbound.
6.9. Statically permit the BGP peering session with BB1 and ICMP echo-replies inbound. All other traffic should be silently dropped.
6.10. Do not use CBAC (firewall feature set) for this task.

2 Points

7. Advanced PIX Firewall

7.1. Configure the PIX to translate any inside host's IP address to the outside interface's IP address.
7.2. Allow for a maximum of 10000 simultaneous connections.

2 Points

7.3. The network administrator is concerned with the possibility of internal hosts participating in a DoS attack, and would like the PIX configured so that once a 4000 embryonic connection threshold has been breached, the PIX will intercept TCP SYN packets on behalf of the destination. Once the number of embryonic connections falls below 4000, the PIX should stop intercepting TCP SYN packets.

2 Points

7.4. Permit telnet access to the PIX from any IP address on the inside interface.
7.5. Ensure that when users telnet into the PIX they receive all possible syslog messages.
7.6. Users logged into the PIX via the console should only receive severity level 5 and below messages.

2 Points

7.7. Users on the inside of the PIX have complained that they are unable to ping or traceroute to IP addresses on the outside.
7.8. Configure the PIX to allow the inside users to successfully ping and traceroute to IP addresses on the outside of the PIX.

2 Points

7.9. In the future, a multicast server will be installed in VLAN 19. This server will need to send a multicast stream (225.25.25.25) to a client located in VLAN 119.
7.10. Configure the PIX to allow this multicast stream through.

3 Points

7.11. Your company has hired an outside consultant to help configure the PIX firewall. Since the consultant is uncomfortable using the CLI, he has asked that the PIX be configured to allow management using the PDM. After voicing concerns with your manager that GUIs are for beginners and the CLI is the ONLY way to configure a firewall, your manager insisted that the PIX be configured to allow the consultant access via HTTP.

7.12. Configure the PIX to support the PDM from the consultant's computer's IP address of 183.X.19.50.

2 Points

7.13. After recent incorrect changes were made to the company's DNS server, a host in VLAN 119 with the IP address of 183.X.119.200 incorrectly resolves to 183.X.119.20.

7.14. The network administrator has requested that the PIX be configured to redirect packets from the inside destined for 183.X.119.20 to 183.X.119.200.

2 Points

8. AAA

8.1. Recently a W32.Blaster.Worm variant infected Windows servers located in VLAN 19. The variant propagated itself to other Windows servers using TCP port 135. In order to help stop the spread of the worm until a software patch for the server is released, the network administrator recommended that the R1 and PIX block TCP port 135 traffic. However, the internal software development team manager voiced concerns that the development team needs TCP port 135 permitted through R1 and the PIX. In order to stop the spread of the worm, but still permit legitimate TCP port 135 traffic, users will be required to authenticate to R1 or the PIX prior to being permitted out of VLAN 19 on TCP port 135.

8.2. Configure the PIX to require users to authenticate by opening a HTTP connection to 183.X.19.100 and entering username USER1 along with the password of CISCO prior to permitting TCP port 135 connections through.

8.3. The PIX should authenticate this user against the AAA server.

8.4. Apply the appropriate configuration to the AAA server for this task.

4 Points

8.5. When users in VLAN 19 need to connect on TCP port 135 through R1, these users should be required to create a HTTP connection to R1 and authenticate prior to R1 permitting the TCP port 135 traffic through.
8.6. R1 should only allow TCP port 135 connections inbound on interface E0/0 for sessions that have been authenticated.
8.7. R1 should use TACACS+ with the AAA server for authenticating these sessions.
8.8. Users will be authenticating using the username TCP135 along with the password of CISCO.
8.9. Apply the appropriate configuration to the AAA server for this task.

4 Points

8.10. The network administrator would like to enable NOC users to perform basic administrative tasks on R5 according to the following requirements:

- Authenticate telnet sessions using the username NOC and the password CISCO
- This authentication should occur against the local username/password database
- The NOC user's password should be stored as an MD5 hash in R5's configuration
- Without using the **username** command with *privilege* option or the **privilege level** line command, place the NOC user in privilege level 5 upon logging in
- Give the NOC user access to the **clear line** and **clear counters** commands
- Account for the privilege level 5 commands using the AAA server
- Use TACACS+ as the communication protocol with the AAA server
- Source the TACACS+ session off R5's Loopback 0 interface

8.11. Apply the appropriate configuration to the AAA server for this task.

4 Points

9. IDS

Read the access instructions for the IDS Sensor in the introduction for this lab prior to starting this section.

9.1. An IDS sensor has been installed to monitor traffic between the PIX and the VPN3005.
9.2. Only allow management of the IDS sensor via HTTPS from the AAA server's IP address of 10.0.0.100.
9.3. Span traffic from between the PIX and VPN3005 to the IDS sensor's sensing interface.

3 Points

9.4. Configure the IDS Event Viewer to manage the IDS sensor.
9.5. Alter the default view to filter traffic destined to the PIX's outside IP address.

1 Point

9.6. Configure a manual shun on the IDS sensor to deny all packets inbound on the outside interface of the PIX sourced from 208.50.100.67.
9.7. This manual shun should never timeout.

2 Points

9.8. The network administrator would like to be notified whenever someone changes the password through a telnet connection. Create a custom signature to trigger an alarm of high severity whenever a telnet session contains the string "password".

2 Points

9.9. In addition to your manager's earlier request to secure R3's interface E0/0, your manager has requested that R3 perform intrusion detection inbound on its E0/0 interface.

9.10. Configure R3 to meet the following requirements:

- Log alarms to a syslog server located at 10.0.0.100
- Send only the necessary messages to the syslog server
- Alarm and drop packets that trigger on any information-gathering alarms
- Disable the "Fragmented ICMP Traffic" signature
- Do not include the 183.X.37.64 through 183.X.37.127 IP addresses as part of the protected network

3 Points

This page left intentionally blank

IE's Security Workbook Lab 2

Difficulty Rating (10 highest): 6

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	4
ISDN/PPP	5
Routing Protocols	14
VPN	16
IP Services	9
General Security	27
Advanced PIX Firewall	12
AAA	7
IDS	6

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain IE_SEC between SW1 and SW2.
1.2. Authenticate the VTP domain with the password CISCO.

1 Point

1.3. Your network administrator has voiced some concerns relating to the security of SW1's port Fa0/16 which is being used in the company's public conference room. In order to provide added security for this connection, the network administrator has requested that only a device with the MAC address of 1234.5678.9abc be allowed to connect this port.
1.4. If any other device attempts to connect to SW1's port Fa0/16 a log message should be generated and the port's state should be changed to error-disabled.

3 Points

2. ISDN/PPP

2.1. Configure ISDN DDR between R4 and R5 using the physical BRI interfaces.
2.2. Any IP traffic should be permitted to initiate and maintain a call, but OSPF should not keep an ISDN connection up unnecessarily.

2 Points

2.3. Configure PPP encapsulation on the ISDN link between R4 and R5.
2.4. When R5 calls R4, R4 should issue an authentication challenge with the username ROUTER4. When R5 receives this challenge, it should respond with the username ROUTER5 and a hash value that represents the password CISCO.
2.5. R5 should never authenticate R4.
2.6. Use local AAA authentication for this task.

3 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. The VPN3005 should use R5 as its default gateway.
3.3. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.4. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.5. Configure RackXPIX as the PIX's hostname.

1 Point

3.6. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.7. The IDS should use R1 as its default gateway.
3.8. Configure RackXIDS as the IDS's hostname.

1 Point

3.9. Authenticate all OSPF adjacencies within areas 0 and 170 using simple password authentication.

2 Points

3.10. Authenticate all OSPF adjacencies within area 345 using the strongest authentication type supported by OSPF.

1 Point

3.11. Configure RIPv2 between R2 and the PIX.
3.12. The PIX should generate a default route to R2.
3.13. Authenticate RIP updates between R2 and the PIX using the password CISCO. This password should be sent in clear text.

2 Points

3.14. Configure RIPv2 between R6 and the PIX.
3.15. The PIX should generate a default route to R6.
3.16. Authenticate RIP updates between the PIX and R6 using a hash value that represents the password CISCO.

2 Points

3.17. Configure a BGP peering session through the PIX between R2 and R6.
3.18. Secure the BGP peering session between R2 and R6 using a hash value that represents the value of CISCO.

2 Points

3.19. Configure OSPF area 51 on the private interface of the VPN3005.
3.20. Use 150.X.11.11 as the OSPF router ID.
3.21. Configure static routes on the VPN3005 for the 54.X.1.0/24, 132.X.0.0/16, 150.X.0.0/16, 204.12.X.0/24, and 10.0.0.0/8 networks pointing to 132.X.115.5.
3.22. These static routes should be redistributed into OSPF and appear in BB2's routing table as E2 routes.

2 Points

4. VPN

4.1. A new corporate policy has dictated that all traffic between VLAN 44 and VLAN 3 be encrypted.

4.2. If R3 or R4 lose their Frame Relay connection to R2, the encrypted traffic should flow across the ISDN through R5. The traffic should remain encrypted when using the ISDN connection.

4.3. This encrypted traffic should use the following parameters:

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: Default
- ISAKMP Encryption: DES
- ISAKMP SA Lifetime: 2400 seconds
- ESP Encryption: DES
- ESP Authentication: HMAC-MD5

4.4. The use of static routes is permitted for this task.

4 Points

4.5. Configure the PIX to support Cisco's VPN client using the following parameters:

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: SHA
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5
- Address Pool: 10.255.255.1-10.255.255.254
- Group Dame: CCIELAB
- Group Password: CISCO
- Username: CCIEUSER
- User Password: CISCO
- DNS Server: 132.X.29.50
- Default Domain: internetworkexpert.com
- Idle Timeout: 1800 seconds

4.6. Using AAA, the PIX should authenticate this user against its local username/password database.

4 Points

4.7. Encrypt all ICMP ping traffic between R1 and R6's Loopback0 interfaces using the following parameters:

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: Default
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-SHA

4 Points

4.8. Create a LAN-to-LAN VPN between the 192.10.X.0/24 network on the VPN3005 and the 10.3.3.0/24 network on R3 using the following parameters:

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- Diffie-Hellman Group: 2
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5

4.9. This configuration should continue to function in the event the VPN3005's public IP address is changed.

4 Points

5. IP Services

5.1. Configure NAT on R4. Interface S0/0.1234 and interface BRI0/0 should be the outside interfaces and interface E0/0 should be the inside interface.
5.2. Use 132.X.255.0/24 for the address pool. Advertise this network into OSPF. The use of one static route is permitted.
5.3. A web server with the IP address of 132.X.4.100 should be reachable via the IP address 132.X.255.100. The web server is running on the standard HTTP port of 80. SSL connections should also be permitted to this server.
5.4. Any attempts to FTP to this server should be redirected to 132.X.4.101.
5.5. Users should still be allowed to telnet to R4 using the outside interfaces' IP addresses and the Loopback0 address.

4 Points

5.6. Your manager has become concerned with packets coming from BB1 with spoofed source IP addresses. Configure R6 to drop packets without a verifiable source address received on its ATM connection to BB1.

2 Points

5.7. Create an additional Loopback interface (Loopback2) on R3 using the IP address 1.1.1.1/32.
5.8. Ensure all telnet sessions from R3 will automatically source their connection off of this new Loopback interface.
5.9. Do not advertise this new Loopback with any routing protocol but ensure that R3 can still telnet to other devices (i.e. R1, R2, etc).

3 Points

6. General Security

6.1. After returning from a network security class, one of your network administrators has convinced your manager that R6 is open to many security vulnerabilities. To say the least, your manager is not happy that these vulnerabilities have been left unchecked for so long.

6.2. In order to appease your manager, configure R6 to conform to the following security recommendations:

- Configure the ATM interface to confirm to RFC 2827
- Disable CDP and proxy-arp on the Ethernet segment to the PIX
- Disable BOOTP and DHCP server
- A banner message should be displayed to all users that telnet into the router that states:

  Access to this device or the attached networks is prohibited without express written permission. Violators will be pinged on sight.

3 Points

6.3. Your NOC engineers have noticed that SW2 is being polled via SNMP from an unauthorized source which appears to be coming in from behind BB3. After complaining to the network administrator of BB3 to help track the source of the SNMP polling, you have decided to just filter the SNMP traffic from BB3.

6.4. After putting in a change control request to add the SNMP filtering, management has rejected the request as the last change to SW2 caused a major network outage.

6.5. Since management will not allow changes to SW2, configure SW1 to filter SNMP packets destined for SW2 that are sourced from any IP address other than IP addresses belonging to the 132.X.0.0/16 network.

3 Points

6.6. After further investigation it appears that the device polling SW2 via SNMP is internal to your network.
6.7. In order to help track down the source of the SNMP packets, configure SW2 to generate a log message whenever a device attempts to poll it using the Read-Only community string 'public'.
6.8. These log messages should be sent to a syslog server at 132.X.33.100.

2 Points

6.9. Your manager has determined that R1 and SW1 should only be managed via SSH as opposed to telnet.
6.10. Configure SSH support on R1 and SW1.
6.11. Authenticate users against the AAA server at 10.0.0.100.
6.12. Users will be authenticating with the username SSH and the password of CISCO.
9.11. Apply the appropriate configuration to the AAA server for this task.

2 Points

6.13. Authenticate users logging into R6 using local AAA authentication.
6.14. Configure the usernames NOC and ADMIN both with passwords CISCO.
6.15. Users that enter using username NOC should be placed in privilege level 0. After entering the router they should be allowed access to privilege level 1 by using the password of LEVEL1.
6.16. Users that login with the username of ADMIN should be automatically placed in privilege level 15.

3 Points

6.17. In response to recent ICMP DoS attacks on a web server located in VLAN 69, a new company policy dictates that ICMP echo traffic inbound on R6's ATM connection to BB1 should be limited to 128kbps.
6.18. After implementing this new policy you have noticed that legitimate ICMP echo requests are being dropped. In order to help deal with this issue, you have decided to allow the ICMP traffic to burst to 25% of the allowed rate.

3 Points

6.19. After recent security issues internal to your network, your manager has requested that R1's interface E0/0 be secured. After trying to figure out what your manager meant by "secured", you have decided to just implement CBAC (firewall feature set) on R1 using the following parameters:

- Treat interface E0/0 as the outside interface and S0/0.1234 as the inside interface
- Allow all TCP and UDP sessions initiated from the inside to return inbound on the outside interface
- Permit outside hosts to connect via SSH to any device on the inside of R1 with the exception of outside hosts in the 204.12.X.0/24 network
- Permit all HTTP connections inbound
- Permit all necessary routing protocol traffic inbound
- Deny all other traffic

6.20. Do not apply an outbound access-list on R1's interface E0/0 to accomplish this task.

5 Points

6.21. On R1, configure CBAC to timeout idle TCP sessions after 30 minutes of inactivity. Inactive UDP sessions should be timed out after three (3) minutes.

1 Point

6.22. Recently a new worm has been spreading through the Internet by exploiting a known vulnerability in Microsoft's Internet Information Server (IIS). Your manager is worried that the internal IIS servers located in VLANs 3 and 33 will be affected by this worm, and has asked that R1 and R6 be configured to prevent this worm from coming in their Internet connections to BB1 and BB3. The only information you have about this worm is that it sends a HTTP GET request containing the strings "cmd.exe" or "root.exe".

6.23. Configure R1 to drop any HTTP packets received on interface E0/0 that contain URLs with these strings before forwarding the packets out interface S0/0.1234.

6.24. Configure R6 to drop any HTTP packets received across the ATM cloud that contain URLs with these strings before forwarding the packets out on interface Fa1/0/0.

5 Points

7. Advanced PIX Firewall

9.12. Configure the PIX to translate any inside host's IP address to the outside interface's IP address.

1 Point

7.1. A web server has recently been installed in VLAN 29. The server's IP address is 132.X.29.100. The network administrator has requested that this web server be available to users outside of the PIX. This web server should be accessible from outside of the PIX via the IP address 132.X.69.100.

7.2. Permit both HTTP and SSL connections to this server.

2 Points

7.3. Any FTP connections that are attempted to this new web server's outside IP address (132.X.69.100) should be redirected to a FTP server at 132.X.29.101. This FTP server is configured to permit FTP sessions on both port 21 and 10021.

7.4. To maintain compliance with the corporate security policy, ensure that the PIX performs application inspection for the FTP connections made to port 10021 along with port 21.

2 Points

7.5. Using only one access-list entry on the PIX, permit any device on the inside of the PIX to ping and traceroute to destinations outside of the PIX.

2 Points

7.6. In order to ensure accurate time on the PIX, the network administrator has requested the PIX be configured to receive time via NTP from BB1.

7.7. For added security, configure the PIX to authenticate BB1's NTP updates using key 1 with an MD5 hash that represents the value CISCO.

