COMPUTER ENGINEERING SERIES

Computer Network Security

Ali Sadiqui

ISTE

WILEY

Computer Network Security

Series Editor
Jean-Charles Pomerol

Computer Network Security

Ali Sadiqui

ISTE

WILEY

First published 2020 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Control Number: 2019952965

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-78630-527-5

Contents

Preface

This book is meant for students preparing for the CCNA security exam (210-260 IINS), whether they are in professional training centers, technical faculties or in training centers associated with the "Cisco Academy" program. Nevertheless, it may also prove useful to anyone who is interested in information security, whether they work in a professional setting or are simply an IT user.

The book covers all subjects listed in the syllabus for the Cisco exam mentioned above. However, we have also integrated certain practical cases from the real work of networks that we deemed important.

Each chapter begins by presenting a theoretical concept related to a pre-determined security objective and then provides the CLI commands and screenshots of the GUI needed to secure the network component. Practical tasks are suggested at the end to help the student apply this configuration and gain mastery over the concept presented.

This book was developed in collaboration with a training and certification team from Cisco in order to ensure that the content was clear and simple. The book aims to present, in a single volume, the state-of-the-art and good practices to put in place a secure information system.

We hope that the book meets the expectations of our students and helps them obtain their certification while also allowing anyone interested in this topic to better understand the different concepts of information security.

Ali SADIQUI
November 2019

Introduction

Introduction to CCNA Security

The “CCNA Security” certificate is a test that validates the knowledge and qualifications required to secure a network made up of Cisco infrastructure.

This allows a network professional to demonstrate the skills required to develop security infrastructure, recognize threats to the network and vulnerabilities in the network, and mitigate these threats in order to maintain integrity, confidentiality and the availability of data and devices.

Prerequisites

1) In order to optimize your learning from this book, it is highly recommended that you examine the objectives required for the following certifications:

– CCENT Cisco;

– CCNA routing and commutation.

Conventions for command syntax

2) The conventions followed in this book to present the syntax for commands are given below:

– text in **bold**: indicates the commands or keywords;

– *italics*: denote the arguments or user variables;

– vertical lines (|): indicate alternative and mutually exclusive elements;

– square brackets ([]): indicate optional elements;

– curly brackets ({}): indicate a necessary choice;

– curly brackets within square brackets ([{}]): indicate a necessary choice in an optional element.

1

Fundamentals of Network Security

This chapter studies the following subjects:

– the chief objectives of securing a network;

– information security terminology:

  - general terminology,

  - types of hackers,

  - malicious codes;

– the types of network security:

  - physical security,

  - logical security,

  - administrative security;

– the chief risks related to the logical security of a network:

  - the different kinds of network attacks,

  - measures for network security,

  - vulnerability audit measures

1.1. Introduction

Network security is the branch of computer science that consists of protecting all components of a computer network in order to prevent unauthorized access, data stealing, misuse of a network connection, modification of data, etc. The aim of

Computer Network Security, First Edition. Ali Sadiqui.

network security is to provide proactive defense methods and mechanisms to protect a network against internal and external threats.

1.1.1. *The main objectives of securing a network*

The three main objectives in securing a network are to ensure:

– **confidentiality**: this consists of protecting data stored on or traveling over a computer network from unauthorized persons;

– **integrity**: this maintains or ensures the reliability of data. The data received by a recipient must be identical to the data transmitted by the sender;

– **availability**: this ensures that network data or services are constantly accessible to users.

1.1.2. *Information security terminology*

1.1.2.1. *General terminology*

– **A resource**: any object that has value for an organization and must be protected.

– **A vulnerability**: a weakness in a system, which may be exploited by a threat.

– **A threat**: a potential danger to a resource or to the functioning of a network.

– **An attack**: this is an action carried out to harm a resource.

– **A risk**: the possibility of an organization's resource being lost, modified, destroyed or suffering other negative consequences. The risk may arise from a single threat or several threats or the exploitation of a vulnerability:

$$A\ risk = a\ resource + a\ threat + a\ vulnerability$$

– **A countermeasure**: protection that mitigates a potential threat or a risk.

1.1.2.2. *Types of hackers*

There are different kinds of hackers in the field of information technology:

– "**hackers**": this group is defined as people who are "network maniacs" and only wish to understand the working of computer systems, while also testing their own knowledge and tools;

– "**white hat hackers**": these are individuals who carry out safety audits in order to test that an organization's computer networks are well-protected;

– "**black hat hackers**": these are experienced individuals who work towards illegal ends by carrying out data theft, hacking accounts, infiltrating systems etc.;

– "**gray hat hackers**": individuals who are a mix of a "white hat" and "black hat" hackers;

– "**blue hat hackers**": these are individuals who test bugs in order to ensure that applications work smoothly;

– "**script-kiddies**": these are individuals with very basic IT security management skills and who try to infiltrate systems using scripts and programs developed by others;

– "**hacktivists**": these are individuals who are chiefly driven by ideological motives;

– "**phreakers**": these are individuals who are specialized in attacking telephonic systems. In general, they work towards placing free calls;

– "**carders**": these are individuals who specialize in attacking smart card systems.

1.1.2.3. *Malicious codes*

The most common types of malicious codes or malware that may be used by hackers are:

– **virus**: this is a program that attaches itself to a software to carry out a specific, undesirable function on a computer. Most viruses need to be activated by the user. However, they can also be set to "idle mode" for prolonged periods as they can also be programmed to avoid detection;

– **worms**: these are independent programs that exploit known vulnerabilities with the aim of slowing down a network. They do not need to be activated by the user, and they can duplicate themselves and attempt to infect other hosts in the network;

– **spyware**: these are spy software that are generally used in order to influence the user, to buy certain products or services. Spyware is not usually automatically self-propagating but install themselves without permission. They are programmed to:

- collect the user's personal information,

- track browsing activity on the internet in order to detect the user's preferences,

- redirect HTTP requests towards pre-set advertising sites;

– **adware**: this refers to any software that displays advertisements without the user's permission, often in the form of pop-up windows;

– **scaryware**: this refers to a category of software that is used to convince users that their system has been infected by viruses and suggests solutions, with the goal being to sell software;

– **Trojan horse**: this is a program characterized by two features:

- behavior that is apparently useful to the user,

- hidden malicious behavior, which usually leads to access to the machine on which this software is executed;

– **ransomware**: ransomware is a program that is designed to block access to a computer system, by encrypting the contents until a certain amount of money is paid in order to restore the system.

1.2. Types of network security

We identify three categories of network security.

1.2.1. *Physical security*

Physical security involves all aspects of the environment in which the resources are installed. This may include:

– the physical security of server rooms, network devices etc.;

– the prevention of accidents and fires;

– uninterrupted power supply;

– video surveillance etc.

1.2.2. *Logical security*

Logical security refers to the implementation of an access control system (using a software) in order to secure resources. This may include:

– applying a reliable security strategy for passwords;

– setting up an access model that is based on authentication, authorization and traceability;

– ensuring the correct configuration of network firewalls;

– putting in place IPS (intrusion prevention systems);

– using VPNs (Virtual Private Network) etc.

1.2.3. *Administrative security*

Administrative security allows the internal monitoring of an organization using a manual of procedures.

This may include:

– preventing errors and frauds;

– defining the responsibilities of different actors or operators;

– protecting the integrity of the company's property and resources;

– ensuring that all operations concerning handling of material are recorded;

– rationally managing the company's property;

– ensuring effective and efficient management of activities.