2 Points

7.8. Create an additional Loopback interface on R2 and R6. Use the 10.2.2.2/24 IP address for R2 and 10.6.6.6/24 for R6.
7.9. Create a GRE tunnel between R2 and R6. Use the 10.26.26.0/24 subnet for addressing inside this tunnel with R2 using .2 and R6 using .6.
7.10. Configure R2 and R6 to advertise these new Loopbacks to each other using EIGRP AS 1. Do not redistribute or advertise these networks (new Loopbacks and tunnel) into any other routing protocol.

3 Points

8. AAA

8.1. Against your recommendation, the network administrator has decided that R5 should be managed via HTTP.
8.2. Configure R5's HTTP management server to use TCP port 8080.
8.3. Authenticate users via TACACS+ with the AAA server using the following parameters:
- Authenticate the TACACS+ session with the AAA server using the password CISCO
- Source the TACACS+ session off R5's Loopback0 interface
- The users will be authenticating with the username R5WEB and the password CISCO

9.13. Apply the appropriate configuration to the AAA server for this task.

3 Points

8.4. Configure R3 to authenticate users telneting into it with the following requirements:
- Authenticate the TACACS+ session with the AAA server using the password CISCO.
- Create a user named USER1 with the password CISCO in the AAA server. USER1 should be placed in privilege level 15 upon login.
- When USER1 successfully logs in, execute the **show users** command automatically, but do not automatically log USER1 off R3 after the **show users** command executes.
- Create a user named USER2 with the password CISCO in the AAA server. USER2 should be placed in privilege level 2 and given access to all debug commands and the **undebug all** command.

4 Points

9. IDS

Read the access instructions for the IDS Sensor in the introduction for this lab prior to starting this section.

9.1. An IDS sensor has been installed to monitor traffic as it enters your network via the Ethernet connection to BB3. The command and control interface is connected to SW1's interface Fa0/10.
9.2. Allow management via telnet and HTTPS from IP addresses in the 10.0.0.0/24 network.

1 Point

9.3. Span traffic from SW1's interface Fa0/24 to the IDS sensor's sensing interface which is connected to SW2's interface Fa0/10. Use VLAN 111 as the remote-span VLAN.

1 Point

9.4. Configure the IDS to support shunning on SW1 and SW2.
9.5. Enable the IDS sensor to access SW1 using the username IDS and the password CISCO via SSH. SW2 should be accessible via telnet using the same username/password combination.
9.6. The blocking interfaces should be the VLAN783 interfaces on both SW1 and SW2.
9.7. The IDS sensor should never block BB3's IP address of 204.12.X.254.

2 Points

9.8. Configure the IDS Event Viewer on the Windows 2000 Server for viewing of the IDS sensor's alarms.
9.9. Alter the default view on the IDS Event Viewer to exclude any ARP related signatures.
9.10. Enable all L2/L3/L4 Protocol signatures on the IDS sensor with the exception of the "RFC1918 address" signature.

2 Points

IE's Security Workbook Lab 3

Difficulty Rating (10 highest): 8

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	5
ISDN/PPP	11
Routing Protocols	10
VPN	21
IP Services	9
General Security	12
Advanced PIX Firewall	13
AAA	12
IDS	7

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain IE_SEC between SW1 and SW2.
1.2. Authenticate the VTP domain with the password CISCO.

1 Point

1.3. Recently an 802.11b access point has been connected to port Fa0/23 of SW2 as a test install before a full scale wireless implementation. However, one of your top executives has not been happy with the performance of it. After further investigation, you have determined that there are too many users being serviced by this single access point. Since this executive has the final say in whether your group will get the funding for the project, your local Cisco® SE has recommended that you restrict access through the access point only to the executive. Since you don't want the executive to suspect anything, you do not want to have to ask him for the MAC address of his wireless card. In order to accomplish this, configure SW2 so that traffic is only allowed in from the access point if it is sourced from the executive's PC. Assume that this PC will be the first to connect to the access point after this configuration is performed.

4 Points

2. ISDN/PPP

2.1. Using PPP encapsulation, configure ISDN DDR between R4 and R5.
2.2. R4 should use dialer profiles and R5 should use legacy ISDN.
2.3. R4 and R5 should permit any IP traffic to initiate and maintain a call.
2.4. Do not permit any other protocols across the ISDN connection other than IP.

3 Points

2.5. Configure R4 to authenticate R5 using CHAP authentication.
2.6. R4 should refuse to be authenticated via CHAP or PAP authentication.
2.7. Configure R5 to attempt authentication of R4 using CHAP. If CHAP is not accepted by R4, R5 should offer PAP authentication. If PAP authentication is refused, R5 should still allow the connection to come up.
2.8. R5 should not use any username commands or authenticate with the AAA server for this task.

4 Points

2.9. R4 should allow for a maximum of three failed authentication attempts before dropping a call.

1 Point

2.10. Configure a subinterface .1 on R6.
2.11. Configure the ATM PVC 0/30X on this subinterface.
2.12. Configure PPP over ATM on this VC using interface Dialer1.
2.13. The IP address of this interface should be 54.X.8.6/24.
2.14. BB1 is configured to authenticate R6 using PAP authentication. R6 should use the username ROUTER6 and the password CISCO for PAP authentication.
2.15. Do not use the **ppp authentication pap** interface command to accomplish this task.

3 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.3. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.4. Configure RackXPIX as the PIX's hostname.

1 Point

3.5. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.6. The IDS should use R2 as its default gateway.
3.7. Configure RackXIDS as the IDS's hostname.

1 Point

3.8. Authenticate the EIGRP adjacencies between R1, R4, and R5 using a secure hash value of the password CISCO.

1 Point

3.9. Configure OSPF area 51 on the VPN3005's public and private interfaces.
3.10. The VPN3005 should use 150.X.11.11 as its OSPF router ID.
3.11. All OSPF adjacencies in OSPF area 51 should be authenticated with the clear-text password CISCO.

2 Points

3.12. Configure OSPF area 0 on the outside interface of the PIX using process-id 1.
3.13. The AAA server is preconfigured to expect authenticated OSPF adjacencies using the clear-text password CISCO. Configure the PIX to accommodate this adjacency.

2 Points

3.14. Configure OSPF area 0 on the inside interface of the PIX using process-id 2.
3.15. All OSPF adjacencies in OSPF this area 0 should be authenticated with a secure hash value of the password CISCO.
3.16. Advertise the routing information learned on the outside interface of the PIX to the OSPF routing domain running on the inside interface of the PIX.

2 Points

4. VPN

4.1. The network administrator has requested that a host in VLAN 39 be given access to a server located in VLAN 52. The traffic should be encrypted between this host and R5. The host will be using Cisco's VPN Client.

4.2. Configure R5 to support Cisco's VPN client using the following parameters:

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-SHA
- Address pool: 10.105.105.1-10.105.105.50
- Group Name: IPSECGROUP
- Group Password: CISCO
- Username: IPSECUSER
- Password: CISCO

4.3. This configuration should continue to function in the event that R5's Frame Relay connection to R1 is down.

4.4. R5 should authenticate this user against the AAA server using TACACS+. If communication with the AAA servers fails, R5 should authenticate the user locally. Apply the appropriate configuration to the AAA server for this task.

6 Points

4.5. Using only one GRE tunnel, configure a full meshed GRE tunnel topology between R1, R4, and R5. Source the tunnel off each router's respective Loopback 0 interface. Use 10.255.255.Y/24 for addressing inside the tunnel.

4.6. Do not use the **tunnel destination** interface command to accomplish this task.

2 Points

4.7. Create additional Loopback interfaces (Loopback 1) on R1, R4, and R5. Use 10.255.Y.Y/24 for addressing on these new Loopback interfaces.

4.8. On R1, R4, and R5 enable OSPF area 0 for the Loopback 1 and GRE tunnel interface (10.255.Y.Y/24 and 10.255.255.Y/24).

4.9. Advertise the Loopback 1 networks as /24's into OSPF.

1 Point

4.10. Encrypt the multipoint GRE tunnel on R1, R4 and R5 using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: AES-256
- ESP Authentication: HMAC-SHA

4.11. To reduced unnecessary overhead, this configuration should not encapsulate the IP header of the GRE packets.

4.12. Ensure this configuration continues to function in the event that R4 and R5 are routing across the ISDN to reach each other's Loopback 0 interfaces.

4 Points

4.13. On R4 and the VPN3005, encrypt IP traffic between 174.X.38.0/24 and the following subnets: 174.X.1.0/24, 174.X.4.0/24, 174.X.45.0/24, and 174.X.145.0/24

4.14. The VPN3005 should not permit HTTP traffic through the IPSec tunnel.

4.15. Limit the IPSec tunnel to 128kbps on the VPN3005.

4 Points

4.16. The network administrator has requested that TCP and UDP traffic sourced from or destined to the 174.X.38.0/24 subnet between R3 and R6 be encrypted using the following parameters:
- ISAKMP Authentication Method: RSA-SIG
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
- ESP Encryption: AES-256
- ESP Authentication: HMAC-SHA
- Enable Perfect Forward Secrecy

4 Points

5. IP Services

5.1. The network administrator is concerned about possible SYN flood DoS attacks on servers in VLAN 255 and has requested that R6 be configured to help prevent attacks against these servers.
5.2. Configure R6 to intercept TCP sessions destined for servers in VLAN 255. R6 should reset the TCP session if the connection has not established within 15 seconds.
5.3. R6 should start dropping partial connections once there are more than 1500, and should stop dropping them when the number of partial connections has fallen below 1200.
5.4. The decision as to which partial connections are dropped should be random.

4 Points

5.5. The network administrator has requested that R5 be configured to give access to a web server located in VLAN 52 with the IP address of 192.10.X.100 to hosts in VLAN 53. This web server should be reachable via 204.12.X.100 on TCP ports 80, 443, and 8080.
5.6. Configure R5 to respond to ICMP echo requests sent to the 204.12.X.100 IP address.

2 Points

5.7. Configure NAT on R6 to translate any 150.X.0.0/16 IP addresses using a NAT pool consisting of 192.168.X.50 and 192.168.X.51 when sent across the ATM cloud. Do not translate any other IP addresses.
5.8. Ensure that pings sourced from a 150.X.0.0/16 IP address can ping BB1.
5.9. The use of one static route is permitted for this task.

3 Points

6. General Security

6.1. Ensure that any passwords stored in R3's configuration are not readable in the **show run** output.

1 Point

6.2. Create an object group on the PIX named HOSTS1. Put 10.100.100.100 and 10.100.100.101 in this object group.
6.3. Create an additional object group on the PIX named HOSTS2. Put 10.100.100.200 and 10.100.100.201 in this object group.
6.4. Using a single access-list statement, deny ICMP echo requests on the inside interface from these hosts.

3 Points

6.5. An outside consultant recommended that R5 and R6's interfaces to the BB routers be secured according to RFC 2827.
6.6. Configure R5 and R6's interfaces connecting to the BB routers to conform to this recommendation.

2 Points

6.7. Using CBAC (firewall feature set), configure R5's interface E0/0 to allow inspection of telnet and SMTP sessions to a server located at 192.10.X.50.
6.8. Do not block returning traffic on R5's interface E0/0 to any other host in the 192.10.X.0/24 network.

3 Points

6.9. A new worm has been spreading through the Internet by exploiting a known vulnerability in Microsoft's Internet Information Server (IIS). You have been tasked with configuring R6 to prevent this worm from coming in from BB1. The information you have about this worm from a CERT® Advisory states that the worm sends the following string to the web server on TCP port 80, "ALL YOUR BASE ARE BELONG TO US".

6.10. Configure R6 to drop any HTTP packets containing this string before forwarding the packet out the Fa1/0/0.67 and Fa1/0/0.255 subinterfaces.

3 Points

7. Advanced PIX Firewall

7.1. Configure the PIX to translate the 174.X.0.0/17 IP addresses to 10.0.0.20 through 10.0.0.30, and translate the 174.X.128.0/17 IP addresses to 10.0.0.31 through 10.0.0.50. Translate all other IP address to 10.0.0.51.

2 Points

7.2. To help protect against internal hosts from participating in a DoS attack, configure the PIX to allow for a maximum of 2500 TCP connections and 2000 half open sessions for each of the 10.0.0.21-10.0.0.30 and 10.0.0.31-10.0.0.50 NAT pools.

1 Point

7.3. Since the PIX is configured to allow any internal IP address to be translated, the network administrator is concerned with the possibility of IP spoofing.

7.4. Configure the PIX to drop packets received on the inside interface for which it does not have a valid route to the source for.

2 Points

7.5. The network administrator has installed a multicast server in VLAN 9 and has requested that the PIX be configured to allow a multicast stream destined for the group 226.26.26.26 through the PIX to clients located in VLAN 39.
7.6. The PIX's inside interface should only support an IGMP version that understands the concept of an explicit IGMP leave message.

3 Points

7.7. In the near future a Microsoft Exchange server will be moved from VLAN 9 to VLAN 39 with the IP address of 10.0.0.200.
7.8. The network administrator has requested the PIX be configured to permit access from the outside to this server that will be located in VLAN 39 using 10.0.0.200 on TCP ports 25 and 2525.
7.9. This Microsoft Exchange server will be using ESMTP. Ensure that the PIX will allow for the extended SMTP commands.

3 Points

7.10. A previous co-worker added the following conduit to the PIX:
conduit permit tcp host 10.0.0.75 eq telnet 10.0.0.0 255.255.255.0
7.11. Since conduits will not be support in future PIX OS versions, you have been tasked with converting this conduit to an access-list.
7.12. Use access-list number 150 for this task.

2 Points

8. AAA

8.1. The network administrator has requested that all HTTP sessions through the PIX to any web server located in VLAN 9, except the AAA server, be authenticated by the PIX prior to being granted access.
8.2. The PIX should authenticate these users locally.
8.3. The users will be entering username WEB along with the password CISCO.
8.4. Apply the appropriate configuration to the AAA server for this task.

3 Points

8.5. Configure the PIX to display the following banner to these users connecting via HTTP:

Access to this server is for authorized personnel only

1 Point

8.6. Recently, a contractor made authorized configuration changes to R6. After the changes were completed, the contractor made additional unauthorized configuration changes to R6 so that the contractor's computer would be accessible from the Internet. After recommending to your manager that this contractor be dismissed, your manager has decided to just move this contractor's computer to the outside interface on the PIX (VLAN 9) to help secure the internal network from the contractor.

8.7. Your manager has requested that R6 be configured to authenticate users logging in against the AAA server. The contractor will be logging into R6 using the username TROUBLEMAKER along with the password of CISCO. This user should be automatically placed into privilege level 15.

8.8. Configure the PIX to allow users in VLAN 9 to telnet to R6's Loopback 0 interface via 10.0.0.6.

8.9. Apply the appropriate configuration to the AAA server for this task.

3 Points

8.10. Your manager has additionally requested that double authentication occur whenever the contractor attempts to telnet to R6.

8.11. Configure the PIX to authenticate the contractor locally prior to allowing the telnet session through to R6 using the username TROUBLEMAKER along with the password of CISCO.

8.12. The contractor's IP address is 10.0.0.50. Do not require any other hosts in VLAN 9 to perform this authentication when telneting to R6.

2 Points

8.13. In order to help document the contractor's actions, you have decided to configure accounting with the AAA server as follows:
- Account when an EXEC process is created on R6
- Account for any level 15 commands executed on R6
- Account with the AAA server whenever the contractor authenticates through the PIX
- Account for failed authentication attempts on R6

8.14. Apply the appropriate configuration to the AAA server for this task.

3 Points

9. IDS

Read the access instructions for the IDS Sensor in the introduction for this lab prior to starting this section.

9.1. Your company has installed an IDS sensor to monitor traffic within VLAN 52.
9.2. Only allow management of the IDS sensor via telnet and HTTPS from the AAA server's IP address of 10.0.0.100.
9.3. Configure the PIX to allow the AAA server to communicate with the IDS senor. The AAA server should be able to telnet and browse (HTTPS) to 10.0.0.10 and reach the IDS sensor.

3 Points

9.4. To ensure accurate time, configure the IDS sensor to receive time via NTP from BB1.
9.5. Authenticate the NTP updates using key 1 along with the password of CISCO.

1 Point

9.6. Configure SW1 and SW2 to allow the IDS's sensing interface to monitor traffic from SW1's interface Fa0/5 and SW2's interface Fa0/24.

1 Point

9.7. Due to a recent security vulnerability with certain IOS versions, the network administrator has requested that a custom signature be created according to the following requirements:

- ATOMIC.L3.IP engine: Signature 20001
- IP Protocol Number: 77
- Severity: high
- Event Action: log

2 Points

This page left intentionally blank

IE's Security Workbook Lab 4

Difficulty Rating (10 highest): 7

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	4
ISDN/PPP	12
Routing Protocols	12
VPN	15
IP Services	4
General Security	18
Advanced PIX Firewall	15
AAA	11
IDS	9

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain IE_SEC between SW1 and SW2.
1.2. Authenticate the VTP domain with the password CISCO.

1 Point

1.1. Port Fa0/16 of SW1 connects to an 802.11b wireless access point. Since there are only four hosts which should be accessing your network through this access point, the new corporate policy dictates that traffic from other hosts should not be allowed in this port. The MAC addresses of these four hosts are as follows:

Host	MAC Address
1	0050.7014.8ef0
2	00d0.586e.b710
3	00c0.144e.07bf
4	00d0.341c.7871

1.2. Configure SW1 so that traffic is only allowed in this port if it is sourced from one of the above MAC addresses.
1.3. In the case that other hosts try to access this port, a syslog message should be sent to the server 10.0.0.100.

3 Points

2. ISDN/PPP

2.1. Configure ISDN DDR between R4 and R5 using the physical BRI interfaces.
2.2. Use PPP encapsulation along with PPP multilink on the ISDN connection.
2.3. The second B channel should be brought up by R4 irrespective of the interface load.

3 Points

2.4. The network administrator has requested that the ISDN connection only be brought up whenever R5 loses IP connectivity to R4.
2.5. Once IP connectivity has been restored for at least 120 seconds, R5 should drop the ISDN connection.

2 Points

2.6. Configure R4 to authenticate remote devices inbound and outbound calls using an authentication method that sends the username and password in clear text.
2.7. R4 should authenticate remote devices using TACACS+ with the AAA server. If communication with the AAA server fails, R4 should use its local username and password database. Ensure that the passwords in the username command are stored in the R4's configure using the strongest password encryption supported when using PPP authentication.
2.8. R5 should never authenticate a remote device for inbound or outbound calls.
2.9. Ensure that R4 or R5 always use their hostnames for any authentication process along with the passwords of CISCO.
2.10. Apply the appropriate configuration to the AAA server for this task.

3 Points

2.11. Using the physical interfaces on R1 and R2, configure a Frame Relay connection between them.
2.12. Administrators of your network are concerned about insecure traffic being passed across this Frame Relay cloud. In order to ensure that recipients of your traffic are legitimate, a new corporate policy dictates that the Frame Relay PVC between R1 and R2 must be authenticated with a secure hash algorithm.
2.13. R1 should send the username ROUTER1, along with a hash value that represents the password CISCO for authentication. R1 should authenticate R2 against the AAA server using TACACS+.
2.14. R2 should send the username ROUTER2, along with a hash value that represents the password CISCO for authentication.
2.15. Apply the appropriate configuration to the AAA server for this task.

4 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.3. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.4. Configure RackXPIX as the PIX's hostname.

1 Point

3.5. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.6. The IDS should use R3 as its default gateway.
3.7. Configure RackXIDS as the IDS's hostname.

1 Point

3.8. Configure OSPF area 51 between the VPN3005 and R4.
3.9. Configure OSPF area 51 between the VPN3005 and BB2.
3.10. Configure OSPF area 51 between the PIX and R3.
3.11. The PIX should generate a default into area 51.
3.12. All adjacencies within OSPF area 51 should be authenticated with a secure hash value of the password CISCO with the exception of the adjacency between the VPN3005 and BB2.

3 Points

3.13. Configure an additional OSPF process on the inside interface of the PIX to connect to R1. This interface should run in OSPF area 0.
3.14. Redistribute the area 51 OSPF process in this OSPF process.
3.15. Authenticate all OSPF adjacencies within this area using the clear-text password CISCO.

3 Points

3.16. Recently, a rogue routing device was connected to VLAN 57 which injected false routing information into the network. In order to avoid this problem in the future, your network administrator has requested that you configure SW1 and R5 so that other devices in VLAN 57 cannot hear their OSPF traffic.
3.17. Configure the network to reflect this policy.

3 Points

4. VPN

4.1. The network administrator has requested that the VPN3005 be configured to allow IPSec connections using the Cisco VPN client according to the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: SHA
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-SHA
- Group Name: IEGROUP
- Group Password: CISCO
- Username: IEUSER
- Password: CISCO
- VPN Address Pool: 192.168.255.1-192.168.255.100
- Use NAT Transparent Mode

4.2. When a client connects, their assigned IP address should be injected into OSPF and RIP to ensure connectivity to the clients.

4 Points

4.3. Configure the VPN3005 to authenticate the IEUSER against the AAA server using RADIUS.

4.4. Apply the appropriate configuration to the AAA server for this task.

2 Points

4.5. The network administrator has requested that R5, the PIX, and the VPN3005 be configured to enable a LAN-to-LAN VPN between the 163.X.19.0/24, 192.10.X.0/24, and 10.5.5.0/24 networks using the following parameters:
- ISAKMP Authentication Method: RSA-SIG
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5
- CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll

4.6. The use of one static route on the PIX and VPN3005 is permitted for this task.

4.7. Configure the VPN3005 to deny ICMP echo requests from the 10.5.5.0/24 network to BB2's IP address of 192.10.X.254.

6 Points

4.8. A new corporate policy dictates traffic between the IDS sensor and the management server located in VLAN 4 is encrypted when sent across the Frame Relay cloud. Using IPSec, encrypt traffic only between the hosts 10.3.3.10 and 10.0.0.100 on R3 and R4.
4.9. For accounting purposes, the IP addresses of the IDS sensor and management should not be encapsulation inside of IPSec.

3 Points

5. IP Services

5.1. Configure R2 to drop packets received on its E0/0 interface without a verifiable source IP address.
5.2. Packets with an RFC 1918 source IP address should not be subject to this configuration.
5.3. Do not use policy routing or the **ip access-group** interface level command to accomplish this.

2 Points

5.4. Users have complained about reachability issues to networks learned from BB1. After further investigation, it appears that BB1 does not have full reachability to your internal network.
5.5. Configure R6 to translate IP traffic as it leaves towards BB1 using the 54.X.1.100 IP address.
5.6. Do not translate addresses from the 204.12.X.0/24 network.

2 Points

6. General Security

6.1. The network administrator is concerned with ICMP fragment DoS attacks against internal servers. The network administrator has requested that R2 and R6 deny fragmented ICMP packets inbound from VLAN 263.

6.2. Log any fragmented ICMP packets to the routers' consoles.

2 Points

6.3. After a recent security audit, the auditors noticed that R2 and R6 will inform any requesting host the subnet masks of their connected interfaces. Since this can be used by a potential attacker to help map out the network, the auditors have recommended that R2 and R6 not support this feature on their interfaces connected to VLAN 363.

6.4. Configure R2 and R6 to conform to the auditors' recommendation.

1 Point

6.5. The auditors further recommended that R2 and R6 be configured to display a basic warning message to anyone attempting to login via telnet.

6.6. Configure R2 and R6 to display the following banner to users attempting to login:

This system is for use by authorized users ONLY. Unauthorized use and/or access is to this system is not allowed.

6.7. This banner should not be displayed once the users have successfully logged in.

2 Points

6.8. The network administrator has requested that the IDS not receive ICMP echo requests from any IP address except the management server's IP address of 10.0.0.100.

6.9. Do not apply any configuration to the IDS sensor or R3 to accomplish this.

2 Points

6.10. After recent issues with telnet password security, the network administrator has requested that R1 be configure to only allow SSH connections. Telnet access should be disabled on R1.
6.11. R1 should authenticate users against the AAA server and fail over to local authentication in the event the AAA server is unavailable.
6.12. Create a user in the AAA server named SSH along with the password of CISCO.
6.13. Apply the appropriate configuration to the AAA server for this task.

3 Points

6.14. Configure R5 to drop all telnet traffic received inbound on its interface E0/1.
6.15. Do not apply an access-list to an interface for this task.

2 Points

6.16. Recently, it was discovered that hosts behind BB3 were attempting to gain access to servers located across the ATM cloud. The network administrator has requested that R6 be hardened according the following requirements.

- Treat interface Fa1/0/0 as the outside interface and interface ATM0/0/0.1 as the inside interface
- Using CBAC (firewall feature set), permit returning TCP/UDP sessions and ICMP packets that were initiated from R6 itself or from behind R6 inbound on the outside interface
- Permit any traffic sourced from the 163.X.0.0/16 and 150.X.0.0/16 networks inbound
- Permit users across the ATM cloud to receive traceroute replies to destinations in the 204.12.X.0/24 network only
- UDP port 53 sessions through R6 should timeout after twice the default value
- Without using an access-list, log to the console all TCP packets, including the number of bytes
- Permit GRE traffic between BB3's 204.12.X.254 and BB1's 54.X.1.254 IP addresses
- Log and drop any ICMP echo requests not sourced from the 163.X.0.0/16 and 150.X.0.0/16 networks inbound
- Permit all other ICMP traffic inbound
- Permit necessary routing protocol traffic inbound
- Deny all other traffic

4 Points

6.17. After securing R6's interface Fa1/0/0, the administrator of BB3 has complained that servers behind BB3 are under ICMP DoS attack. The attack appears to be coming from behind R6 across the ATM cloud.
6.18. To help solve this issue, configure R6 to allow for only 128kbps of ICMP traffic inbound from the ATM cloud.
6.19. Do not use the **rate-limit** command for this task.

2 Points

7. Advanced PIX Firewall

7.1. Configure the PIX to translate any inside IP address to the outside interface's IP address.
7.2. Allow for a maximum of 5000 TCP connections and 2500 embryonic connection.

2 Points

7.3. Configure the PIX to log all possible syslog messages to the syslog server at 10.0.0.100.
7.4. The syslog messages should be sent using PIX syslog facility 19.

2 Points

7.5. The network administrator has requested that the syslog messages be timestamped. To ensure accurate timestamps, configure the PIX to receive time via NTP from BB1 and BB3.
7.6. Authenticate the NTP updates using key 1 along with the password of CISCO.
7.7. If BB1 and BB3 have the same stratum, the PIX should prefer updates from BB3 over BB1.

3 Points

7.8. The network administrator has requested that the PIX be configured to allow outside SMTP access to a Microsoft Exchange server with the IP address of 163.X.19.75. The SMTP server should be reachable to the outside users via the IP address 163.X.39.75.

2 Points

7.9. After enabling access to the Microsoft Exchange server, you have noticed that users behind the PIX can send mail without problems, but users on the outside can not send mail through the PIX to the server.
7.10. After looking over the PIX configuration and verifying the translation, you decide to test the SMTP connection from the outside. When telneting to the SMTP server on port 25 and issuing the EHLO command, you receive a "500 unrecognized command" message. After looking over the logs on the Exchange server itself, you notice that your connection was never connected to the server and the PIX must have generated the "500 unrecognized command" message.
7.11. Configure to PIX to not generate the "500 unrecognized command" message for the EHLO SMTP command and, in turn, allow users outside of the PIX the ability to send e-mail.

3 Points

7.12. After a recent DoS attack, a server with the IP address of 163.X.39.175 that was previously located in VLAN 39 has been moved to VLAN 19. Due to proprietary software applications on the server that are licensed to the server's IP address of 163.X.39.175, the server's IP address could not be changed when moved to VLAN 19.
7.13. Configure the PIX to allow hosts on the outside to reach this server via HTTP and FTP.
7.14. To assist with troubleshooting, allow hosts on the outside to ping this server's IP address.

3 Points

8. AAA

8.1. The network administrator has requested telnet sessions be permitted from the 163.X.19.0/24 subnet the PIX.
8.2. Authenticate these telnet sessions against the AAA server.
8.3. Users will authenticate with the username USER1 along with the password of CISCO.
8.4. When a user telnets to the PIX they should receive the following prompt: *Enter Your Authentication Credentials*
8.5. If the user fails authentication, they should receive the following message: *Call the help desk at 877-224-8987 for assistance if you need access to this device*
8.6. Apply the appropriate configuration to the AAA server for this task.

3 Points

8.7. The network administrator has requested SSH sessions be permitted from any address on the inside interface of the PIX.
8.8. Use the local username/password database on the PIX to authenticate these users.
8.9. Create a user named SSHUSER along with the password of CISCO for this task.

2 Points

8.10. The network administrator would like to provide access to an internal web server with the IP address of 163.X.19.100 to users in the 204.12.X.0/24 network. The network administrator would like R2 to authenticate these users against the AAA server prior to them being given access to the web server. The network administrator has stated that lock-and-key security should not be used.
8.11. R2 should use TACACS+ with the AAA server for authenticating these sessions.
8.12. Require the users to enter the username of WEB along with the password of CISCO.
8.13. Apply the appropriate configuration to the AAA server for this task.

4 Points

8.14. In order to ease troubleshooting related to these users accessing the web server, permit them to ping the web server once they have authenticated.

2 Points

9. IDS

Read the access instructions for the IDS Sensor in the introduction for this lab prior to starting this section.

9.1. An IDS sensor has been installed to monitor network traffic destined to your company's internal servers through the PIX.
9.2. Only allow management of the IDS sensor via HTTP and HTTPS from the AAA server's IP address of 10.0.0.100.
9.3. Configure the IDS Event Viewer on the AAA server to manage the IDS sensor.
9.4. Span VLAN 39 traffic to the IDS sensor's sensing interface.

3 Points

9.5. Configure the IDS sensor to shun on the PIX's outside interface. The IDS will use SSH for communication with the PIX.
9.6. Configure the PIX to allow the IDS sensor to connect using SSH to its outside interface.
9.7. Do not use the **username** command on the PIX or authenticate the SSH session against the AAA server for this task.

3 Points

9.8. Enable all General Windows and Windows NT/2K/XP signatures on the IDS sensor.
9.9. Change the General Windows signature 3202 from severity medium to high.

1 Point

9.10. The network administrator has requested that the IDS capabilities of R2 be enabled to help guard against SPAM e-mail. The network administrator would like R2 to alarm whenever it receives an email message on its interface E0/0 and there are more than 100 recipients in the message.
9.11. The alarms should be sent to 10.0.0.100.

2 Points

IE's Security Workbook Lab 5

Difficulty Rating (10 highest): 7

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	8
ISDN/PPP	6
Routing Protocols	10
VPN	15
IP Services	4
General Security	22
Advanced PIX Firewall	10
AAA	10
IDS	15

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain CISCO on SW1 and SW2.
1.2. Authenticate VTP between SW1 and SW2 using the password CISCO.

1 Point

1.3. After a recent issue with a user installing a switch on their desk and connecting unauthorized computer systems to the network, your manager has asked that the user's port (SW1 Fa0/21) be configured to only allow the corporate desktop PC's MAC address to connect. After informing the manager that the user could easily workaround the restriction, you recommended that a better solution would be to implement 802.1x authentication. After hearing your case for 802.1x, you manager has insisted on using a simpler solution even though it has many flaws.
1.4. Configure SW1 to only allow this one MAC address of 1234.5678.abcd to connect to SW1 Fa0/21. If another MAC address connects to this port, the port's state should change to error-disable.
1.5. After the port is disabled SW1 should check every one minute to see if the correct host is connected to the port.

2 Points

1.6. A notebook computer that contains sensitive company marketing data was recently found left unsecured in the company's meeting room. Since this notebook is not permitted to be connected in public areas, your manager has requested you to configure the network so that this computer is only allowed to connect to port Fa0/22 of SW1.
1.7. The computer's MAC address is dcba.8765.4321.
1.8. Configure the network to reflect this policy.

2 Points

1.9. After a recent security audit, it was found that R1 and the PIX contained ARP entries for computers that were not authorized to be connected in VLAN 19. Since this portion of the network is considered a DMZ, only R1 and the PIX should be allowed to communicate in this VLAN. In order to make it harder for someone to just plug a computer into VLAN 19 and communicate with the PIX or R1, you have decided to disable ARP within the VLAN. After researching a filtering technique, you have determined that IP ARP uses the Ether-Type value 0x806.
1.10. Configure the network to reflect this policy.

3 Points

2. ISDN/PPP

2.1. Using PPP encapsulation, configure legacy ISDN DDR between R4 and R5.

1 Point

2.2. Configure R4 to call R5 if it loses connectivity to R5's Loopback0 interface via R3.
2.3. R4 or R5 should never be allowed to call each other based on interesting traffic.
2.4. R5 should never drop a call due to the lack of interesting traffic.

2 Points

2.5. To ensure proper routing table convergence and rerouting of traffic flows, configure R4 to maintain the call to R5 for three minutes upon relearning the route to R5's Loopback via R3.

1 Point

2.6. Configure R4 to request authentication of R5 using CHAP. R5 should reject CHAP authentication and offer PAP authentication as an alternative. R4 should not accept this offer to use PAP, but continue the PPP negotiation process without performing authentication. In the end, no authentication should take place but the ISDN call should still connect.
2.7. Use local AAA authentication for this task.

2 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. The VPN3005 should use R2 as its default gateway.
3.3. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.4. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.5. The IDS should use the PIX as its default gateway.
3.6. Configure RackXIDS as the IDS's hostname.

1 Point

3.7. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.8. Create an OSPF process on the outside interface of the PIX using process-id 1. The PIX should generate a default into OSPF.
3.9. Configure RackXPIX as the PIX's hostname.