NOTE.– You can now attempt Exercise 1.

1.3. The main risks related to the logical security of the network

1.3.1. *Different kinds of network attacks*

1.3.1.1. *Reconnaissance attacks*

The aim of reconnaissance attack or "passive attack" is to collect information on the target network in order to detect all the vulnerabilities. In general, this attack uses the following basic methods:

– "**ping sweep**": the attacker sends ping packets to a range of IP addresses to identify the computers that are part of a network.

– **port scanning**: the attacker carries out a port analysis (TCP and UDP) in order to discover what services are being run on a target computer;

– **packet sniffing**: "packet sniffing" makes it possible to capture data (generally Ethernet frames) that are traveling over a network, with the aim of identifying MAC addresses, IP addresses or the number of ports used in a target network. This attack can even make it possible to discover user names or passwords. The most commonly used packet capture software is **wireshark** and **tcpdump**.

1.3.1.2. *Password attacks*

The goal of these attacks is to discover usernames and passwords in order to access various resources. There are two commonly used methods in this type of attack:

– **dictionary attack**: this method uses a list of words or phrases that are commonly used as passwords;

– **brute force attack**: this method tries out all possible combinations of letters, numbers and symbols to detect a user's password.

1.3.1.3. *Access attacks*

The aim of these attacks is to try and recover sensitive information about network components. The following methods are commonly used to carry out an access attack:

– **phishing**: phishing is an attempt to recover sensitive information (usually financial information such as credit card details, login, password, etc.), by sending unsolicited emails with fake URLs;

– **pharming**: this is another network attack that aims to redirect traffic from one website to another website;

– "**Man-in-the-middle**" **attack**: an attacker places themselves between two network components to try and benefit from the data being exchanged. This attack is based, among other things, on:

- **spoofing**: this is a practice in which communication is sent from an unknown source disguised as a reliable source for the receiver. This makes it possible to deceive a firewall, a TCP service, an authentication server etc. Spoofing may take place at several levels: MAC address, IP address, TCP/UDP port, a DNS domain name,

- **hijacking**: the attacker hijacks a session between a host and server to obtain unauthorized access to this service. This attack relies on spoofing;

– **mixed attacks**: Mixed attacks combine the characteristics of viruses, worms, and other software to collect user information.

1.3.1.4. *Network attacks against availability*

– **DoS** or Denial of Service attacks are attacks that render a service unavailable in various ways. These attacks can be divided into two main categories:

- **denial of service by saturation**: these attacks consist of flooding a machine with false requests so that it is unable to respond to real requests;

- **denial of service by exploiting vulnerability**: these attacks consist of exploiting a weakness in a remote system in order to make it unavailable.

– **DDoS** or *Distributed Denial of Service* attacks are a type of DoS attack originating from many connected computers controlled by hackers who attack from different geographic locations. The principles underlying these attacks are based on the follow methods (among others):

- **SYN flood attacker**: an attacker sends several TCP-SYN packets to set up a 'TCP' connection without sending a “SYN-ACK” message;

- **ICMP flood**: an attacker sends the target computer multiple fake ICMP packets.

1.3.1.5. *Close attacks*

A close attack is unusual in that the attacker is physically close to the target system. The attacker takes advantage of the fact that they are close to the target devices to reset a router, for example, or start a server with a CD etc.

1.3.1.6. *Attacks on the approval relationships*

When taking control of a network machine, the attacker exploits the relationship of approval between this machine and the various peripheral devices on a network in order to gain greater control.

1.3.2. *Network security measures*

In order to ensure greater security to a network within a company, the following measures are recommended:

– **separation of resources**: the network of resources of an organization and various sensitive data must be located in different security zones (for example, creation of a DMZ cone). Access to the network of an organization and to databases must be carried out through highly monitored mechanisms.

– **deep protection**: network security devices must be used in different locations of the organization’s network;

– **the "least privilege" rule**: each user must be assigned only the minimal level of access required to carry out a given task;

– **adequate protection**: protection mechanisms must be installed in a reliable and effective manner at all levels of the network;

– **restricting the consultation of information**: only information required for carrying out a specific task must be provided to a given employee.

– **separation of tasks and job rotation**: the separation of tasks and job rotation contributes to a better implementation of security policies in organizations and to the reduction of vulnerabilities.

1.3.3. *Vulnerability audit measures*

A computer network audit must include the following five categories:

– **preventive measures**: these include precautions taken to prevent the exploitation of a vulnerability, through the use of a firewall, physical locks and an administrative security strategy;

– **detective measures**: these include the retrieval of all information on intrusion into the network or system using system logs, intrusion prevention systems (IPS), anti-spoofing technologies and surveillance cameras;

– **corrective measures**: these include determining the cause of a security violation and then mitigating these effects through updating viruses or IPS;

– **recovery measures**: these enable system recovery after an incident;

– **deterrence measures**: these discourage persons who try to breach network security.

1.4. Exercises to test learning

ETL 1.–

1. What security term refers to property or data that is valuable to an organization?

a. A risk.
b. A resource.
c. A countermeasure.
d. A vulnerability.

2. Which of the following elements represents a physical security measure?

a. The policy of changing security agents.
b. The daily verification of equipment event logs.
c. Implementing electronic locks.
d. Putting in place access lists.

3. Which of the following is a reason for using firewalls?

a. Preventing unauthorized access of incoming or outgoing requests into a network.
b. Preventing damage to a computer in case of fire.
c. Facilitating the downloading of data from websites.
d. Detecting and cleaning viruses on a computer.

4. Which of the following respects confidentiality of information?

a. Discussing confidential data over the telephone.
b. Disclosing confidential information only to authorized persons.
c. Downloading confidential information on a shared website.
d. Sending confidential information to a colleague.

5. Match the type of hacker to their description.

Type of hacker	Description
1. Carders	a. Individuals who use their computer skills for financial gain or to harm individuals or organizations
2. Hacktivists	b. They usually contribute to the identification and repair of security weaknesses within a system.
3. Phreakers	c. They chiefly attack smartcard systems in order to exploit their vulnerabilities.
4. White Hat	d. Individuals who use their computer skills in order to bring about political or social change.
5. Black Hat	e. People who make use of telephone networks to place calls for free.

6. What kind of malicious program *may be described as a software that attaches itself to another program in order to execute an undesirable function*?

a. Virus.

b. Spyware.
c. Trojan.
d. Adware.
e. Worm.

7. What is the chief characteristic of worms?

a. A worm can run independently.
b. A worm must be activated by an event on the host system.
c. A worm disguises itself as a legitimate software.
d. Once installed on the host system, the worm does not replicate itself.

8. Classify the security measures into physical, logical or administrative.

Physical security	Logical security	Administrative security

- Defining the time of entry and exit from the computer room.
- Installing an incident protection system.
- Installing a firewall.
- Defining rules for an ACL.
- Recording all operations related to the handling of equipment.
- Installing surveillance cameras.
- Changing the location of an IPS system.
- Defining the length of encryption key.
- Mandating that all visitors wear badges.
- Putting in place the “least privilege” principle for accessing equipment.

9. Which of these describes spam?

a. Collecting information about a person or an organization without authorization.
b. Carrying out an unauthorized action such as modifying or deleting files.
c. Putting an unnecessary load on the system by copying files.
d. Sending unwanted masses in bulk.

10. Which of the following elements describes how a security breach must be reported?

a. Using the telephone.
b. Sending an email to the IT manager.

c. Using any means of communication.
d. Using the method given in the organization's security policy.

11. When you access a website, what icon in the address bar indicates that the site is secured?

a. An arrow.
b. A lock.
c. A star.
d. A shield.

12. Which of the following may intercept and use your messages for its own purposes?

a. The media.
b. Governments.
c. Advertising agencies.
d. Crime networks.
e. All of the above.

13. What is the main method that is used to protect against malware?

a. Using encrypted authentication technologies.
b. Installing an antivirus software on all host devices.
c. Blocking ICMP responses.
d. Deploying intrusion prevention systems across the network.

14. Which of the following describes a Trojan horse?

a. Malware embedded in a seemingly legitimate executable program.
b. Malware that sends extreme amounts of data in order to block a service.
c. An electronic dictionary used to obtain the network administrator's password.
d. A software used to convince users that their system has been infected by viruses.

ETL 2.–

1. What simple countermeasure can be used to mitigate a "**ping sweep**" attack?

a. Use encrypted authentication protocols.
b. Installing an antivirus on the hosts.

c. Deploying “anti-sniffer” software on all network devices.
d. Blocking ICMP echo responses on all network devices.

2. What network security countermeasures can be used to protect against DoS attacks? Choose two answers.

a. Installing antivirus software.
b. Putting in place IPS (intrusion protection systems).
c. Installing applications to authenticate users.
d. Installing anti-spoofing technology.
e. Putting in place data encryption technology.

3. How can you define a **“ping sweep”**?

a. This is a network scanning technique that can discover available hosts available in an IP address range.
b. This is an application that allows the capture of all network packets sent over a LAN.
c. This is a technique that examines a range of port numbers (TCP or UDP) available on a LAN.
d. This is a technique that can discover all the IP addresses available on a LAN using frame analysis.

4. What are the two characteristics of DoS attacks? Choose two answers.

a. They always precede access attacks.
b. They try to compromise the availability of a network, host, or application.
c. They are difficult to carry out and are only initiated by highly skilled attackers.
d. They always use the ICMP protocol.
e. They are easy to detect.

5. What happens in a spoofing attack?

a. An attacker modifies the data that transits over the network to access confidential information.
b. An attacker sends large amounts of network traffic to a device to make it inaccessible to users.
c. An attacker sends poorly formatted frames to a target device to cause it to malfunction.
d. An attacker sends malicious code to steal all data stored on a device.

6. What is the type of attack where an attacker uses an unauthorized access point to capture network traffic from a targeted user?

a. Attacks on the approval relationship.
b. Buffer overflow attack.
c. "Man-in-the-middle" attack.
d. DDoS attack

7. This is a type of network security attack in which the intruder takes control of communication between two entities in order to use it for his benefit.

a. Phishing.
b. Buffer overflow.
c. Pharming.
d. Hijacking.
e. SYN flood.

8. What happens in a buffer overflow attack?

a. An attacker redirects traffic from one website to another website.
b. Attackers send multiple queries from many connected computers in different geographic regions to render a service unavailable.
c. The attacker combines the characteristics of viruses, worms and other software to collect information about users.
d. The attacker tries to write additional data in the saturated memory of an equipment.

9. What is the risk of sharing too much information on social networking sites?

a. Phishing.
b. Buffer overflow.
c. Pharming.
d. Hijacking.
e. Ransom.

10. How many characters must be used to create a strong password?

a. Eight characters.
b. Sixteen characters.
c. The maximum number of characters possible.
d. The number of characters does not matter.

11. Strong passwords can be difficult to remember, what can you do to avoid forgetting them?

a. Use acronyms or phrases that are easy to remember.
b. Develop a password strategy.
c. Use password management software with encryption.
d. All of the above.

12. How long does it take for an attacker to detect a 10-character password?

a. Less than an hour.
b. Less than a week.
c. Less than a month.
d. It depends on many factors.

13. An attacker uses the **wireshark** tool to discover usernames and administrative passwords. What kind of network attack is this?

a. A “Man-in-the-middle” attack.
b. A DoS attack.
c. A reconnaissance attack.
d. A close attack.

2

Securing Network Devices

This chapter studies the following topics:

– the types of network traffic:
  - the management plane,
  - the control plane,
  - the data plane;
– securing the management plan:
  - securing passwords,
  - implementing connection restrictions,
  - securing access through control lines, VTY and auxiliaries,
  - assigning administrative roles: protecting access using privilege levels;
– protecting access through the management of "views" and "super-views":
  - securing configuration files and the system,
  - using automated security features;
– securing the control plan.

2.1. Types of network traffic

Cisco has categorized the different types of network traffic into different "planes" of communication. It has defined three such planes: the management plane, the control plane and the data plane.

Computer Network Security, First Edition. Ali Sadiqui.

– **the management plane**: this includes traffic used by a network administrator to configure network devices. It is generally made up of protocols, such as **Telnet, SSH** and **SNMP**;

– **the control plane**: this includes traffic between the network devices, transmitted to each other for discovery and/or for automatically configuring the network, such as the traffic of updating **routing protocols** or ARP protocol, for instance.

– **the data plane**: this is the actual traffic of end users in the network.

2.2. Securing the management plan

Securing the management plan includes, among others, the following:

– applying a secure password policy;

– securing console, VTY and auxiliary access;

– securing and archiving configurations;

– enabling logging to record all changes;

– using NTP (Network Time Protocol) to synchronize clocks on network devices.

2.3. Securing passwords

The following must be taken into account when applying a password policy:

– change passwords often;

– include alphanumeric characters, uppercase letters, lowercase letters, symbols and spaces in passwords;

– do not use passwords that will be easy to detect;

– encrypt all passwords;

– set a minimum of 10 characters for passwords;

Command	Description
Router(config)# **service password-encryption**	Encrypts all passwords.

Router(config)# **security passwords min-length** *length*	Applies a minimum length to all new passwords. Existing passwords will not be affected. The length can be from 1 to 16. It is recommended to have 10 or more characters.
Router(config)# ***enable algorithm-type {md5|scrypt|sha256|} secret*** *password*	Encrypts the password with your preferred mode, using the MD5 algorithm.

2.4. Implementing connection restrictions

2.4.1. *Configuring a login banner*

A banner is a feature used on Cisco systems that makes it possible to display a text message when a Cisco machine is being used. Cisco recommends that a legal notification banner be displayed in all interactive sessions. There are two main reasons for this:

– the banner must be used to alert intruders as well as users to the security policy that is applied, to which they are subject;

– the banner must be used to quickly identify the terminal being accessed.

Command	Description
banner exec	Defines a personalized banner that is displayed each time that the EXEC mode is initiated.
banner login	Defines a personalized banner that is displayed before the username and password are entered.
banner motd	Defines a personalized “message-of-the-day” banner.

2.4.2. *Configuring connection parameters*

Command	Description
login block-for X **attempts** Y **within** Z	This blocks access for “X” seconds after “Y” login attempts within “Z” seconds.
Login quiet-mode access-class {acl-name|acl-number}	Defines an ACL to authorize connections when access is blocked by the login block-for.

Login delay second	Sets up a delay between successive attempts to login.
login on-failure log [every login]	Creates an entry in the event log every time a connection attempt fails. This command may be customized.
login on-success log [every login]	Creates an entry in the event log every time there is a successful login attempt.