1 Point

3.10. Perform basic authentication for all OSPF adjacencies across the Frame Relay network between R2, R3, R4, and R5.
3.11. Use the **area 2345 authentication** command under the OSPF process to accomplish this task.

1 Point

3.12. Perform MD5 authentication for the OSPF adjacency between R4 and R5 across the ISDN link.

1 Point

3.13. Authenticate all OSPF adjacencies within area 0, including the virtual link between R1 and R3, using MD5 authentication.
3.14. Do not use the **area 13 virtual-link 150.X.1.1 authentication message-digest** command on R3, but use the **area 13 virtual-link 150.X.3.3 authentication message-digest** command on R1 to accomplish this task.
3.15. Do not alter the OSPF router ID's to accomplish this task.

1 Point

3.16. Configure an additional OSPF process on the PIX using process-id 2.
3.17. Configure OSPF area 51 between R6, the PIX, and BB2.
3.18. Ensure that R6 and BB2 can use the PIX to reach the rest of the network.

1 Point

3.19. Configure a BGP peering session between R1 and R6 through the PIX.
3.20. Authenticate this BGP peering session using the password CISCO.

3 Points

4. VPN

4.1. Your company has decided to allow access to a server located in VLAN 8 for users behind BB1. Users behind BB1 should be able to reach the server by the 54.X.1.100 IP address for both FTP and HTTP.

4.2. Encrypt this traffic between R6's interface Fa1/0/0 and R3's interface E0/1 using the following parameters:

- ISAKMP Authentication Method: RSA-SIG
- ISAKMP Hash: MD5
- CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
- ESP Encryption: 3DES

4.3. Users should also be able to ping this server using the 54.X.1.100 IP address, but the network administrator has asked that ICMP echo and echo-replies not be encrypted.

4 Points

4.4. In the future, a new Ethernet interface will be added to R3, R4, and R5. These new interfaces will be addressed using 192.168.3.0/24, 192.168.4.0/24, and 192.168.5.0/24 respectively. Traffic between these new networks will be kept separate from the rest of the network by using GRE tunnels, and will be encrypted by using IPSec.

4.5. In order to test this design before the new interfaces are actually installed, the network administrator has requested that each router be temporarily configured with a Loopack2 interface using the same addresses that will be assigned to the Ethernet interfaces in the future. Fully meshed GRE tunnels should be configured between the routers using unnumbered IP addresses based on their Loopback2 interfaces.

4.6. Enable EIGRP routing for these new Loopbacks using AS 1. These routes should not be redistributed into any other routing protocol.

4.7. The GRE tunnel between R3 and R4 should be encrypted using the following parameters:

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ISAKMP Lifetime: 12 hours
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5
- Perfect Forward Secrecy: Group 2

4.8. This configuration should use the minimal number of **crypto map** commands needed.

3 Points

4.9. Encrypt the remaining GRE tunnels between R3, R4, and R5 using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: AES 256
- ESP Authentication: HMAC-SHA

4.10. This configuration should continue to function in the event that R4 and R5 are using the ISDN connection for communication.

4 Points

4.11. The network administrator would like to use Cisco's VPN client software to access the 192.10.X.0/24 network while away from the office.

4.12. Configure the PIX to allow the VPN client to connect using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-SHA
- Group Name: ADMINGROUP
- Group Password: CISCO
- Username: ADMIN
- User Password: CISCO
- IP Address Pool: 192.168.0.0/24
- Idle Timeout: 600 Seconds
- Allow for split tunneling to destinations outside of the 192.10.X.0/24 and 150.X.6.0/24 networks

4.13. Use local AAA authentication to authenticate the ADMIN user.

4 Points

5. IP Services

5.1. The network administrator has brought to your attention that BB1 and BB3 are not able to reach certain IP addresses within your network. After requesting that R4 and R6 be configured to advertise the 10.0.0.0/8, 162.X.0.0/16, and the 150.X.0.0/16 networks to BB1 and BB3 via BGP, the network administrator has stated that only the 162.X.0.0/16 and the 150.X.0.0/16 networks will be advertised via BGP to BB1 and BB3.

5.2. Advertise these networks via BGP to BB1 and BB3.

5.3. Ensure that IP addresses in the 10.0.0.0/8 network can still reach BB1 and BB3.

2 Points

5.4. After a recent security audit it was found that anyone who knew the names of the router configuration files on the TFTP server were able to download them using a TFTP client application. Since this is not acceptable, you have decided to implement a more secure solution for backing up router configurations.

5.5. An FTP server with the IP address of 10.0.0.100 has been set up to store R4's configuration files. Configure R4 to use anonymous FTP to connect to this server.

5.6. The FTP server will only allow connections from the 150.X.4.4 IP address.

2 Points

6. General Security

6.1. Your network administrator has requested that the PIX be configured to allow SSH connections from the inside network of 192.10.X.0/24, and from the 162.X.55.0/24 network on the outside interface.

6.2. Telnet should be permitted on the inside interface only from the management station's IP address of 192.10.X.150.

2 Points

6.3. After recent unauthorized access to a server running a proprietary application with the IP address of 162.X.55.100, the network manager has requested that R5 be configured to authenticate users accessing this server prior to allowing them to connect using their client software.
6.4. The users will need to log in using the username APP and the password CISCO. R5 should authenticate these users via TACACS+ using the AAA server located in VLAN 8.
6.5. Upon successful authentication, the users should be allowed access to the server using only destination TCP port 4550.
6.6. For ease of use for the end users, the developer of the proprietary application has altered the client's software to connect to R5 using TCP port 7005 and automatically send the username APP along with the password CISCO prior to attempting to connect to the server itself.
6.7. Configure R5 and the AAA server to support these requirements.
6.8. Do not use authentication proxy to accomplish this task.

4 Points

6.9. After a recent security issues related to servers located in VLAN 4, a new corporate policy dictates that R4 be hardened according to the following requirements.

- Treat R4's E0/0 interface as the outside interface and all other interfaces as inside
- Disable CDP on the outside interface
- Drop packets that are source routed
- Without using CBAC, permit TCP or UDP sessions that were initiated from behind R4 inbound from the outside
- Allow access to a server located at 10.4.4.100
- Outside users should be able to connect to the 10.4.4.100 server using IP address 204.12.X.100
- Using only one access-list entry, allow connections to all TCP ports except port 25
- If packets are denied via an access-list, do not notify the source that the packet was dropped
- Permit any necessary routing protocol traffic
- Deny all other traffic

5 Points

6.10. The network administrator would like all ICMP echo requests that are destined for the PIX to be filtered within VLAN 19.
6.11. Since an outbound filter on R1 will not affect traffic sourced by R1 itself, do not apply this filtering policy to R1 to accomplish this task.

3 Points

6.12. A new corporate policy dictates that anyone connected to R1 should not be able to telnet to any other device from R1.
6.13. Do not apply an access-list to any interface to accomplish this task.

2 Points

6.14. After recent reports from your company's Human Resources department showed that users are spending nearly 25% of their time browsing the Internet, your manager has requested that R4 and R6's connections to their respective BB routers be configured to restrict access to outside web servers during work hours.
6.15. Configure R4 and R6 to filter all outbound TCP port 80 traffic forward the BB routers between the hours of 8am and 5pm GMT Monday thru Friday.
6.16. To ensure accurate filtering, configure R4 and R6 to receive time via NTP from their respective BB routers.
6.17. R4 and R6 should validate the BB routers for NTP using key 1 along with the password CISCO.

4 Points

6.18. After implementing the new filtering policy for outbound HTTP traffic, users have complained that they are unable to reach web servers needed to perform their jobs. In response to this you have decided to allow access to the web servers at 50.1.201.4, 50.0.200.5, and 51.1.200.4.during work hours (8am to 5pm GMT Monday thru Friday).
6.19. Use only one access-list entry to accomplish this task.

2 Points

7. Advanced PIX Firewall

7.1. Configure the PIX to provide PAT translations for users on the inside network of 192.10.X.0/24 accessing resources outside of the PIX using its interface IP address of 162.X.19.9.
7.2. Users from any other inside IP addresses should use the 162.X.19.128/26 address space for NAT translations.

2 Points

7.3. Filter traffic sourced from hosts with the IP addresses of 192.10.X.120, 192.10.X.130, and 192.10.X.140 inbound on the inside interface of the PIX.
7.4. Ensure that future hosts can be added to this filter without the need to add additional access-list statements.

2 Points

7.5. The network administrator has requested that the PIX be configured to assign IP addresses dynamically to users in VLAN 100 using the following parameters:

- Address Pool: 192.10.X.64/26
- DNS servers: 192.10.X.200 and 192.10.X.201
- Domain: internetworkexpert.com
- Ping IP addresses in the address pool and allow up to one second for a reply before allocating a particular IP address from the address pool

2 Points

7.6. Users behind the PIX have reported that they are unable to ping or traceroute to IP addresses on the outside of the PIX.
7.7. Configure the PIX to allow the users to ping and traceroute but not allow other ICMP traffic through the PIX.
7.8. Ensure that future ICMP traffic can be added to these filters without the need to add additional access-list statements.

1 Point

7.9. The network administrator has requested that the PIX be configured to log only emergency level messages to the console.
7.10. Users connected to the PIX remotely via SSH should receive error level messages and below.
7.11. Debug level and below should be logged to a syslog server located at IP address 192.10.X.175.
7.12. Timestamp all syslog messages.
7.13. Ensure accurate time by having the PIX receive time via NTP from BB2. Authenticate NTP from BB2 using key 1 along with the password CISCO.

3 Points

8. AAA

8.1. After a recent network outage that involved unauthorized changes made during the workday on R1, a new corporate policy dictates that R1 authorize and account for all level 15 commands.
8.2. R1 should be configured to authenticate a user named ADMIN along with the password CISCO with the AAA server. If the AAA server is not available, the user should be authenticated against the local username/password database. R1 should use RADIUS with the AAA server for this task.
8.3. Level 15 command authorization for the ADMIN user should be handled locally on R1.
8.4. Account for all level 15 commands with the AAA server.
8.5. Apply the appropriate configuration to the AAA server for this task.

3 Points

8.6. Configure R3 to authenticate telnet sessions against the AAA server using TACACS+.
8.7. R3 should source the TACACS+ connections off its most reliable interface.
8.8. Create a user in the AAA server named USER1 along with the password CISCO.
8.9. USER1 should be placed in privilege level 7 while USER2 should be placed in privilege level 0.
8.10. Allow USER1 access to the **snmp-server** configuration commands in the global configuration.
8.11. Apply the appropriate configuration to the AAA server for this task.

2 Points

8.12. Allow USER1 access to the **debug ip rip** and **undebug all** commands on R3.
8.13. Authorize and account for these commands with the AAA server.
8.14. Apply the appropriate configuration to the AAA server for this task.

2 Points

8.15. Configure R4 to allow a user named NOC with the password of CISCO to perform the following tasks:
- View the router's hostname and interfaces in the running configuration.
- Allow the NOC user to perform a **shutdown** and **no shutdown** on any interface.
- Deny access to change the router's hostname.

8.16. Authentication for the user NOC should be preformed against the AAA server.
8.17. Apply the appropriate configuration to the AAA server for this task.

3 Points

9. IDS

Read the access instructions for the IDS Sensor in the introduction for this lab prior to starting this section.

9.1. An IDS sensor has been installed to monitor traffic within VLAN 211.
9.2. Allow management of the IDS sensor via HTTPS from IP addresses in the 192.10.X.0/24 and 10.0.0.0/24 networks.
9.3. The AAA server should be able to reach the IDS's 192.10.X.10 IP address via 162.X.19.10 through the PIX.

3 Points

9.4. Configure SW1 and SW2 to span traffic from VLAN 211 to the IDS sensor's monitoring interface.

1 Point

9.5. Configure the IDS to shun inbound on R2's interface E0/0.
9.6. The IDS sensor should communicate with R2 using telnet.

2 Points

9.7. Configure the IDS sensor to log and shun for the ICMP echo request signature.

2 Points

9.8. The network administrator has requested that the PIX be configured for intrusion detection support according to the following requirements:

- Disable the IP Fragments Overlap and IP Fragment Attack signatures
- Alarm on informational signatures on the inside and outside interfaces
- Alarm, drop, reset on attack signatures on the outside interface
- Log the IDS alarms to 10.0.0.100

3 Points

9.9. After recent security issues the network administrator has requested that R3 be configured to perform basic IDS functions.
9.10. Configure R3 to meet the following parameters:

- Audit packets that are received inbound on interface E0/1
- Alarm and drop traffic that triggers an attack alarm
- The attack alarms should be sent to a NetRanger Director located in VLAN 100
- The NetRanger Director's IP address inside of the PIX is 192.10.X.222, and should be accessible from R4 through the PIX using its 192.10.X.222 IP address
- Use HostID 5000 and ORGID 1000 for the Post Office Parameters when communicating with the NetRanger Director
- Alarm and Drop traffic that triggers an informational signature
- Disable signature 3106
- Disable signature 2004 from hosts in the 204.12.X.0/24 network
- Ensure the AAA server can still communicate with devices in the network when this configuration is applied

4 Points

This page left intentionally blank

IE's Security Workbook Lab 6

Difficulty Rating (10 highest): 7

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	5
ISDN/PPP	6
Routing Protocols	13
VPN	19
IP Services	4
General Security	26
Advanced PIX Firewall	8
AAA	15
IDS	4

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain INTERNETWORKEXPERT between SW1 and SW2.
1.2. Authenticate the VTP domain with the password CISCO.

1 Point

1.3. Your company has set up three computers in the company's public meeting room to accommodate sales engineers with presentations. In order to restrict access to the corporate network, your manager has requested that a maximum of three hosts be permitted to communicate on SW1's interface Fa0/7.
1.4. Configure SW1 to meet these requirements.

2 Points

1.5. Recently, it has come to your attention that a sales engineer has circumvented the three-host limitation in the meeting room by connecting a router to one of the RJ-45 jacks in the meeting room. The network administrator has requested that the SW1 be configured in such a way as to stop this router from communicating if it is connected to interface Fa0/7.
1.6. The router's MAC address is 1234.4568.90ab.
1.7. This configuration should not affect the other hosts in the meeting room.

2 Points

2. ISDN/PPP

2.1. Configure legacy ISDN DDR between R4 and R5.

1 Point

2.2. The network administrator has requested that the ISDN link between R4 and R5 be treated as a backup connection. The network administrator would like R5 to call R4 whenever it loses IP connectivity to R4 via R2.
2.3. Ensure that R5 determines when the call is placed and when the call is dropped.
2.4. R4 should only drop a call in the event of an authentication failure or a call from a phone number other than R5 number.

3 Points

2.5. Your company has decided to migrate away from Challenge Handshake Authentication Protocol (CHAP) and implement the newer Extensible Authentication Protocol (EAP). Management has requested for R4 and R5's CHAP configuration be converted over to EAP.
2.6. R4 and R5's configuration related to CHAP is as follows:

```
R4:
username ROUTER5 password CISCO
!
interface BRI0/0
 encapsulation ppp
 ppp authentication chap callin
 ppp chap hostname ROUTER4

R5:
username ROUTER4 password CISCO
!
interface BRI0/0
 encapsulation ppp
 ppp authentication chap
 ppp chap hostname ROUTER5
```

2 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. The VPN3005 should use R4 as its default gateway.
3.3. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.4. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.5. The IDS should use the VPN3005 as its default gateway.
3.6. Configure RackXIDS as the IDS's hostname.

1 Point

3.7. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.8. Configure RackXPIX as the PIX's hostname.

1 Point

3.9. Authenticate the OSPF adjacency between R3 and R4 using an MD5 hash value of the password CISCO.
3.10. Use the **area 0 authentication message-digest** router configuration command for this task.

2 Points

3.11. Configure plain-text authentication using the password of CISCO for the OSPF adjacency between R2 and R3.

1 Point

3.12. Configure OSPF area 279 on the outside interface of the PIX using process ID 279.
3.13. Authenticate the OSPF adjacency with SW1 using plain text authentication and the password CISCO.

2 Points

3.14. Configure OSPF area 0 on the inside interface of the PIX using process ID 1.
3.15. Authenticate the OSPF adjacencies between the PIX, the AAA server, and R1 using plain text authentication. Use the password of CISCO for this task.
3.16. *The AAA server is preconfigured for this task.*

3 Points

3.17. Configure the PIX to advertise the OSPF 279 process's routes to the AAA Server and R1.
3.18. Configure the PIX to translate the 10.0.0.0/24 subnet using the PIX's outside interface's IP address.
3.19. Ensure that R1 can ping SW1's Loopback 0 address.