2.5. Securing access through console lines, VTY and auxiliaries

2.5.1. *Securing access through the console line and deactivating the auxiliary line*

Command	Description
Router(config)# **username** *name* **privilege** *level* **secret** *password*	Creates a database of local users and encrypt their passwords.
Router(config)# **line vty 0 4** Router(config-line)# **login local**	–
Router(config-line)#**exec-timeout** *minutes seconds*	Sets the inactivity period to a specific value. The default value is 10 minutes.
Router(config-line)# **line aux 0**	Access the “auxiliary line” mode.
Router(config-line)# **no exec**	Disables the auxiliary port.

2.5.2. *Securing VTY access with ssh*

Command	Description
Router(config)# **ip ssh version [1|2]**	It is recommended that version 2 be used.
Router(config)# **ip ssh time-out** *seconds*	Defines the number of seconds to wait before the SSH client responds during the negotiation phase. The default value is set to 120 seconds.
Router(config)# **ip ssh authentication-retries** *integer*	Limits the number of login attempts. The default value is 3.
Router(config)# **login block-for** *seconds* **attempts** *tries* **within** *Seconds*	Secures the VTY connection.
Router(config-line)# **transport input ssh**	Uniquely authorizes the SSH sessions.
Router(config-line)# **access-class** *ACL-number*	Applies an ACL to control access to the VTY line.

2.6. Allocation of administrative roles

2.6.1. *Privilege levels of the IOS system*

Privilege levels determine a user's ability to run certain commands on a router. By default, Cisco routers have three privilege levels, namely "zero", "user" and "privileged":

– **level zero**: this allows only five commands: *logout*, *enable*, *disable*, *help* et *exit*;

– **user level (level 1)**: this provides very limited read-only access to the router;

– **privileged level (level 15)**: this provides complete control over the router.

For added flexibility, Cisco routers can also be configured to use 16 different privilege levels (from 0 to 15).

2.6.2. *Configuring a privilege level*

Command	Description
Router(config)# **privilege** *mode* { **level** *level command* | **reset** *command* }	Allows the use of a command at a custom privilege level.
Router(config)# **enable secret level** *level password*	Assigns a password at the custom privilege level.
Router> **enable** *level*	Accesses the custom privilege level.

Example for the use of the commands

Command	Description
R1(config)# **privilege exec level 5 ping**	Allows permission to use the "ping" command at privilege level 5.
R1(config)# **privilege exec level 5 reload**	Allows permission to use the "reload" command at privilege level 5.
R1(config)# **enable secret level 5 tri**	Enables the configuration of an **Enable** password to access level 5.
R1> **enable 5** Password:	Allows user access with privilege 5. In addition to regular Level 1 commands, Level 5 users can also use the "**ping"** and "**reload"** commands.
R1# **show privilege** Current privilege level is 5	Privilege Level Verification.

NOTE.– When a command is defined for a privilege level, all commands whose syntax is a sub-set of this command are also defined at this level. For example, if the "**show ip route**" commands are automatically defined at level 10, the "**show**" and "**show ip**" commands are automatically defined at privilege level 10, unless these commands are individually defined at different levels.

2.6.3. *Setting a privilege level per user*

It is recommended that you configure a privilege level for each user. This is possible using the commands:

Router(config)#**username** *name* **privilege** *privilege-level* **secret** *password*

Example

```
Router(config)#username user1 privilege 5 secret
Ci$co012
Router(config)#username user2 privilege 12 secret
Ci$co013
```

2.6.4. *Setting a privilege level for console, VTY, and auxiliary line access*

By default, console, auxiliary, or VTY (virtual terminal lines) are assigned the privilege level 1. To modify the default privilege level of these access lines, proceed as follows:

Command	Description
R1(config)# **line console** 0	Access console (or auxiliary) port.
R1(config-line)#**privilege level** 4	Define a privilege level to use this mode.
R1(config)# **line vty** 0 4	Access VTY mode.
R1(config-line)#**privilege level** 10	Define a privilege level to use this mode.

NOTE.– You can now attempt Exercise 1.

2.6.5. *Securing access with the management of "views" and "super-views"*

2.6.5.1. *Introducing views*

Although users can control CLI access through privilege levels, these features do not provide network administrators with more options. CLI views provide more detailed access control capability, thereby improving security.

Views also have the following characteristics:

– a "AAA" model must first be activated (see Chapter 4);

– the user account may be on the local machine or on an external "AAA server";

– the access level given to a "view" takes priority over the "privilege" level;

– the user can use their privilege level if no "view" level has been assigned to them;

– only one "view" can be configured per user;

– when configuring "views", names and passwords are case-sensitive.

To configure a view, proceed as follows:

Command	Description
R1(config)# **parser view Vue1**	Creates a view named "View1".
R1(config-view)# **secret cisco123**	Assigns a password to the "view".
R1(config-view)# **commands exec include show**	This view can use all the "**show"** commands of the EXEC mode.
R1(config-view)# **commands exec include ping**	This view can use the "**ping"** command of the EXEC mode.
R1(config-view)# **commands exec exclude telnet**	This view cannot use the "**telnet"** command of the EXEC mode.
R1# **enable view Vew1** Password:	Connects to the view View to1 to verify it.

2.6.5.2. *Introduction to super-views*

A "super-view" is a collection of one or more "views" that allows administrators to easily define commands authorized per user.

Super-views have the following characters:

– a super-view cannot be directly configured by commands. It groups together the configuration of the set of views that constitute it;

– a view can be shared between several super-views;

– users connected to a super-view can access all commands configured in the views that are part of the super-view;

– deleting a super-view does not delete all views associated with this view.

To configure a view, proceed as follows:

Command	Description
Router(config)# **parser view** *Super-view-name* **Superview**	Creates a super-view in global configuration mode.
Router(config-view)# **secret** *password*	Assigns a password to the super-view.
Router(config-view)# **view** *view-name*	Assigns an existing view to the super-view.
Router# **username** *U1* **view** *Super-view-name*	Assigns a super-view to a user.
Router# **enable view** *view-name*	Connects to the super-view.
R1#**show parser view all**	Displays the list of super-views.

2.6.6. *Securing configuration files and the IOS system*

The Cisco IOS system provides the ability to create copies of the IOS image or of the configuration file. The archives are stored in "bootset" format, which is protected against deletion.

To archive the IOS image file or the configuration file, proceed as follows:

Command	Description
R1(config)# **secure boot-image**	Secures the IOS image by hiding it in Flash memory. This can only be seen in ROMMON mode.
R1(config)# **secure boot-config**	Secures the configuration file.
R1# **show secure bootset**	Displays the archive status of the Cisco IOS image and the configuration file.

To restore the IOS image file from a secured archive, following an incident, proceed as follows:

Command	Description
Router#**reload** Proceed with reload? [confirm]	Restarts the router.
rommon 1 > **dir flash:**	Enters the ROMMON mode and displays the available "bootset" files.
rommon 2 > **boot flash:c1841-advipservicesk9-mz.124-20.T1.bin**	Restarts the router using the indexed image.
Router(config)#**secure boot-config restore flash:.runcfg-20120701-090211.ar**	Restores the secured configuration.

2.6.7. *Using automated security features*

2.6.7.1. *Introduction*

Autosecure is a simple security configuration script that disables nonessential system services and allows you to configure the recommended security level**.** The **Autosecure** command starts a command line wizard in the same way as when using the installation program to configure a router.

2.6.7.2. *Configuration*

Router# *auto secure*

--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of the router but it will not make router absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure will be shown here. For more details of why and how this configuration is useful, and any possible side effects, please refer to Cisco documentation of AutoSecure.

At any prompt you may enter "?" for help.

Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure.

Is this router connected to internet? [no]:y

…

2.7. Securing the control plane

2.7.1. *Introduction*

Protecting the control plane requires protecting the packets that are generated or received by network devices, and that are used for discovering and using the network itself such as, for example, the traffic to update routing protocols (OSPF, EIGRP, RIP, etc.) as well as the traffic of the ICMP or ARP protocols.

The protection of this stream makes it possible to avoid injecting erroneous routing information to carry out attacks such as DoS or "Man-in-the-middle" attacks, among others.

It must be noted that the solutions proposed for this protection are only limited to securing the authentication of network elements and not the encryption of flows exchanged between devices.

2.7.2. *MD5 authentication*

There are two shared key authentication methods: plain text and MD5 message. Since plain text authentication is not very widely used, the MD5 method is often used to carry out the secured identification of network devices.

In this method, the key is never shared over the network. Instead, the key is combined with other parameters in order to compute a single value, called the hash value, which is used for authentication. (For more information, see Chapter 8.)

2.7.3. *Configuring OSPF protocol authentication*

OSPF supports two types of MD5, authentication configurations, namely per interface or per zone:

– to configure per interface MD5 authentication, proceed as follows:

Command	Description
router(config)#**interface** *interface-type* outer(config-if)#**ip ospf authentication message-digest**	Configures per interface authentication.
router(config-if)#**ip ospf message-digest-key** *key-id* **md5** *key*	Defines the authentication settings.

– to configure per zone MD5 authentication, proceed as follows:

Command	Description
router(config-router)#**area** *area-id* **authentication message-digest**	Configures per zone authentication.
router(config)#**interface** *interface-type* router(config-if)#**ip ospf message-digest-key** *key-id* **md5** *key*	Defines the authentication settings.

2.7.4. *Configuring EIGRP protocol authentication*

In order to configure the MD5 authentication for EIGRP, we must perform the following operations:

– configure a key chain;

– configure a key ID under the key chain;

– specify a password for the key ID;

– specify the acceptance and expiry time for the key (optional).

Proceed as follows:

Command	Description
router(config)#**key chain** *name-of-key-chain*	A key chain makes it possible to configure multiple keys that may then be used to carry out secured authentication. This makes it possible, for example, to configure a validity period for a given key or to use a series of rotary keys for limited periods of time in order to reduce the probability of having a compromised key.

router(config-keychain)#**key** *key-id*	Creates a key and enter the key configuration mode.
router(config-keychain-key)#**key-string** *key-string*	Configures a secret key.
router(config)#**interface** interface-type router(config-if)#**ip authentication key-chain eigrp** *as-number key-chain-name*	Configures the use of a chain of specific keys for authentication.
router(config-if)#**ip authentication mode eigrp** *as-number* **md5**	Configures the use of MD5 authentication.

NOTE .– EIGRP only supports MD5 authentication.

2.7.5. *Configuring RIP authentication*

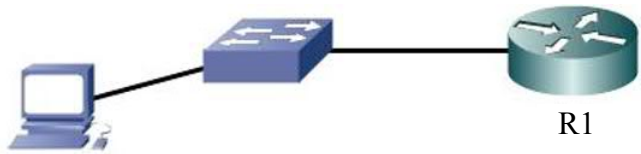
To configure MD5 authentication for RIP, proceed as follows:

Command	Description
router(config)#**key chain** *name-of-key-chain*	Creates the key chain.
router(config-keychain)#**key** *key-id*	Creates a key and enter the key configuration mode.
router(config-keychain-key)#**key-string** *key-string* router(config-keychain-key)#end	Configures a secret key.
router(config)#**interface** *interface-type* router(config-if)# **ip rip authentication key-chain** *key-chain-name*	Configures the use of a specific key chain for authentication.
router(config-if)#**ip rip authentication mode md5**	Configures the use of MD5 authentication.

2.8. *Exercises for application*

EXERCISE 1.–

Topology



Addressing table

Device	Interface	IP address / subnet mask	Operating system (GNS3)	Gateway
R1	G0/0	192.168.0.1/24	c2600-adventerprisek9-mz.124-1	–
PC1	NIC	192.168.0.2/24	Windows 7	192.168.0.1

Objectives

- Securing passwords.
- Putting in place connection restrictions.
- Assigning administrative roles.

Software to be used

- Packet Tracer.
- Or GNS3.

Part A: establishing the basic device configuration

1.1. Configure the host name as indicated in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

Part B: securing passwords

1. Set a minimum password length of 8 characters.

R1(config)# *security passwords min-length 8*

2. Configure the password for the privileged mode.

2.1. Define a word in clear text for this mode.

R1(config)# **enable password Ci$c0123**

2.2. Can you read this password from the "**show run**" command?

.....

2.3. Set an encrypted password for the privileged mode.

R1(config)# **enable secret Ci$c0ena**

2.4. Can you read this password from the "**show run**" command?

.....

3. Configure the console ports, auxiliary ports and virtual access lines.

3.1. Configure a console port password and set the inactivity interval to 5 minutes.

R1(config)# **line console 0**
R1(config-line)# **password Ci$c0con**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **login**
R1(config-line)# **logging synchronous**

3.2. Configure a password on the VTY lines and set the inactivity interval to 2 minutes.

R1(config)# **line vty 0 4**
R1(config-line)# **password Ci$c0vty**
R1(config-line)# **exec-timeout 2 0**
R1(config-line)# **login**

3.3. Disable the auxiliary port.

R1(config)# **line aux 0**
R1(config-line)# **no exec**

3.4. Access R1 from PC1 *via* Telnet.

PC1> **telnet 192.168.0.1**

4. Encrypt all passwords.

4.1. Use the "Password-Encryption Service" command to encrypt console and VTY passwords.

R1(config)# **service password-encryption**

4.2. Can you read console and VTY passwords from the "**show run**" command?

……..

Part C: putting in place connection restrictions

1. Configure up a login warning banner.

1.1. Configure a warning for unauthorized users using the "**motd**" command.

R1(config)# **banner motd $** *Access strictly forbidden for unauthorized persons $*
R1(config)# *exit*

1.2. From the command "**show run**", what has replaced the character "$" on the configuration file?

……..

Part D: securing access to VTY lines

1. Configure ssh connections.

Use the following options to configure ssh connections:

– domain name: **tri.local**;

– username: **sshadmin** with the password: **Ci$c0ssh**;

– the RSA encryption key is **1024 bit**;

– the SSH version used is version 2;

– the wait time is ***90s***;

– the number of login attempts is ***3***;

– authorize the ***ssh*** and ***telnet*** sessions.

2. Configure the connection parameters.

2.1. Use the "**login block-for**" command to configure the connection being stopped for ***60s*** if two connection attempts have failed within ***30s***.

R1(config)#**login block-for 60 attempts 2 within 30**

2.2. Use the "**Login delay**" command to configure a delay of 5 seconds between successive connection attempts.

R1(config)#**login delay 5 (GNS3)**

2.3. Add an entry to the event log each time a connection attempt was successful.

R1(config)#**login on-success log**

or:

R1(config)# **login on-success log every 1 (GNS3)**

3. Create two new user accounts with a secret password.

R1(config)# **username user01 secret user01pass**
R1(config)# **username user02 secret user02pass**

4. Connect to R1 from a telnet session.

4.1. Establish a **telnet** session to R1 from PC1.

PC1> **telnet 192.168.1.1**

4.2. Have you been asked to enter a user account? Why?

……..