2 Points

4. VPN

4.1. The network administrator has requested that even though VLAN 4 and 5 are using the same IP subnets, R4 and R5 should be configured to allow the users in the two VLANs to communicate with each other.
4.2. Users in VLAN 4 should appear to be in the 10.4.4.0/24 subnet to users in VLAN 5, while users in VLAN 5 should appear in the 10.5.5.0/24 subnet to users in VLAN 4.
4.3. Encrypt the traffic between VLAN 4 and VLAN 5 with the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5

4.4. The configuration should continue to function when the ISDN link is active.
4.5. A static route on R4 and R5 is permitted for this task.

6 Points

4.6. A new corporate policy dictates that R4, R5, and R6 be configured to encrypt IP traffic between users in VLANs 4, 5, and 6.
4.7. Encrypt this traffic using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: SHA
- ISAKMP Encryption: DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-SHA

4.8. Ensure that the Diffie-Hellman key exchange process uses the strongest key size supported.
4.9. You are permitted to use static routes to accomplish this.

4 Points

4.10. The network administrator has requested that the PIX and VPN 3005 be configured to allow the communication between VLAN 19 and VLAN 118.
4.11. Encrypt all IP traffic between these two networks using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5

5 Points

4.12. Your manager has informed you that users in VLAN 6 will need to access the IDS sensor's management interface. Your manager requests that the IP traffic between VLAN 6 and VLAN 118 be encrypted, but this encryption should use the least amount of processing cycles on R6's CPU.
4.13. Configure the VPN3005 and R6 to meet these requirements.

4 Points

5. IP Services

5.1. Recently, a server with the IP address of 204.12.X.100 located in VLAN 363 was moved. Since the network administrator did not update the DNS records accordingly, you have been tasked to ensure that users in VLAN 4 and 5 can still access this server via its new IP address of 112.0.0.1 even though its DNS name still resolves to 204.12.X.100.
5.2. Configure R6 to meet these requirements.

2 Points

5.3. The network administrator has requested that R6 be configured to receive time from BB1 via NTP.
5.4. Configure R6 to authenticate the NTP updates from BB1 using key 1 along with the password CISCO.

2 Points

6. General Security

6.1. Configure the PIX to only allow SSH connections from the following IP addresses:

- 191.X.23.3
- 191.X.34.4
- 191.X.45.4

1 Point

6.2. Recently, the administrator of BB2 was troubleshooting a problem and noticed that SW1 was connecting BB2 to R3. After asking your network administrator questions about the switch, you have decided that switches in your network should not announce themselves to BB2 or BB3 anymore.

6.3. Make the appropriate configuration changes to ensure that SW1 and SW2 do not announce their presence to the BB routers but continue to do so to your internal devices.

2 Points

6.4. After recent security issues related to users outside of your network accessing internal resources, a new corporate policy dictates that R3 be hardened according to the following requirements:

- Treat E0/1 interface as the outside interface and all other interfaces as inside interfaces
- Disable CDP on the outside interface
- Drop packets that are source routed
- Disable NTP on the outside interface
- Disable BOOTP and DHCP
- Using CBAC (firewall feature set), permit returning TCP, UDP or ICMP sessions that were initiated from behind R3 should be permitted in the outside interface
- Deny traffic sourced from any RFC 1918 address in the outside interface unless the traffic was initiated by a device behind R3
- Deny traffic sourced from the 191.X.0.0/16 network inbound on the outside interface
- If packets are denied by an access-list, do not notify the source that the packet was dropped
- Permit TCP connections to a server located in VLAN 79 with the IP address of 191.X.79.100
- Translate traffic sourced from the 191.X.55.0/24 network to 204.12.X.30 when sent out of the outside interface
- Permit any necessary routing protocol traffic
- Deny all other traffic

6.5. Ensure that the IPSec tunnels between R4, R5, R6 and the VPN3005 and IP routing protocol traffic are not affected by this configuration.

4 Points

6.6. After implementing the new security policy on R3, users in VLAN 6 have complained that they are unable to access a server located in VLAN 79 with the IP address of 191.X.79.100.

6.7. After discussing the situation with your manager, you requested to allow hosts with source IP addresses 10.6.6.0/24 network to be received on R3's interface E0/1 to enable access to the server in VLAN 6. However, your manager has denied this request to relax the security policy.

6.8. Without making changes to R3's security policy, allow the VLAN 6 users to connect to the 191.X.79.100 server.

3 Points

6.9. Your manager has informed you that users within your network are playing JAVA web-based games. You manager has requested that R3 be configured to deny users from downloading JAVA applets from any HTTP servers except servers located in VLAN 363.

2 Points

6.10. After implementing the changes to deny the JAVA applets, it has come to your attention that some users are still able to play these JAVA-based games from servers not located in VLAN 363. After further investigation, you have discovered that R3 is allowing the users to continue to download JAVA applets when the users are connected to an HTTP server that is running on a non-standard TCP port.

6.11. Allow the users to continue to connect to HTTP servers on the non-standard ports of 8080 and 10080 but deny the downloading of JAVA applets from servers using these TCP ports.

3 Points

6.12. As soon as you thought the JAVA filtering was finished, your manager noticed a user was still able to play the JAVA web-based games. After further investigation, you have determined that the users are connecting to a server with the IP address of 113.0.0.1 using the FTP port of 21.

6.13. Configure R3 to permit TCP connections to the server on port 21 but deny the downloading of JAVA applets.

2 Points

6.14. After a recent security audit, the auditors noticed that the PIX is responding to ICMP echo-requests on its outside interface. Management has asked that the PIX silently discard any ICMP echo-requests destined for its outside interface.

2 Points

6.15. The network administrator has recently reported that a web server located in VLAN 6 with the IP address of 10.6.6.100 was the subject of a TCP SYN flood DoS attack. Against your recommendation, due to the limited processing power of R6's CPU and memory, the network administrator has requested that R6 be configured to intercept and validate HTTP connections made to that particular server.

2 Points

6.16. Configure R6 to drop idle TCP sessions to the server (10.6.6.100) after 360 minutes of inactivity.

1 Point

6.17. After heated negotiations with the administrator of BB1 concerning allowing users access to a web server located in VLAN 363 across the ATM cloud, you have agreed to allow access to the server with the IP address of 204.12.X.150 until 00:01 Jan 1, 2007 UTC.
6.18. At that time, access to the server should be denied to the users across the ATM cloud.
6.19. Configure R6 to meet these requirements.

4 Points

7. Advanced PIX Firewall

9.14. Configure the PIX to translate any inside host's IP address to the outside interface's IP address.
9.15. Provide PAT translations for all outbound HTTP connections using 191.X.79.200.

1 Point

7.1. Redirect TCP connections destined for 191.X.79.50 port 15023 and 191.X.79.51 port 15023 to R1 port 23.
7.2. Use only one access-list statement for this task.

1 Point

7.3. Redirect TCP connections destined for 191.X.79.50 port 15123 to R1 port 23.
7.4. Do not add any additional access-list entries for this task.

1 Point

7.5. The network administrator has requested that users on the inside of the PIX be restricted to only being connected to one server in VLAN 363 with the IP address of 204.12.X.175.
7.6. Permit access to this server on TCP port 80 and deny access to all other IP addresses in VLAN 363.

1 Point

7.7. Users behind the PIX have reported that they are unable to traceroute to IP addresses on the outside of the PIX. The network administrator requested that the users only be permitted to receive traceroute replies from IP addresses in the 191.X.0.0/16 network.

2 Points

7.8. Configure the PIX to send all possible syslog messages to 10.0.0.100.
7.9. Timestamp these syslog messages.
7.10. To ensure accurate timestamps of the syslog messages, configure the PIX to receive time via NTP from BB2. The PIX should authenticate the NTP updates from BB2 using key 1 along with the password CISCO.

2 Points

8. AAA

8.1. A new corporate policy dictates that all telnet connections through the PIX (inside to outside) must be authenticated by the PIX prior to allowing access.
8.2. The PIX should authenticate these users against the AAA server.
8.3. The users will be authenticating with the username PIX and the password CISCO.
8.4. Apply the appropriate configuration to the AAA server for this task.

4 Points

8.5. The new policy also dictates that the PIX perform accounting for these telnet sessions.
8.6. Configure the PIX to account for these telnet sessions with the AAA server.

2 Points

8.7. Authenticate users telneting into R4 against the AAA server.
8.8. This communication with the AAA server should continue to function in the event that R4's Frame Relay connection is down. Do not base this communication off of R4's Loopback 0 interface.
8.9. Users will be authenticating with the username R4 and the password CISCO.
8.10. Do not configure this authentication as the default authentication method on R4.
8.11. Configure the PIX to permit R4 access to the AAA server via TACACS+.
8.12. Apply the appropriate configuration to the AAA server for this task.

4 Points

8.13. If R4 fails to communicate with the AAA server, users telneting in should be authenticated via the local username/password database.
8.14. Only allow a user named ADMIN with the password CISCO to authenticate locally.
8.15. This user should be placed in the highest privilege level upon login.

2 Points

8.16. Configure PPP encapsulation on the serial connection between R2 and R3.
8.17. Authenticate this connection using CHAP authentication.
8.18. R2 should send the username ROUTER2 and R3 should send the username ROUTER3. Both should use the password CISCO.
8.19. R3 should authenticate R2 using its local username/password database.
8.20. R2 should authenticate R3 against the AAA server.
8.21. Apply the appropriate configuration to the AAA server for this task.

3 Point

9. IDS

Read the access instructions for the IDS Sensor in the introduction for this lab prior to starting this section.

9.1. An IDS sensor has been installed to monitor traffic between SW1 and the PIX.
9.2. Allow management of the IDS sensor via HTTPS from IP addresses in the 10.0.0.0/24 network.
9.3. Configure the IDS sensor to allow SW2 to connect via SSH for management purposes.
9.4. Span VLAN 79 traffic to the IDS sensor's monitoring interface.

3 Points

9.5. Configure the IDS Event Viewer to manage the IDS sensor.
9.6. Disable informational and low alarm severity levels.
9.7. Alter the default view to filter traffic sourced from the 191.X.79.0/24 subnet.

1 Point

IE's Security Workbook Lab 7

Difficulty Rating (10 highest): 8

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	5
ISDN/PPP	8
Routing Protocols	13
VPN	22
IP Services	15
General Security	16
Advanced PIX Firewall	4
AAA	4
IDS	13

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain IE_SEC on SW1 and SW2.
1.2. SW1 should not act upon VTP updates from SW2.
1.3. Do not use VTP transparent mode for this task.

2 Points

1.4. The network administrator has informed you that two new servers will be connected to SW2. These servers will be installed in VLAN 8. The first server will be connected to SW2's port Fa0/20 and the second to SW2's port Fa0/21. For security reasons the network administrator has asked the SW2 be configured to not allow these two servers to communicate with each other.
1.5. Do not use an access-list to accomplish this task.

2 Points

1.6. For additional security configure SW1 to not forward unicast frames with an unknown destination MAC addresses out port Fa0/20.

1 Point

2. ISDN/PPP

2.1. Configure legacy ISDN DDR between R4 and R5.

1 Point

2.2. Configure R5's BRI0/0 interface to be in standby mode unless its Frame Relay subinterface to R4 is down.
2.3. When the subinterface is down, R5 should be allowed to initiate calls to R4 for any IP traffic.
2.4. R4 should never be allowed to call R5 based on interesting traffic or drop a call from R5 due to the lack of interesting traffic.

2 Points

2.5. Configure PPP encapsulation on the ISDN connection between R4 and R5.
2.6. Configure R4 to authenticate R5 using PAP authentication. R4 should authenticate R5 against the AAA server located at 10.0.0.100.
2.7. Configure R5 to send the username ROUTER5 along with the password CISCO for PAP authentication.
2.8. Users should be able to login to R4 using telnet along with the username of ROUTER5 and the password of CISCO1.
2.9. Apply the appropriate configuration to the AAA server for this task.

2 Points

2.10. For cost control and added security, configure R4 to call R5 back. This callback should be based on the username. R4 should receive the callback string from the AAA server.
2.11. Apply the necessary configuration on R4 and the AAA server to accomplish this task.

3 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.3. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.4. Configure RackXPIX as the PIX's hostname.

1 Point

3.5. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.6. The IDS should use the PIX as its default gateway.
3.7. Configure RackXIDS as the IDS's hostname.

1 Point

3.8. Authenticate all OSPF adjacencies within area 0 using the password CISCO. The password should not be readable when using a network analyzer on the OSPF packets.

2 Points

3.9. Perform basic authentication of the OSPF adjacencies in area 367 using the password CISCO.
3.10. Do not use the **area 367 authentication** command to accomplish this task.

1 Point

3.11. Configure authentication for EIGRP between R4 and R5. Use key 1 along with the key-string of CISCO1.
3.12. R4 and R5 should be configured to rotate keys to key 2 with the key-string of CISCO2 at 00:00 on Jan 1, 2009.
3.13. To ensure accurate key rotation, configure R4 and R5 to be NTP peers with each other and allow them to accept the old key from 23:55 31 Dec, 2008 until 00:05 Jan 1, 2009.

3 Points

3.14. Configure OSPF area 0 between SW2, the VPN3005, and the PIX.
3.15. The PIX should use 150.X.9.9 as its OSPF router ID and the VPN3005 should use 150.X.11.11.
3.16. Authenticate all OSPF adjacencies within this area using simple password authentication.

2 Points

3.17. Configure static routing to allow the VPN3005 and the PIX to reach the rest of the network.
3.18. The routes on the VPN3005 and the PIX should not point directly to an interface, but should allow at least partial reachability in the event that either R2 or R5's Ethernet interfaces are down.
3.19. Ensure that SW2 can use this routing information to reach the rest of the network.

2 Points

4. VPN

4.1. The network administrator has requested that the AAA server located at 10.0.0.100 be given access to the IDS sensor's command and control interface. The traffic between the AAA server and the IDS sensor should be encrypted when sent between R4 and the PIX. Encrypt this traffic using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES

4.2. This configuration should still function in the event of R4's Frame Relay subinterface to R5 being down.

4.3. You are allowed one static route on R4 to accomplish this.

4 Points

4.4. The network administrator has installed a new server to manage R1, R2, R3, and R5. The server is located in VLAN 5. The network administrator has requested that the management traffic between the routers and the server be encrypted inside GRE tunnels.

4.5. Create an additional Loopback (Loopback 2) on R1, R2, R3, and R5 using 10.100.100.Y/32 for addressing.

4.6. Create GRE tunnels to connect R1 to R2, R2 to R3 and finally R2 to R5. Use 10.12.12.0/24 for the tunnel between R1 and R3. Use 10.23.23.0/24 for the tunnel between R2 and R3. Use 10.25.25.0/24 for the tunnel between R2 and R5.

4.7. Advertise these new Loopback interfaces, VLAN 5, and tunnel networks through the GRE tunnels between the routers (R1, R2, R3, and R5) using RIPv2. Ensure that these routes never leak to other routers (R4, R6, etc).

3 Points

4.8. Encrypt the GRE tunnels between R1 & R2 and R2 & R5 using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5

3 Points

4.9. Encrypt the GRE tunnel between R2 and R3 using the following parameters:
- ISAKMP Authentication Method: RSA-SIG
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5

4.10. Use only one **crypto isakmp key** command on R2 to accomplish this task.

3 Points

4.11. The network administrator needs to give access to a server located in VLAN 255 to an outside consultant. The consultant will be using Cisco's VPN client to connect to the VPN3005.

4.12. Configure the VPN3005 to allow the VPN client to connect using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-SHA
- PFS: 1024 bits
- SA Lifetime: 1000KB
- Group Name: CONSULTANT_GROUP
- Group Password: CISCO
- Username: CONSULTANT
- Password: CISCO
- IP Address Pool: 192.168.0.0/24
- Simultaneous Logins Allowed: 2
- Idle Timeout: 600 Seconds

4.13. Ensure that this consultant can reach the VPN3005 using the VPN client (IPSec over UDP) when coming from behind BB3.

5 Points

4.14. You manager has asked that users in VLAN 7 be given access to the payroll server located at 10.0.0.101. Your manager has stressed the importance that this traffic not be easily compromised when transported across the network.
4.15. Encrypt this traffic between R3 and R4 using ESP/3DES/HMAC-MD5.
4.16. The source and destination IP addresses of the communication between the clients in VLAN 7 and the server in VLAN 4 should be not be hidden when transported across the network.

4 Points

5. IP Services

5.1. You have recently noticed that certain portions of your network are not able to reach BB1 and BB2. After requesting that R6 be configured to advertise the 10.0.0.0/8, 141.X.0.0/16, and 150.X.0.0/16 networks to BB1 and BB2, the network administrator has mandated that only the 141.X.0.0/16 network be advertised to BB1 and BB2.
5.2. Advertise the 141.X.0.0/16 network via BGP to BB1 and BB2.
5.3. Ensure that hosts in the 10.0.0.0/8 and 150.X.0.0/16 networks can still reach the networks learned from BB1 and BB2.

2 Points

5.4. It recently has come to your attention that BB1 and BB2 are using your network as a transit network. After further investigation, it appears that BB1 and BB2 have an IPSec tunnel that connects to each other through your network. After failed attempts to contact the administrators of BB1 and BB2, you have decided to not advertise AS54's networks to AS254 and vise versa. Upon implementing the changes to R1 and R6, the network administrator insisted that filtering will not work, as BB1 and BB2 might be using static routes to reach each other through your network. Since realizing that this is a valid workaround for them, you have decided to filter IPSec traffic inbound on R1 and R6. After implementing the filter, the network administrator has voiced concerns to management that IPSec will need to be allowed to flow from BB1 and BB2 to users behind BB3.

5.5. Since filtering off the IPSec based on all the possible source/destination IP address combinations will be a real headache, implement a technique to allow IPSec traffic into your network from BB1 and BB2 put not allow it to flow between BB1 and BB2. This technique should not rely on filtering based on the source or destination IP address.

5 Points

5.6. The network administrator has given access to users behind BB2 to a web server located in VLAN 7 (10.7.7.100). After the users have complained that they can not reach this server's IP address, you explained to the network administrator that giving the users the RFC1918 address of the server does not enable them to reach it. After spending 15 minutes trying to explain to the network administrator that even through the 10.7.7.0/24 network is reachable from inside your network, that it is not reachable by users outside of your network since you are not advertising the private networks to them. After 15 more minutes of listening to the network administrator ramble on about how IP addresses are globally significant and only MAC addresses are locally significant, you told him to just have the users behind BB2 connect to 141.X.7.100 and get out of the computer room before he breaks something.

5.7. Configure R1 so that the users behind BB2 can reach the web server on port 80 by using the 141.X.7.100 address.

5.8. R1 should respond to pings sent to 141.X.7.100.

3 Points

5.9. After users reported slow response to a server located in VLAN 100, you have discovered that the server appears to be under a Smurf attack originating from IP addresses behind BB2.
5.10. Configure R1 to limit the traffic involved in this attack to 128kbps.

2 Points

5.11. A new corporate policy dictates for R1 and R6 to be configured to block all traffic sourced from addresses in the RFC1918 address space, along with traffic sourced from their own networks (141.X.0.0/16 and 150.X.0.0/16) from coming in from BB2 and BB1.
5.12. Traffic that is filtered should be logged to a syslog server located at 10.0.0.102. These log messages should be timestamped with the routers current date and time.
5.13. For ease of management of the log messages on the server, ensure that R1 and R6 use their Loopback0 interfaces as the source address for these messages.
5.14. Configure R1 and R6 to also account for any packets that are denied by this access-list policy.

3 Points

6. General Security

6.1. A new corporate policy dictates that all connections for management purposes to R1, R4, R6, and a terminal server located on VLAN 255 be accessed via SSH.
6.2. For added security, the policy dictates that the RSA generated keys on the routers should be of the largest size supported.
6.3. Users will need to connect to the terminal server though the PIX. The terminal server's IP address is 141.X.255.254/24.
6.4. Configure the PIX to allow SSH connection to the terminal server using the IP address 141.X.100.254.

2 Points

6.5. Configure the PIX to allow users from any IP address to connect to the inside interface via SSH. Allow users from the 10.0.0.0/24 network to connect to the PIX from the outside interface.
6.6. Authenticate these users against the AAA server. Create a user called SSHUSER along with the password CISCO in the AAA server for this task.

2 Points

6.7. After giving access to the web server located in VLAN 7 to the users behind BB2, the network administrator is now concerned that unauthorized users may be accessing the server from the outside. Upon recommending to the web server administrator that it would be simple to just enable authentication on the web server itself, the web server administrator stated that unauthorized access to the web server is a network security issue and not an issue that the web server's administrator should have to deal with.

6.8. Since the web server administrator refused to authenticate the users on the server itself, management has tasked you with authenticating the users when they first enter your network.

6.9. Configure R1 to support authentication proxy for users connecting to the web server's outside global NAT IP address of 141.X.7.100.

6.10. The users will be authenticating with the username AUTH and the password CISCO.

6.11. Allow for a maximum of three (3) login attempts.

6.12. Apply the appropriate configuration to the AAA server for this task.

6 Points

6.13. After a recent security issue relating to severs in VLAN 100, a new corporate policy dictates that R4's connection to BB3 be secured. Configure R4's E0/1 interface to meet the following requirements:

- Permit outside access to a FTP server located in VLAN 100 with the IP address of 141.X.100.105
- The FTP server is running on TCP port 21 along with TCP port 10021
- Permit outside access to a web server located in VLAN 4 with the IP address is 10.0.0.150
- The web server should be reachable by the outside via the IP address 204.12.X.100 on port 80
- Allow users behind R4 to ping and traceroute to addresses on the outside
- TCP or UDP sessions that were initiated from behind R4 should be permitted inbound
- Inspect all FTP sessions on TCP ports 21 and 10021
- Permit any necessary routing protocol traffic
- Deny all other traffic

3 Points

6.14. Recently the web server located in VLAN 4 was compromised. A worm was installed on the server and was causing the server to launch attacks against similar servers in other parts of the network.

6.15. Using CBAC (firewall feature set), configure R4 to allow users in VLAN 43 to connect to the web server at 10.0.0.150 (204.12.X.100) but do not allow the web server to send traffic through R4 if it is not in response to a client's request. All other traffic from the web server should be dropped as it enters R4's interface E0/0.

3 Points

7. Advanced PIX Firewall

7.1. Configure the PIX to provide PAT translations for inside users accessing resources outside of the PIX using its interface IP address of 141.X.100.9.

1 Point

7.2. Configure the PIX to allow SNMP polling from 10.0.0.100 using the community string private.

1 Point

7.3. The network administrator recently hired a consultant to install and configure a DNS server for the users behind the PIX. After the consultant left, the network administrator noticed that the DNS entry for a file server with the IP address 10.7.7.150 was incorrectly entered in the DNS server as 10.70.70.150.

7.4. Configure the PIX to redirect traffic destined for the incorrect DNS entry's IP address of 10.70.70.150 to 10.7.7.150.

2 Points

8. AAA

8.1. After recent unauthorized configuration changes to R5, a new corporate policy dictates that access to R5 and command authorization be controlled by the AAA server.

8.2. Configure R5 to meet the following requirements:

- Telnet sessions should be authenticated against the AAA server
- If the AAA server is unavailable, users should be authenticated locally
- Create a user in the AAA server named ADMIN with the password CISCO
- This user should have full access to any commands and automatically be placed in privilege level 15 upon logging in
- Create a user in the AAA server named NOC with the password CISCO
- This user should have full access to any commands, but should not be allowed to make any changes to the configuration
- This user should be able to view the full configuration of the router when they issue a **show run**.

8.3. Apply the appropriate configuration to the AAA server for this task.

4 Points

9. IDS

Read the access instructions for the IDS Senor in the introduction for this lab prior to starting this section.

9.1. An IDS sensor has been installed to monitor traffic inbound from BB2. The sensor's command and control interface is connected to SW1's interface Fa0/10.
9.2. Allow management via SSH and HTTPS from addresses in the 10.0.0.0/24 and 141.X.0.0/16 networks. The IDS sensor should be accessible through the PIX via HTTPS and SSH from the outside by the IP address 141.X.100.10.
9.3. Configure the IDS sensor to allow R5 to connect via SSH for management purposes.

3 Points

9.4. Span traffic received on SW2's port Fa0/24 to the IDS sensor's sensing interface which is connected to SW2's port Fa0/10.
9.5. For the purposes of shunning, enable the IDS sensor to access R1 using the username IDS and the password CISCO via SSH.
9.6. The blocking interface should be R1's E0/0 interface.

2 Points

9.7. Since you are receiving too many false positives from traffic sourced by 192.10.X.150, configure the IDS sensor to filter all signatures for traffic sourced from that IP address.

2 Points

9.8. The network administrator has requested that the IDS sensor shun any host that triggers IDS signature 6920 (TCP Flood).

3 Points

9.9. After recent security issues the network administrator has requested that R4 be configured to perform basic IDS functions.

9.10. Configure R4 to meet the following parameters:

- Audit packets that are received inbound on interface E0/1
- Alarm and drop traffic that triggers an attack alarm
- Log alarms to the router's console
- Alarm, drop and reset traffic that triggers an attack alarm
- Alarm and drop traffic that triggers an informational alarm
- Disable the "Impossible IP Packet " signature
- Allow hosts in the 204.12.X.0/24 network to ping R4's interface E0/1

3 Points

IE's Security Workbook Lab 8

Difficulty Rating (10 highest): 7

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	5
ISDN/PPP	5
Routing Protocols	12
VPN	24
IP Services	12
General Security	22
Advanced PIX Firewall	9
AAA	5
IDS	6

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain IE_SEC between SW1 and SW2.
1.2. Authenticate the VTP domain with the password CISCO.

1 Point

1.3. The network administrator has reported that a few computers connected to SW2's interface Fa0/22 are being used in a DDoS attack. Until the computers can be isolated and shut down, the network administrator has requested the SW2 only accept 1Mbps of unicast traffic inbound on this interface.
1.4. SW2's interface Fa0/22 has its port speed set to 10Mbps.

2 Points

1.5. After discussing plans to implement more VLAN ACLs on SW1 in the future, your local Cisco SE has recommended that SW1 be optimized to support as many ACEs (access control entries) as possible on the 3550.
1.6. Configure SW1 as per the SE's recommendation.

2 Points

2. ISDN/PPP

2.1. Configure ISDN DDR between R4 and R5 using the dialer interfaces.

1 Point

2.2. Configure R4 to call R5 automatically whenever R4's Frame Relay subinterface to R5 goes down.
2.3. R4 should call R5 once the subinterface has been down for 30 seconds. To ensure full convergence of OSPF, R4 should disconnect the ISDN call once the subinterface has been back up for 120 seconds.
2.4. R5 should never be configured to call R4 or drop a call from R4 due to the lack of interesting traffic.

2 Points

2.5. Configure PPP encapsulation on the ISDN connection between R4 and R5.
2.6. Configure R4 and R5 to authenticate each other using CHAP with a password of CISCO. R5 should authenticate R4 via the AAA server. R4 should also use AAA but should authenticate using its own locally configured usernames and passwords.
2.7. Configure an authentication protocol that uses TCP for transport with the AAA server. Use the key CISCO and a source address of 150.X.5.5 for this communication.
2.8. Apply the appropriate configuration to the AAA server for this task.

2 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. The VPN3005 should use R4 as its default gateway.
3.3. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.4. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.5. Configure RackXPIX as the PIX's hostname.

1 Point

3.6. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.7. The IDS should use R3 as its default gateway.
3.8. Configure RackXIDS as the IDS's hostname.

1 Point

3.9. Configure OSPF area 59 between R5 and the PIX.
3.10. The PIX should use 150.X.9.9 as its OSPF router ID.

2 Points

3.11. Configure OSPF area 51 between the PIX and BB2.
3.12. Allow the routes from OSPF area 59 to be passed into area 51. These routes should appear as E2 routes in BB2's routing table.

2 Points

3.13. Configure OSPF area 0 on the private interface of the VPN3005.
3.14. Use 150.X.11.11 as the OSPF router ID.
3.15. The VPN3005 should send routing information about the 136.X.0.0/16 and the 150.X.0.0/16 networks to SW1 and SW2 via OSPF.
3.16. Static routes are permitted on R4 to provide reachability to the networks behind the VPN3005.

3 Points

3.17. Authenticate the OSPF area 0 adjacencies between the VPN3005, SW1, and SW2 using type-1 authentication.

2 Points

4. VPN

4.1. The network administrator would like to give access to a web server used by your company's accounting department in VLAN 4 to the users behind the PIX. The web server's IP address is 10.4.4.100.
4.2. Encrypt TCP traffic between the PIX and the web server using the following parameters:
- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: Default
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5

4.3. Your network administrator has informed you that the IP address of the PIX will be changed in the future. Ensure that R4's IPSec configuration does not need to be altered to accommodate this change.
4.4. This configuration should still function in the event of R4's Frame Relay subinterface to R5 fails.
4.5. The use of static routes is permitted.

5 Points

4.6. The network administrator has informed you that users in VLAN 103 will need to access servers in VLAN 4.
4.7. Create a LAN-to-LAN VPN between VLAN 4 and VLAN 103 using the strongest IPSec encryption algorithms supported by R3 and R4.
4.8. For added security, ensure that a new IPSec security association is negotiated every ten (10) minutes and that the security association keys are not based off previous keys.
4.9. The use of static routes is permitted.

4 Points

4.10. Your manager has requested that the PIX be configured to allow secure access to servers behind the PIX on the 192.10.X.0/24 network. After requesting that the users install the Cisco VPN client to access the network behind the PIX, the users have informed you that they are not allowed to install any additional software on their corporate workstations. After doing some research, you have decided to use PPTP that is supported by their Windows 2000 computers.
4.11. Configure the PIX to support PPTP using the following parameters:

- 192.168.0.1 to 192.168.0.100 for the address pool
- CHAP and MSCHAP authentication
- Local authentication (username CISCO and password CISCO)
- Require encryption (40- or 128-bit)

5 Points

4.12. Encrypt TCP and UDP traffic between the 192.10.X.0/24 and the 136.X.7.0/24 networks on the PIX and the VPN3005 using the following parameters:
- ISAKMP Authentication Method: RSA-SIG
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5

4.13. The use of static routes is permitted.

5 Points

4.14. Create a LAN-to-LAN VPN between the 10.0.0.0/24 and the 136.X.8.0/24 networks on R5 and the VPN3005 using the following parameters:
- ISAKMP Authentication Method: RSA-SIG
- ISAKMP Hash: MD5
- ISAKMP Lifetime: 12 minutes
- ISAKMP Encryption: 3DES
- CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
- ESP Encryption: AES-192
- ESP Authentication: HMAC-SHA

4.15. Users in the 136.X.8.0/24 network should never be permitted to initiate the IPSec tunnel.

5 Points

5. IP Services

5.1. A proprietary application server that was previously located in VLAN 2 has been moved to VLAN 103. Shortly after the move, users began to complain to the network administrator that they could not connect to the server. After further investigation, you have discovered that their client application accesses the server via its IP address, and this setting cannot be changed without bringing in a contract developer to alter the client application to support the new IP address of the server. Since it was your recommendation to move the server, the network administrator has asked you to solve the problem without having to bring in the contract developer.

5.2. The server's previous IP address was 136.X.2.100 and its new IP address is 136.X.103.100. The clients communicate with the server using TCP ports 3000-3500.

3 Points

5.3. You have recently noticed that BB1 and BB3 are not able to reach addresses in your network. After requesting that R6 be configured to advertise the 10.0.0.0/8, 136.X.0.0/16, and the 150.X.0.0/16 networks to BB1 and BB3, the network administrator has rejected the request.

5.4. Without advertising your networks to BB1 or BB3, ensure that devices in your network can ping BB1 and BB3.

2 Points

5.5. The network administrator would like to give access to a web server in VLAN 103 to users behind BB1. The web server's IP address is 136.X.103.101. However, since BB1 does not have a route to this network, the web server should be reachable from BB1 via the IP address 54.X.1.100.

2 Points

5.6. The network administrator has noticed that certain users in VLAN 4 have their default-gateway set to point to their Ethernet interface as opposed to the proper default gateway of R4's E0/0 IP address. However, even though the hosts are not defaulting directly to R4 you have found that they are essentially ARPing for every destination and R4 is responding with its own MAC address. As this behavior is insecure, your network administrator has requested that R4 not answer these ARP requests.

5.7. Configure the network to reflect this request.

2 Points

5.8. Users are complaining about slow response time to a web server at IP address 136.X.2.102. After further investigation, it appears that the web server is undergoing a HTTP SYN flood DoS attack from behind BB1.

5.9. In order to help deal with these attacks against the web server, configure R6 to send a TCP reset to the web server for any TCP sessions that fails to reach the established state after ten (10) seconds.

5.10. R6 should not perform any sort of proxy function for the TCP sessions to the web server.

3 Points

6. General Security

6.1. The network administrator has requested that R3 and R4 be configured to support SSH.
6.2. The routers should wait for the SSH client to respond up to a maximum of 30 seconds.
6.3. An idle SSH session should be disconnected after five (5) minutes.
6.4. The users will be authenticating with the username SSH along with the password of CISCO.

2 Points

6.5. The network administrator would like to give access to R5 to an outside consultant in order to assist with troubleshooting a network problem. The outside consultant will need access to enable and disable "ip rip" debugging. Without giving all users in privilege level 1 these commands or giving the consultant access to privilege level 15, ensure that the consultant can access these commands.
6.6. The outside consultant will be logging in using the username CONSULTANT and a password of CISCO.