4.3. Define the VTY lines to use the login accounts defined locally.

R1(config)# **line vty 0 4**
R1(config-line)# **login local**

4.4. Re-establish a **telnet** session to R1 from PC1.

PC1> **telnet 192.168.1.1**

4.5. Try to log in with a wrong user ID or password twice. What message is displayed on PC1 after the second failed attempt?

……..

4.6. What message is displayed on the R1 console after the second unsuccessful connection attempt?

……..

4.7. From PC1, try to establish another **telnet** session to R1 within 60 seconds. What message is displayed on PC1 after the Telnet connection attempt?

……..

4.8. What message was displayed on the R1 router after the Telnet connection attempt?

……..

5. Restrict the connection to R1 only through the use of ssh protocol.

5.1. Configure the VTY lines to use only the ssh protocol.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# exit
```

5.2. From PC1, try to establish another **ssh** and **telnet** session to R1.

Part E: assigning administrative roles

1. Configure the privilege levels.

1.1. Create a new user account with the following options:

– account name: "***SshUser***";

– encrypted password '***SshUpa $$***";

– privilege level ***10***.

R1 (config) # **username SshUser privilege 10 secret SshUpa $$**

1.2. Configure the password "**Priv10P $**" for privilege level 10.

R1(config)#**enable secret level 10** ***Priv10P$***

1.3. Allow the "**ping**" command for this privilege level in the ***exec*** mode.

R1(config)#**privilege exec level 10 ping**

1.4. Allow the "**ssh**" command for this privilege level in the ***exec*** mode.

R1(config)#**privilege exec level 10 ssh**

1.5. Allow all "**show IP**" commands for this privilege level in *exec mode*.

R1(config)#**privilege exec all level 10 show ip**

1.6. Create a new user account with the following options:

– username: "***TelUser***";

– encrypted password "***TelUpa $$***";

– privilege level ***12***.

R1(config)# **username TelUser privilege 12 secret *TelUpa$$***

1.7. Configure the password "***Priv12P $***" for privilege level 12.

R1(config)#**enable secret level 12 Priv12P$**

1.8. Allow the "**ping**" command for this privilege level in the ***exec*** mode.

R1(config)#**privilege exec level 12 ping**

1.9. Allow the "*telnet*" command for this privilege level in ***exec*** mode.

R1(config)#**privilege exec level 12 telnet**

1.10. Allow all *configuration mode* commands for this privilege level

R1(config)#***privilege exec all level 12 configure***

1.11. Follow the same steps to configure a privilege level 13 by endowing it with the following options:

– passwords **Priv13P$**;

– authorized commands: **telnet, traceroute, show** (all), **configure** (all).

1.12. Access privilege levels 10, 12 and 13 and test the configuration.

```
Router>enable 12
Password:
R1#?
Exec commands:
  <1-99>     Session number to resume
  connect    Open a terminal connection
  disable    Turn off privileged commands
```

disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
logout	Exit from the EXEC
no	Disable debugging information
ping	Send echo messages
resume	Resume an active network connection
telnet	Open a secure shell client connection
terminal	Set terminal line parameters

NOTE.–

– 0 (zero) privilege level commands are automatically added.

– All commands that are not desired for a particular privilege level must be individually assigned to other privilege levels.

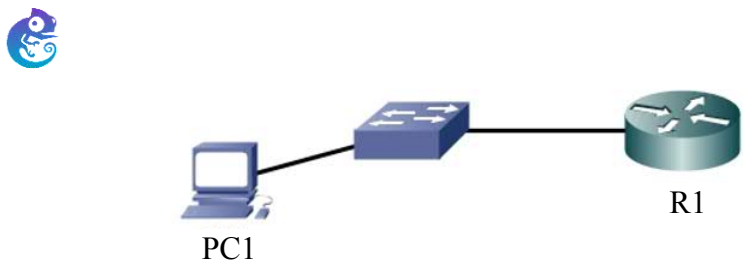
– Tests for results and privilege levels can also be carried out *via ssh using the TelUser* or *sshUser* accounts

1.13. Display the current privilege level.

```
R1# show privilege
```

EXERCISE 2.–

Topology



Addressing table

Device	Interface	IP address / subnet mask	Operating System	Gateway
R1	G0/0	192.168.0.1/24	c2600-adventerprisek9-mz.124-1	–
PC1	NIC	192.168.0.2/24	Windows 7 or higher	192.168.0.1

Objectives

– Securing passwords.

– Putting in place connection restrictions.

– Securing access by managing “views” and “super-views”.

– Securing the configuration files and IOS system.

– Using automated security features.

Software to be used

– GNS3.

Part A: establishing the basic device configuration

1.1. Configure the host name as indicated in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

Part B: securing passwords

1. Set a minimum password length of 8 characters.

R1(config)# **security passwords min-length 8**

2. Configure the password for the privileged mode.

R1(config)# *enable secret Ci$c0ena*

3. Configure the console ports, auxiliary ports and virtual access lines.

3.1. Configure a console port password and set the inactivity interval to 5 minutes.

R1(config)# **line console 0**
R1(config-line)# **password Ci$c0con**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **login**
R1(config-line)# **logging synchronous**

3.2. Configure a password on the VTY lines and set the inactivity interval to 2 minutes.

```
R1(config)# line vty 0 4
R1(config-line)# password Ci$c0vty
R1(config-line)# exec-timeout 2 0
R1(config-line)# login
```

3.3. Disable the auxiliary port.

```
R1(config)# line aux 0
R1(config-line)# no exec
```

3.4. Access the R1 router from PC1 using Telnet.

```
PC1> telnet 192.168.0.1
```

4. Encrypt all passwords.

```
R1(config)# service password-encryption
```

Part C: securing access to VTY lines with ssh

1. Configure ssh connections.

Use the following options to configure ssh connections:

- domain name: **tri.local**;
- username: *sshadmin* with the password: **Ci$c0ssh**;
- the RSA encryption key is ***1024 bits***;
- the SSH version used is ***version 2***;
- the wait time is ***90 seconds***;
- the number of login attempts is ***3***;
- authorize ***ssh*** and ***VTY*** sessions.

2. Configure the connection parameters.

Use the "**login block-for**" command to configure a connection block of ***60 seconds*** if there are two failed connection attempts within ***30 seconds***.