3 Points

6.7. An engineer in your IS department recently installed a Windows 2000 Server (10.0.0.101) in VLAN 5 without installing any of the recommended service packs. Your network administrator is worried that the server will be open to various security vulnerabilities with this default server install. After trying to contact the engineer who installed the server, you have come to discover that the engineer is on vacation. Since you do not have control over the server to install the necessary service packs, you have decided that any users on other networks trying to access the server should first authenticate via telnet to R5 prior to being given access to this server.
6.8. Users should authenticate using the username WEB along with the password CISCO. The password should be stored in R5's configuration as an MD5 hash.

4 Points

6.9. In response to a recent ICMP DoS attack on a web server located in VLAN 103, the network administrator has requested that R3 log all ICMP echo requests destined for any IP address in the 136.X.103.0/24 network.
6.10. These log messages should be sent to a server located at 10.0.0.105 and include the MAC address of the device that forwarded the ICMP echo request to R3.

2 Points

6.11. After a recent security breach with an application server located at 136.X.2.105, a new corporate policy dictates that R2 be configured to secure access to the application server. Users accessing this server should be required to authenticate via a web browser prior to being granted access to the server.
6.12. R2 should use TACACS+ with the AAA server for authenticating the users.
6.13. Create a user called AUTH with the password of CISCO in the AAA server for this task.
6.14. Timeout inactive sessions after 30 minutes.
6.15. Apply the appropriate configuration to the AAA server for this task.

6 Points

6.16. After discovering that the security breach of the server in VLAN 2 appeared to be sourced from users behind BB3, you have decided to secure R6's subinterface to BB3.

6.17. Configure R6's interface Fa1/0/0.63 to meet the following requirements:

- Allow inbound ICMP echo replies, time-exceeded, and port unreachable messages
- Deny all other inbound ICMP packets
- Allow any TCP or UDP sessions that were initiated from behind R6
- Block the download of all JAVA applets
- Inspect all FTP and SMTP sessions
- DNS name lookup entries should expire after three (3) seconds of inactivity
- TCP entries should be removed three (3) seconds after R6 detects the FIN-exchange
- Half open sessions should be deleted after reaching 250 sessions

5 Points

7. Advanced PIX Firewall

7.1. Configure the PIX to provide one-to-one NAT translations for the 192.10.X.0/24 network using the 136.X.59.128/25 addresses. If the 136.X.59.128/25 addresses become depleted, the PIX should do PAT using the 136.X.59.127 IP address.

1 Point

7.2. After having issues trying to troubleshoot a network issue, the network administrator has requested that the PIX allow users on the inside interface to ping and traceroute to devices on the outside.
7.3. Use only one access-list entry to accomplish this task.

1 Point

7.4. The network administrator has requested that the PIX be configured to support management via SSH.
7.5. Configure the PIX to allow SSH connections from the 192.10.X.0/24 network on the inside interface and from any IP address on the outside interface.

2 Points

7.6. Users are complaining that access to certain servers through the PIX is very slow. After investigation, you have determined that these servers appear to be trying to connect back to the clients on TCP port 113.
7.7. Without permitting this traffic to the clients, solve this issue.

2 Points

7.8. After a recent exploit involving Microsoft's Active-X was discovered, the network administrator has requested that the PIX be configured for content filtering of all Active-X components. Configure the network to reflect this request.

1 Point

7.9. The network administrator would like to allow access to a web server located at 192.10.X.105 to users outside of the PIX. This web server should be accessible via 136.X.59.100 on port 80.
7.10. Users outside of the PIX should be able to ping this server.

2 Points

8. AAA

8.1. A few of the network administrators do not understand how to use the IOS CLI and have requested that R2 be setup to be managed via a web browser.
8.2. In order to minimize the risk of managing R2 via the web, use the following parameters:
- Only allow HTTPS access
- Authenticate users via the AAA server using TACACS+
- Permit access only from the 136.X.2.0/24 subnet

8.3. Apply the appropriate configuration to the AAA server for this task.

3 Points

8.4. The network administrator has requested that any privilege level 15 commands executed on R4 be accounted for.
8.5. Configure the AAA server and R4 to account for all privilege level 15 commands.
8.6. Do not account for privilege level 1 commands.
8.7. Apply the appropriate configuration to the AAA server for this task.

2 Points

9. IDS

Read the access instructions for the IDS Sensor in the introduction for this lab prior to starting this section.

9.1. An IDS sensor has been installed to monitor traffic between R5 and the PIX. The sensor's command and control interface is connected to SW1's interface Fa0/10.
9.2. Configure the sensor to allow management via SSH and HTTPS from IP addresses in the 10.0.0.0/24 and 136.X.0.0/16 networks.
9.3. Configure the sensor to allow R3 to connect via SSH.

2 Points

9.4. SPAN traffic from VLAN59 to the sensor's sensing interface which is connected to SW2's port Fa0/10. Use VLAN 111 as the remote-span VLAN.
9.5. Enable the IDS sensor to access the PIX using the username IDS and the password of CISCO via SSH.
9.6. The PIX should authenticate the IDS user using the AAA server.
9.7. The blocking interface should be the outside interface.

2 Points

9.8. Configure the IDS sensor to permanently shun any traffic from 132.X.2.50 on the PIX's outside interface.

2 Point

This page left intentionally blank

IE's Security Workbook Lab 9

Difficulty Rating (10 highest): 9

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	6
ISDN/PPP	10
Routing Protocols	12
VPN	14
IP Services	9
General Security	17
Advanced PIX Firewall	11
AAA	12
IDS	9

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain IE_SEC between SW1 and SW2.
1.2. Authenticate the VTP domain with the password CISCO.

1 Point

1.3. Your security team is concerned about a rogue network device posing as the AAA server and intercepting usernames and passwords. In order to prevent this they have asked you to configure the network so that SW1 only allows packets in on port Fa0/20 if it comes from the AAA server's MAC address and IP address. Configure SW1 to reflect this policy.

3 Points

1.4. The network administrator has been receiving complaints from users that they are getting authentication failed messages when trying to connect to the network. After investigating, you have found that these minor outages coincided with your updating of the ACL used to secure the AAA server. You have informed the network administrator that the switch is temporarily blocking traffic through the port that the ACL is being updated on. Although this is a normal and desirable case, the network administrator has requested that this behavior be disabled to ensure maximum uptime for the users.

2 Points

2. ISDN/PPP

2.1. Configure ISDN DDR between R4 and R5 using dialer profiles and PPP encapsulation.
2.2. R4 should allow IP traffic to initiate and maintain a call, but not allow IP protocol 89 traffic to keep the ISDN connection up unnecessarily.
2.3. R5 should never place or drop a call based on interesting traffic

2 Points

2.4. Whenever an ISDN call is placed, R5 should issue an authentication challenge using the alternate hostname of ROUTER5. R4 should respond to this challenge using the alternate hostname of ROUTER4, along with a hash value that represents the password CISCO.
2.5. R4 should also challenge R5. R5 should respond to this authentication challenge using the alternate hostname of ROUTER5. If R5 responds to this challenge with the username router5 as opposed to ROUTER5, R4 should not authenticate the call.

3 Points

2.6. If the direction of the call is inbound on R5, R5 should drop the call and call R4 back. The callback string should be retrieved from the AAA server.
2.7. R5 should not authenticate R4 against the AAA server for this task.
2.8. Apply the appropriate configuration to the AAA server for this task.

3 Points

2.9. The network administrator would like to justify to management the need for a secondary ISDN connection between R4 and R5. In order to help justify the additional ISDN line, the network administrator has requested that R5 record the amount of bytes transmitted and received over the ISDN connection with the AAA server.
2.10. There should only be a single record in the AAA server for each ISDN call.

2 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.3. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.4. Configure RackXPIX as the PIX's hostname.

1 Point

3.5. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.6. The IDS should use R5 as its default gateway.
3.7. Configure RackXIDS as the IDS's hostname.

1 Point

3.8. Configure RIPv2 on the VPN3005 to connect to R6.
3.9. Ensure that no other device in VLAN 116 can hear RIP updates advertised from R6 to the VPN3005.

2 Points

3.10. Configure OSPF area 0 on the PIX and VPN3005 to communicate with the rest of the routing domain.
3.11. All adjacencies in OSPF area 0 should be authenticated with the clear-text password CISCO, with the exception of the adjacency between R4 and R5.
3.12. Do not use the **ip ospf authentication** command on R4's interface connected to the Frame Relay cloud to accomplish this.

3 Points

3.13. Configure the VPN concentrator to advertise reachability information about the rest of the network to R6 and BB1.
3.14. Do not use static routes on the VPN concentrator for this task.

2 Points

3.15. In the future, the VPN concentrator will use the 192.168.100.0/24 network for a VPN client address pool.
3.16. Advertise this address pool into OSPF and RIP on the VPN3005 concentrator.

2 Points

4. VPN

4.1. The network administrator has requested that traffic between the AAA server and the IDS sensor be encrypted using IPSec. The AAA server will be using Cisco's VPN Client to encrypt the traffic between itself and R5.
4.2. Configure R5 to support Cisco's VPN client using the following parameters:
- Use only the default ISAKMP values on R5
- ESP Encryption: AES-256
- ESP Authentication: HMAC-SHA
- CA Enrollment URL: http://10.0.0.100:80/certsrv/mscep/mscep.dll
- Address Pool: 192.168.255.50-192.168.255.60
- Domain Name: internetworkexpert.com
- DNS and WINS Server: 148.X.105.100
- Group Name: IDSGROUP
- Group Password: CISCO
- Username: IDSUSER
- Password: CISCO
- Allow for split tunneling for destinations outside of the 148.X.0.0/16 network

4.3. R5 should authenticate this user (IDSUSER) using its local username and password database.

6 Points

4.4. Create an additional Loopback interface (Loopback 1) on R1, R2, R4, and R5. Use 192.168.255.Y/32 for addressing on these Loopback interfaces.
4.5. Configure a fully meshed GRE tunnel network between these new Loopbacks on R1, R2, R4, and R5. Use 192.168.100.Y/24 for IP addressing inside the tunnel. Do not use the **tunnel destination** interface command to accomplish this task.
4.6. Source the tunnel off of the router's Loopback 0 interfaces.
4.7. Enable EIGRP AS 1 for the Loopback 1 and GRE tunnel networks (192.168.255.Y/32 and 192.168.100.0/24).
4.8. Ensure EIGRP updates from one router are relayed to the other routers through the multipoint GRE tunnel.

4 Points

4.9. Encrypt the multipoint GRE tunnel on R1, R3, R4 and R5 using the following parameters:

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: MD5
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-SHA
- IPSec SA's should be deleted after 20 minutes of inactivity.

4 Points

5. IP Services

5.1. The network administrator has requested that R2 and R3 provide redundant gateways for hosts in VLAN 232. Some of the hosts have their default gateway set to 192.10.X.100, while others have their default gateway set to 192.10.X.101.
5.2. Configure R2 as the active router for the 192.10.X.100 IP address and R3 as the active router for the 192.10.X.101 IP address.
5.3. R3 should take over for the 192.10.X.100 IP address in the event R2's subinterface to R1 goes down.
5.4. R2 should take over for the 192.10.X.101 IP address in the event that both R3's subinterface to R5 and interface E0/0 are down.

3 Points

5.5. Configure R2 and R3 to not allow any other devices to take over the role as the active router.

2 Points

5.6. The network administrator has requested that R3 be configured as a TFTP server for its IOS image (c2600-ik9o3s3-mz.122-15.T13.bin) so that R2 can be upgraded.
5.7. Only allow R2's interface E0/0 IP address to download this image.
5.8. Do not use policy routing or apply an access-list to an interface for this task.

2 Points

5.9. Translate any 10.0.0.0/8 IP addresses on R2 and R3 when sent into VLAN 232. R2 and R3 should translate this traffic to their Loopback 0 interface IP addresses.
5.10. TCP translations should timeout after six (6) hours of inactivity.
5.11. DNS translations should timeout after twice the default allotted time.

2 Points

6. General Security

6.1. The network administrator has requested that an access-list be applied outbound on R3's interface E0/1 that denies ICMP echo requests to BB2's IP address of 192.10.X.254.
6.2. The network administrator further requested that packets sourced by R3 that match this access-list be dropped.

4 Points

6.3. Configure the PIX's outside and inside interfaces to not respond to ICMP echo requests.
6.4. Hosts on the inside of the PIX should be able to ping and traceroute to destinations on the outside interface.

2 Points

6.5. A new corporate policy dictates that anyone connected to R1 should not be able to telnet to any other device from R1.
6.6. Do not apply an access-list to any interface or line to accomplish this task.

2 Points

6.7. The network administrator has requested that R4 allow users across the Frame Relay and ISDN clouds access to a web server located in VLAN 4 with the IP address of 148.X.4.100 during the times of 8am to 5pm Monday through Friday.
6.8. During all other times, users should be required to telnet to R4 on TCP port 3001 and authenticate using the username WEB along with the password CISCO before being given access.

2 Points

6.9. Configure R3 to require users in VLAN 3 to authenticate using HTTP prior to being permitted through the router. Use authentication proxy for this task.
6.10. Display the following banner to the users: *Authorized Users Only!*
6.11. Age out authentication cache entries after 20 minutes of inactivity.
6.12. Users will be authenticating with the username VLAN3 and password CISCO.
6.13. Apply the appropriate configuration to the AAA server for this task.

3 Points

6.14. The network administrator has requested that R6 be secured. The network administrator would like the ATM0/0/0.1 interface to be the outside interface, Fa1/0/0.6 a DMZ interface, and Fa1/0/0.116 as the inside interface. Configure R6 according to the following requirements:
- Apply the following access-list inbound on interface ATM0/0/0.1
  access-list 100 permit tcp any host 148.X.6.100 eq 80
  access-list 100 permit icmp any host 148.X.6.100 echo
  access-list 100 permit udp any any eq rip
  access-list 100 deny ip any any
- Apply the following access-list inbound on interface Fa1/0/0.6
  access-list 101 deny ip any any
- Using CBAC, permit returning TCP/UDP sessions and ICMP traffic that was initiated from the inside of R6 to return on the outside and DMZ interfaces.
- Permit returning traffic inbound on Fa1/0/0.6 from the inside and outside interfaces to a web server located in the DMZ with the IP address of 148.X.6.100

6.15. Do not alter access-list 100 or access-list 101 to accomplish this task.

4 Points

7. Advanced PIX Firewall

7.1. Configure the PIX to translate the 10.89.89.0/24 IP addresses to 148.X.255.200-148.X.255.202.
7.2. Translate the 150.X.8.0/24 network to the outside interface of the PIX.
7.3. Exclude the 150.X.8.100 IP address from this translation.

2 Points

7.4. A DHCP server was recently installed in VLAN 255. Configure the PIX to relay any DHCP client requests on the inside interface to the DHCP server at 148.X.255.254

2 Points

7.5. The network administrator has requested that the PIX allow access to a web server with the IP address of 10.89.89.75. The web server should be accessible to the outside users via 148.X.255.75.
7.6. The web server is running on TCP port 80 along with port 8080.
7.7. Ensure that the PIX performs application inspection for the HTTP connections on port 80 along with port 8080.

2 Points

7.8. The network administrator is concerned with the possibility of a DoS attack against the web server. The network administrator has recommended that the PIX only allow for a maximum of 4000 connections to the server, and a maximum of 2000 half-open connections on each TCP port the HTTP server is running on.

2 Points

7.9. The network administrator has installed a DNS server in VLAN 89 with the IP address of 10.89.89.175. The network administrator has requested that the DNS server appear to users outside of the PIX to be running on the same IP address as the web server (148.X.255.75).
7.10. Configure the PIX to allow users on the outside to communicate with the DNS server using IP address 148.X.255.75.
7.11. Allow for DNS zone transfers from the outside.

3 Points

8. AAA

8.1. The network administrator has requested for SSH sessions to be permitted from 148.X.57.7 and 148.X.255.1 on the outside interface of the PIX.
8.2. Authenticate these users against the AAA server using RADIUS.
8.3. Users will be authenticating with the username SSH and password CISCO.
8.4. Apply the appropriate configuration to the AAA server for this task.

2 Points

8.5. After a recent security issues believed to be caused by a host in VLAN 89, a new corporate policy dictates that all outbound telnet sessions through the PIX be authenticated prior to permitting the telnet session through.
8.6. Configure the PIX to authenticate outbound telnet session against the AAA server using TACACS+.
8.7. Ensure that the PIX retries three additional times if no acknowledgments are received from the AAA server, and waits 20 seconds between these retries.
8.8. The network administrator has requested that a certain host in VLAN 89 be exempt from this authentication. The host's current IP address is 10.89.89.50 and MAC address is 1234.4567.890a. The network administrator has informed you that the IP address was received via DHCP. Ensure that this host is exempt from this telnet authentication process even if its IP address changes.
8.9. Apply the appropriate configuration to the AAA server for this task.

4 Points

8.10. The PIX should timeout these sessions if there is no activity for 15 minutes.

1 Point

8.11. After recent unauthorized changes to the PIX were discovered, the network administrator has requested that the PIX to be configured to authorize and account for all commands.
8.12. Configure the PIX to authenticate, authorize, and account with the AAA server.
8.13. Apply the appropriate configuration to the AAA server for this task.

2 Points

8.14. Create a user in the AAA server named PIX along with the password CISCO.
8.15. Allow this user access to all debug commands on the PIX without giving the user access to privilege level 15.
8.16. Ensure that the console is authorized to execute all commands.

3 Points

9. IDS

Read the access instructions for the IDS Sensor in the introduction for this lab prior to starting this section.

9.1. An IDS sensor has been installed to monitor traffic received on SW1's interface VL73 from BB3.
9.2. Only allow management of the IDS sensor via HTTPS from the AAA server's IP address of 10.0.0.100.
9.3. The IDS sensor should be available via TCP port 14433.
9.4. Configure the IDS Event Viewer to manage the IDS sensor.

3 Points

9.5. Configure SW1 and SW2 to SPAN SW1's interface Fa0/24 to the IDS's sensing interface which is connected to SW2's interface Fa0/10.
9.6. Use VLAN 500 as the RSPAN VLAN.

1 Point

9.7. The network administrator is paranoid about people making changes to the routers and would like the IDS sensor to generate a low severity alarm whenever a telnet session contains the string "conf".

2 Points

9.8. Configure IDS inbound on R2's interface E0/0 according to the following requirements:

- Disable signature 2001 for IP addresses in the 148.X.0.0/16 network
- Enable signature 2000 for only IP address 192.10.X.254
- Allow a maximum of 75 event notifications in the routers event queue
- Alarm and drop on informational and attack signatures
- Apply the necessary configure to ensure communication with the AAA server

3 Points

IE's Security Workbook Lab 10

Difficulty Rating (10 highest): 9

Lab Overview:

This lab scenario is a mock lab exam designed to simulate the conditions of Cisco Systems' CCIE Security Lab exam. This lab should be completed within 8 hours. The only resource that should be used while configuring this lab is Cisco's documentation set. This documentation is available in both CD format, and online at http://www.cisco.com/univercd.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. The initial configurations for all routers and switches include IP addressing information.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

The default username and password for the VPN 3005 is admin. The default username and password for the IDS sensor is either cisco/cisco or cisco/ids4210.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 100 points. A score of 80 points is required to achieve a passing score. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Grading for this practice lab is available when configured on Internetwork Expert's racks, or the racks of Internetwork Expert's preferred vendors. See Internetwork Expert's homepage at http://www.internetworkexpert.com for a list of preferred vendors and more information.

Point Values:

The point values for each section are as follows:

Section	Point Value
Catalyst 3550	7
ISDN/PPP	10
Routing Protocols	13
VPN	19
IP Services	8
General Security	12
Advanced PIX Firewall	11
AAA	13
IDS	7

GOOD LUCK!

1. Catalyst 3550

1.1. Configure the VTP domain IE_SEC between SW1 and SW2.
1.2. Authenticate the VTP domain with the password CISCO.

1 Point

1.3. Engineers in your NOC have recently received lots of complaints from various users about a general network slow down. In response to this, one of the Level 1 support engineers reloaded SW1 and SW2. After the reload, the problem went away, but the syslog messages stored in the switches' buffers were lost. This resulted in making the original problem that much harder to track down. This engineer recommended to management that SW1 and SW2 be configured to log their syslog messages to a real syslog server. Instead, management has asked you to configure SW1 and SW2 to store all their syslog messages except debug messages themselves even if they reboot.

2 Points

1.4. Your security team is concerned about non-IP packets coming in from BB3 slowing down the filtering capability of the PIX firewall. In order to take some of the load off of the PIX, you have decided to filter these packets out before they are received by R4.
1.5. Configure the network so that only IP packets are accepted from BB3.

4 Points

2. ISDN/PPP

2.1. Configure ISDN DDR between R4 and R5 using only the physical ISDN interfaces.
2.2. R4 should permit OSPF traffic to initiate and maintain a call. R5 should not initiate a call, nor should it disconnect a call due to its idle-timer expiring.
2.3. R4 and R5 should suppress the periodic OSPF hellos and LSA refresh messages across the ISDN connection.

2 Points

2.4. Configure PPP authentication on R4 and R5 to meet the following requirements:
- R4 should authenticate using PAP with the AAA server for all inbound and outbound calls
- If communication with the AAA server fails, R4 should use local authentication
- R5 should use the username ROUTER5 along with the password of CISCO for PAP authentication
- R5 should authenticate R4 using CHAP authentication for inbound calls only
- R4 should use its hostname along with the password CISCO for this authentication process
- R5 should authenticate R4 using the AAA server
- Use an authentication list named PPPAUTH for this task

2.5. Apply the appropriate configuration to the AAA server for this task.

3 Points

2.6. The primary purpose of the ISDN connection between R4 and R5 is to back up their Frame Relay connection. The network administrator would like the ISDN connection to be used only in the event that either R4 or R5 lose connectivity to R3.
2.7. Configure R4 to call R5 whenever R4 loses IP connectivity to R5's Loopback 0 interface.
2.8. Upon bootup, R4 should wait 360 seconds before performing an initial route check on R5's Loopback.

2 Points

2.9. Configure a subinterface numbered .1 on R6.
2.10. Configure the ATM PVC 0/20X on this interface.
2.11. Configure PPP over ATM on this VC using interface Virtual-Template1.
2.12. The IP address of this interface should be 54.X.7.6/24.
2.13. BB1 will be sending a challenge with the username BB1. R6 should reply with the username ROUTER6 and a hash value based off the password CISCO.
2.14. R6 should not challenge BB1.
2.15. Do not use the **ppp chap password** command to accomplish this.

3 Points

3. Routing Protocols

3.1. Configure the IP addresses for the public and private interfaces of the VPN3005 according to the diagram provided.
3.2. Configure RackXVPN as the VPN3005's hostname.

1 Point

3.3. Configure the IP addresses for the inside and outside interfaces of the PIX according to the diagram provided.
3.4. Configure RackXPIX as the PIX's hostname.

1 Point

3.5. Configure the IP address for the command and control interface of the IDS according to the diagram provided.
3.6. The IDS should use the PIX as its default gateway.
3.7. Configure RackXIDS as the IDS's hostname.

1 Point

3.8. Configure OSPF area 0 on the outside interface of the PIX using process-id 1.
3.9. Authenticate the OSPF adjacency between R4 and the PIX using the clear-text password CISCO.
3.10. Authenticate all other OSPF area 0 adjacencies in this routing domain with a secure hash value of the password CISCO.
3.11. Do not use the **ip ospf authentication message-digest** command on R4 to accomplish this.

3 Points

3.12. Configure OSPF area 0 on the inside interface of the PIX using process-id 2.
3.13. Authenticate the OSPF adjacency between the PIX and SW1 using a secure hash value of the password CISCO.
3.14. Ensure that no other devices can hear OSPF updates sent from SW1 to the PIX.

3 Points

3.15. Configure OSPF area 51 on the VPN3005's public interface to enable IP reachability with the rest of the routing domain.
3.16. The VPN3005 should advertise SW2's Loopback 0 interface into OSPF.
3.17. The use of a static route on the VPN3005 is permitted for this task.

2 Points

3.18. Authenticate all OSPF adjacencies within area 51 using type-2 authentication, with the exception of adjacencies in VLAN 111.
3.19. Authenticate OSPF adjacencies within VLAN 111 using type-1 authentication.

2 Points

4. VPN

4.1. The network administrator has requested that the PIX be configured to allows hosts to connect using Cisco's VPN Client

4.2. Configure the PIX to support Cisco's VPN client using the following parameters:

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: SHA
- ISAKMP Encryption: 3DES
- ESP Encryption: AES-256
- ESP Authentication: HMAC-SHA
- Address Pool: 10.255.255.100-10.255.255.150
- Group Name: GROUP1
- Group Password: CISCO
- Username: USER1
- Password: CISCO

4.3. The PIX should authenticate this user (USER1) against the AAA server.

4.4. Apply the appropriate configuration to the AAA server for this task.

6 Points

4.5. On the PIX and VPN3005, create a LAN-to-LAN VPN between VLAN 255 and VLAN 118 using the following parameters :

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Hash: SHA
- ISAKMP Encryption: 3DES
- ESP Encryption: 3DES
- ESP Authentication: HMAC-MD5

4.6. Configure the VPN3005 to reserve 256kbps of bandwidth for this VPN tunnel.

4 Points

4.7. On the PIX and VPN3005, create a LAN-to-LAN VPN between VLAN 8 and VLAN 118 using the following parameters :

- ISAKMP Authentication Method: PRE-SHARED
- ISAKMP Encryption: 3DES
- ESP Encryption: ESP-NULL
- ESP Authentication: HMAC-MD5

4.8. Configure the VPN3005 to filter ICMP traffic through the VPN tunnel.

4 Points

4.9. The network administrator would like to connect VLAN 3 and VLAN 5 together using a GRE tunnel. All traffic that enters R3's interface E0/1 should be forced through the tunnel. All traffic that enters R5's interface E0/0 should also be forced through the tunnel.
4.10. Encrypt this GRE tunnel using triple DES encryption.
4.11. To reduce overhead on the routers at the expense of security, ensure that the IPSec security associations have an infinite lifetime.
4.12. This configuration should continue to function in the event the Frame Relay connection between R3 and R5 is down.

5 Points

5. IP Services

5.1. Recently, administrators in your NOC have been complaining that it is too hard to decode the output from a traceroute going through your network. Apparently, every time they traceroute they have to look at the IP addressing table to see which device has which IP address. They have requested that all devices in the network simply reply to a traceroute from their Loopback 0 interfaces. Although the other engineers on your team have told the NOC engineers that this is not possible, you know that it can be done. In order to show off your skills to your co-workers, configure R3 so that it always replies to a traceroute from its Loopback 0 interface.

4 Points

5.2. The network administrator has requested that R6 log all critical and below messages to a syslog server with the IP address of 10.0.0.100.
5.3. In order to organize the messages on the syslog server, the syslog server will be expecting these messages to use syslog facility local3.

2 Points

5.4. The network administrator has voiced concerns regarding spoofed IP addresses entering the network through R6, and has requested that unicast reverse path forwarding be enabled on R6's interface to BB1 and BB2.

5.5. Due to various routing anomalies between BB1 and BB2, the network administrator has requested that R6 forward all packets if it has a route to the source of the packet even if the packet was not received on the preferred interface.

2 Points

6. General Security

6.1. The network administrator has requested that R4's interface E0/1 be hardened according to the following requirements:

- Permit inbound access to a web server with the IP address of 164.X.49.100 on TCP port 8080 via 204.12.X.100 TCP port 80
- Permit inbound TCP or UDP sessions that were initiated from behind R4
- Close inactive TCP sessions after 3600 minutes of inactivity
- Allow hosts behind R4 to ping and traceroute to IP addresses on the outside
- Inspect all HTTP sessions on TCP ports 80, and inspect HTTP sessions on TCP 8080 for hosts in VLAN 49
- Translate all 150.X.0.0/16 IP addresses to 204.12.X.150 through 204.12.X.151
- Translate all 10.0.0.0/8 IP addresses to 204.12.X.250 through 204.12.X.251
- Permit any necessary routing protocol traffic
- Deny all other traffic

4 Points

6.2. After implementing the new security policy on R4, the network administrator can not TFTP files to a server at 204.12.X.50.

6.3. Configure R4 to allow for successful TFTP transfers from an inside host to an outside TFTP server.

1 Point

6.4. The network administrator has requested that R3 permit all traffic out it's interface S1/0.345, but only permit the following traffic inbound:

- GRE tunnel and IPSec from R5
- OSPF
- BGP peering session between R4 and R6
- Syslog traffic
- TACACS+ and RADUIS to 10.0.0.100
- ICMP echo, echo reply, and time-exceeded
- ICMP packet type used with path MTU discovery
- Telnet and SSH

3 Points

6.5. Using NAT, configure TCP load distribution on R5 for traffic destined for the virtual IP address of 164.X.55.100. R5 should distribute the connections to 146.X.55.150, 146.X.55.151, and 146.X.55.152.

2 Points

6.6. After a recent issue with false RIP updates being injected into R3's routing table, the network administrator has become paranoid about the possibility of it happening again. The network administrator has requested that the network be configured to only allow R3 to receive RIP updates from the AAA server's IP address of 10.0.0.100.

6.7. Configure the network to meet the request without making changes to R3 or the AAA server.

2 Points

7. Advanced PIX Firewall

7.1. Configure the PIX to translate IP addresses from the 10.7.7.0/24 subnet to the IP address of the outside interface.
7.2. Translate IP addresses from the 10.255.255.0/24 subnet to 164.X.49.60/30.
7.3. Translate all other IP addresses to 164.X.49.70/32.

2 Points

7.4. The network administrator has requested that the PIX be configured to log all severity level 6 messages and below to the syslog server at 10.0.0.100.
7.5. The syslog messages should be sent using syslog facility local5.

2 Points

7.6. After enabling syslog on the PIX, the network administrator has complained that the PIX is flooding the server with %PIX-7-710005: messages.
7.7. Configure the PIX not send this message to the syslog server.

1 Point

7.8. Configure the PIX to allow a multicast stream from a server in VLAN 49 to clients located on the inside interface of the PIX.

2 Points

7.9. The network administrator has requested that the PIX be configured to allocate IP addresses to hosts in VLAN 255 according to the following requirements:

- DNS Servers: 10.255.255.99 and 10.255.255.100
- Domain: internetworkexpert.com
- Address Pool: 10.255.255.170 to 10.255.255.200
- DHCP Lease Length: Twice the default value

2 Points

7.10. An outside consultant has recommended to your network administrator that, because the PIX currently only allows DNS packets that are a maximum size of 512 bytes, by increasing the maximum size to 1024 bytes, users will experience better performance with the DNS server. Since you do not want to get into a discussion with the consultant as to the logic of this recommendation, you have decided that it is easier to just configure the PIX to allow for the 1024 byte DNS packets.
7.11. Configure the PIX to allow for DNS packets up to 1024 bytes.

2 Points

8. AAA

8.1. Recently, a worm infected computers in VLAN 8, and propagated itself to other computers using TCP port 139. Therefore a new corporate policy dictates that all TCP connections outbound on the PIX that use port 139 must be authenticated prior to being permitted out.
8.2. Configure the PIX to require VLAN 8 users to authenticate by telneting to 10.255.255.100 and entering username USER1 along with the password of CISCO. If authentication is successful they should be allowed to make TCP port 139 connections out of the network.
8.3. The PIX should authenticate these users against the AAA server.
8.4. Apply the appropriate configuration to the AAA server for this task.

4 Points

8.5. Recently, a user in the company's NOC made unauthorized changes to the PIX. After recommending that the NOC personnel not be given access to privilege level 15 on the PIX, the NOC manager insists that the NOC personnel need access to view the PIX's running configuration.
8.6. Without giving the NOC personnel access to privilege level 15, allow them to view the running configuration on the PIX.
8.7. Configure the PIX to authenticate the NOC login of NOCUSER along with the password of CISCO against the AAA server.
8.8. Apply the appropriate configuration to the AAA server for this task.

4 Points

8.9. After recent unauthorized changes to R5's configuration, the network administrator would like R5 to be configured to authorize and account for all privilege level 12 commands. Configure R5 to meet the following requirements:
- Authenticate users telneting into it against the AAA server using RADIUS
- If communication with the AAA server fails, R5 should authenticate using the password configured under the VTY lines
- Source the RADIUS packets off R5's most reliable interface
- Add a user named R5USER with the password CISCO into the default group in the AAA server
- R5USER should be placed in privilege level 12 upon login. Do not edit the default group settings in the AAA server for this task.
- Move the **debug** and **undebug** commands to privilege level 12
- Account for all privilege level 12 commands with the AAA server
- R5 should send a start notice and stop accounting notice to the AAA server

8.10. Apply the appropriate configuration to the AAA server for this task.

5 Points

9. IDS

Read the access instructions for the IDS Sensor in the introduction for this lab prior to starting this section.

9.1. An IDS sensor has been installed to monitor traffic as it enters your network via the Ethernet connection to BB3.

9.2. Allow management of the IDS sensor via telnet and HTTPS from IP addresses in the 10.0.0.0/24 subnet.

2 Points

9.3. Span traffic from SW1's interface Fa0/24 to the IDS sensor's sensing interface which is connected to SW2's interface Fa0/10.

1 Point

9.4. Configure the IDS to support shunning on SW1's interface Fa0/24.
9.5. Enable the IDS sensor to access SW1 using the username IDS and the password CISCO via SSH.
9.6. SW1 should authenticate the IDS user against the AAA server.
9.7. The IDS sensor should never block addresses 204.12.X.0/24 network.

2 Points

9.8. The network administrator has noticed an excessive amount of entries in the internal Windows server's web logs that match signature number 5081. The network administrator has requested that the IDS shun any host that triggers this signature.

2 Points