```
R1(config)#login block-for 60 attempts 2 within 30
```

Part D: securing access using "view" management

1. Create a new user account "User01" with the encrypted password" Us01pa$$".

R1(config)# **username User01 secret Us01pa$$**

2. Activeate the "AAA" on R1.

R1# *config terminal*
R1(config)# *aaa new-model*
R1(config)# *exit*

3. Create a "ViewRouter" view.

R1#**enable view**
Password: (*password enable*)
R1#conf t
R1(config)# **parser view ViewRouter**
R1(config-view)#

4. Assign the password "*ViewRouPs*" to this view.

R1(config-view)# **secret ViewRouPs**

5. For this view, allow all the "*show*" commands in *exec* mode.

R1(config-view)# **commands exec include all show**

6. Allow all commands in the *configure* mode.

R1(config-view)# **commands exec include all configure terminal**

7. Allow all commands for the mode in *router* mode.

R1(config-view)# **commands configure include all router**

8. Follow the same steps to create a "ViewTelnet" view and to endow it with the following options:

- Password ***ViewTelPs***;
- The authorized commands: **telnet, traceroute, show** (all).

9. Access the *ViewRouPs* view and test the configuration.

R1#**enable view *ViewRouPs***
Password:
Router#?
Exec commands:
configure Enter configuration mode
disable Turn off privileged commands
enable Turn on privileged commands
exit Exit from the EXEC
logout Exit from the EXEC
show Show running system information

For the **ViewTelnet** view:

R1#**enable view ViewTelnet**
Password:
R1#*?*
Exec commands:
disable Turn off privileged commands
enable Turn on privileged commands
exit Exit from the EXEC
logout Exit from the EXEC
show Show running system information
telnet Open a telnet connection
traceroute Trace route to destination

10. Display the list of views.

R1#**show parser view all**
Views/SuperViews Present in System:
ViewRouter
ViewTelnet
-------(*) represent superview-------

11. Assign "ViewRouter" to "User01".

R1(config)#**username User01 view ViewRouter**

12. Create a super-view, "*SuperView1*" with the password "*$uperView1*".

R1#**enable view**
Password: (*password enable*)
R1(config)# **parser view SuperView1 superview**
R1(config-view)#**secret $uperView1**

13. Assign the "ViewRouter" and "ViewTelnet" views to this super-views.

R1(config-view)# view **ViewRouter**
R1(config-view)# view **ViewTelnet**

14. Display the list of views.

R1#**show parser view all**
Views/SuperViews Present in System:
ViewRouter
ViewTelnet
SuperView1 *
-------(*) represent super-view-------

15. Assign "SuperView1" to "User01".

R1(config)#**username User01 view SuperView1**

Part E: securing configuration files and the IOS system

1. Display the content of the flash memory.

R1#**show flash**:
System flash directory:
File Length Name/status
3 50938004 **c2800nm-advipservicesk9-mz.124-15.T1.bin**
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[51193823 bytes used, 12822561 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write

2. Securing the IOS image file by hiding it in the Flash memory.

R1(config)# **secure boot-image**

3. Securing the current configuration file on the Flash memory.

R1(config)# **secure boot-config**

4. Once again display the content of the Flash memory.

R1#**show flash**:
System flash directory:
File Length Name/status
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[51193823 bytes used, 12822561 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write

5. Can you see the IOS image file? Why?

.....

6. Display the archive status of the Cisco IOS image and of the configuration file.

R1# **show secure bootset**
IOS image resilience version 12.4 activated at 00:01:50 UTC mon. march 1 1993
Secure archive **flash:/c2800nm-advipservicesk9-mz.124-15.T1.bin** type is image (elf) file size is 50938004 bytes, run size is 50938004 bytes
Runnable image, entry point 0x8000F000, run from ram
IOS configuration resilience version 12.4 activated at 00:02:03 UTC mon. march 1 1993
Secure archive **flash:/.runcfg-19930301-000203.ar** type is config configuration archive size 551 bytes

7. Configure the startup from ROMMON and restart the router.

R1(config)#**config-register 0x2100**
R1(config)#**exit**
R1#**reload**
Proceed with reload? [confirm]

8. Display the secured files available in ROMMON mode.

rommon 1 > *dir flash:*

File size Checksum File name
551 bytes (0x227) 0x0227 . **runcfg-19930301-000203.ar**
50938004 bytes (0x3094094) 0x439d **c2800nm-advipservicesk9-mz.124-15.T1.bin**
28282 bytes (0x6e7a) 0x6e7a sigdef-category.xml
227537 bytes (0x378d1) 0x78d4 sigdef-default.xml

9. Start up the router using the indexed image.

rommon 2 > **boot c2800nm-advipservicesk9-mz.124-15.T1.bin**

10. Restore the secured configuration to the archive found in Flash.

R1(config)#**secure boot-config restore flash:. runcfg-19930301-000203.ar**

Part F: using automated security features

1. Review the use of the "Autosecure" script.

.....

2. Start the "autosecure" script and follow the instructions.

R1#**auto secure**

3

Supervising a Computer Network

This chapter will focus on the following topics:

– implementing the Network Time Protocol (NTP):

  - introduction,

  - working,

  - configuration of the NTP;

– implementing the syslog protocol:

  - introduction,

  - working,

  - Syslog protocol configuration;

– implement the Simple Network Management Protocol (SNMP):

  - introduction,

  - working,

  - SNMP configuration.

3.1. Introduction

The management plane includes the traffic of network surveillance protocols, in this case the Syslog and the SNMP protocols. The NTP makes it possible to synchronize the time on network elements, guaranteeing the reliability of the data of the supervised elements.

Computer Network Security, First Edition. Ali Sadiqui.

3.2. Implementing an NTP server

3.2.1. *Introduction to the NTP*

The Network Time Protocol or NTP makes it possible to synchronize the local clock of a component of the computer network with that of a reference server (a public time server on the Internet on an internal time source).

3.2.2. *How the NTP works*

3.2.2.1. *The different NTP levels*

There are NTP servers at different levels (or strata) that correspond to different specifications. Atomic clocks make up Stratum 0 and are directly connected to the servers on Stratum 1; these servers are only accessible to servers on Stratum 2 or Stratum 3. In addition, some of these servers are freely accessible.

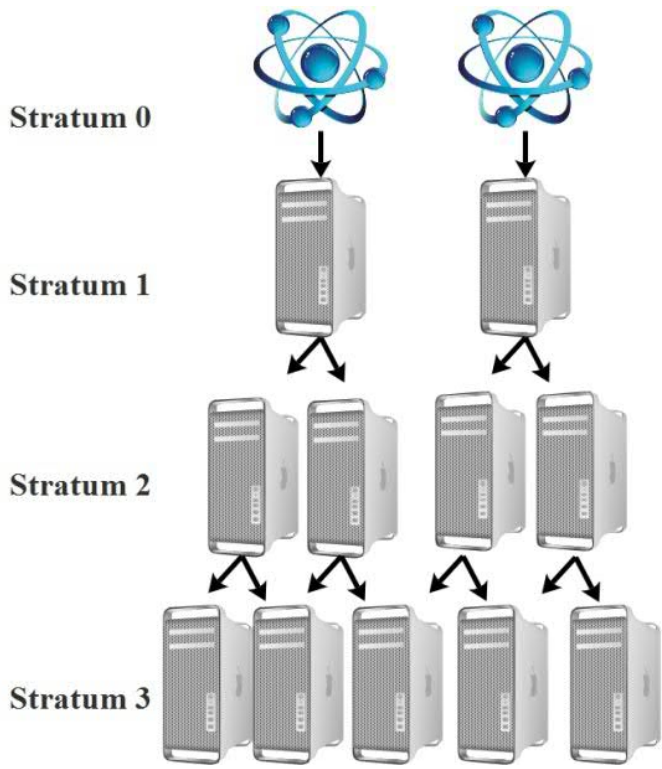


Figure 3.1. *The different NTP levels*

3.2.2.2. *The modes of communication of the NTP*

A client may use several modes to synchronize the clock:

– client / server mode: the client synchronizes with the server time;

– symmetric mode: priority is given to the station that has the shortest synchronization distance.

– multicast mode: This enables the client to get a response from multiple servers.

3.2.3. *NTP configuration*

3.2.3.1. *Configuring an NTP master*

To configure a router as an NTP master router, proceed as follows:

Command	Description
Router(config)# **ntp master** *stratum*	Configures the router so it becomes the NTP master. The number of strata is optional.
Router(config)# **ntp authenticate**	Activates NTP authentication.
Router(config)# **ntp authentication-key** *key-number* **md5** *key-value*	Defines the key ID and the NTP password and encrypts it using MD5.
Router(config)# **ntp trusted-key** *key-number*	Identifies the key on the master. In order to synchronize, an NTP client must provide the appropriate key ID and password.

3.2.3.2. *Configuring an NTP client*

To configure a router as an NTP client, we proceed as follows:

Command	Description
Client(config)# **ntp server** *ntp-server-address*	Defines the NTP master router with which the client will synchronize.
Client(config)# **ntp authentication-key** *key-number* **md5** *key-value*	Defines the key ID and the NTP password and encrypts it using MD5.
Client(config)# **ntp trusted-key** *key-number*	Identifies the trust key.

NOTE.– You can now attempt Exercise 3.

3.3. Implementing a Syslog server

3.3.1. *Introduction to the Syslog*

– The Syslog protocol is used to collect log messages generated by a device or an application. These messages may sometimes be the only way of clarifying why some equipment malfunctioned.

– Syslog messages are typically sent to:

- *console lines*;

- *terminal lines*;

- *a Syslog server*.

– A Syslog server makes it possible to carry out the following tasks:

- centralizing all log files for the different network devices: routers, switches, servers etc;

- archiving logs in a secured location where they can be processed;

- carrying out search and sort on the logs for ease of analysis.

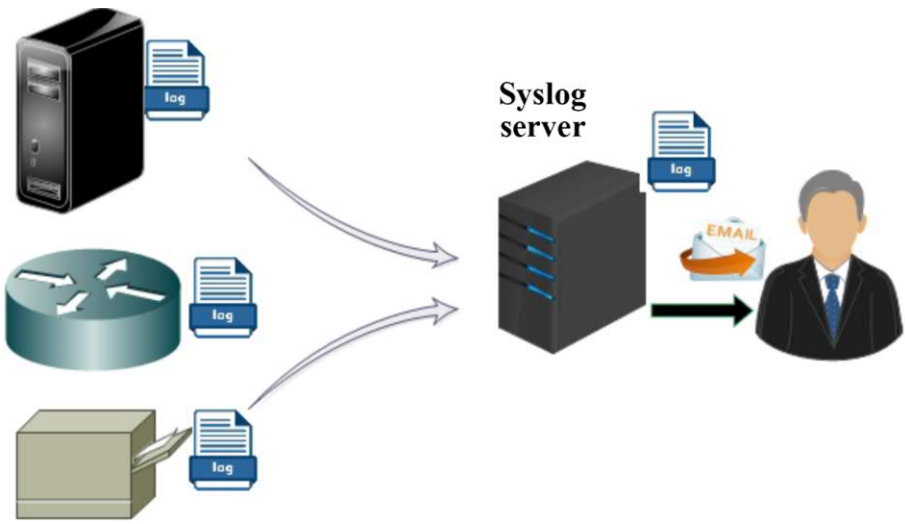


Figure 3.2. *Centralizing log files on a Syslog server*

3.3.2. *How Syslog works*

3.3.2.1. *Syslog severity levels*

A severity level indicates the nature of an error message. There are eight severity levels, from 0 to 7, with 0 (zero) being the most critical and 7 being the least critical. These levels are described below:

Code	Severity	Description
0	Emergencies	System inoperable.
1	Alerts	An immediate intervention is required.
2	Critical	Critical system error.
3	Errors	Operating errors.
4	Warnings	Warning (an error may occur if no action is taken).
5	Notifications	Normal event that must be reported.
6	Informative	For information.
7	Debug	Debugging message.

3.3.2.2. *The format of a Syslog message*

– A log in Syslog format provides the following information, in order: **Seq num:timestamp%FACILTY-SEVERITY-MNEMONIC: message:**

- **Seq num**: this indicates the serial number of an event. This information only appears if the **service sequence-numbers** command has been executed.

- **timestamp**: indicates the date and time at which the event took place. This information only appears if the **service timestamps** command has been run. It must be noted that this command is activated by default;

- **FACILTY**: indicates the component, protocol or process that generated the message. For instance, SYS for the operating system, IF for an interface, etc.;

- **SEVERITY**: a number, between 0 and 7, indicating the severity of the reported event;

- **MNEMONIC**: a code identifying the Syslog message;

- **message**: a description of the event that triggered the Syslog message.

– **Example**: the Syslog message to be analyzed is as follows.

```
39345: May 22 13:56:35.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
```

- **Seq num**: 39345;

- Timestamp: May 22 13:56:35.811;

- FACILTY: LINEPROTO;

- SEVERITY level: 5 (notification);

- MNEMONIC: UPDOWN;

- message **text**: Line protocol on Interface Serial0/0/1, changed state to down.

3.3.3. *Configuring a Syslog client*

To configure a router as a Syslog client, proceed as follows:

Command	Description
Router(config)# **service timestamps log datetime msec**	Activates the timestamps on the debug and log messages.
Router(config)# **logging host** [*ip-address* |*hostname*]	Identifies the address of the Syslog server or its host name.
Router(config)# **logging trap** *level*	Limits the messages sent to the Syslog function depending on the desired severity. The default value is 6 (0 to 6).
Router(config)# **logging on**	Activates the despatch of messages to be logged. The default value is “on”.
Router# **show logging**	Displays the logging status.

3.4. Implementing the Simple Network Management Protocol (SNMP)

3.4.1. *Introducing the SNMP*

– The Simple Network Management Protocol (SNMP) allows you to monitor, diagnose, and manage network equipment remotely.

– SNMP’s objectives can be summarized as follows:

- monitoring the performance of the network and knowing the overall state of the devices (active, inactive, partially operational, operational, network gridlocked etc.);

- detecting problems on the network and managing exceptional events (loss of a network link, an equipment suddenly ceasing to function etc.);

- configure equipment.

– The SNMP works on the application layer of the OSI model and uses the UDP protocol on port 162.

– Many software packages use SNMP to produce graphs that depict the evolution of network traffic or computer systems (Centreon, NetCrunch 5, MRTG, etc.).

3.4.2. *How SNMP works*

3.4.2.1. *The components of an SNMP system*

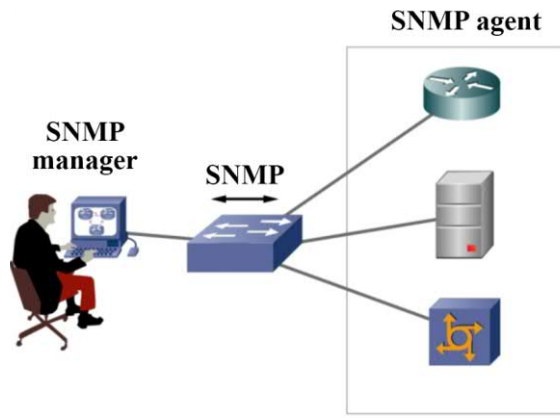


Figure 3.3. *The components of an SNMP system*

An SNMP system is made up of three components:

– **the SNMP manager**: this is a host that executes the SNMP management software. In most cases, this is a computer that is used to monitor the network;

– **the SNMP agent**: this is a software that runs on a network device (router, switch, server etc.) allowing it to be monitored;

– **the Management Information Base (MIB)**: This is a set of object collections managed by the SNMP agent. Each of these collections contains a certain number of variables that may be consulted or modified by the SNMP manager.

3.4.2.2. *The structure of the management information database*

The MIB has a hierarchical structure. Each object has an identifier (OID), which is a series of numbers separated by dots. This makes it possible to give it a unique identifier. For example, 1.3.6.1.2.1.2.2.1.2 is the OID for ifDescr. This value makes it possible to describe a network interface (e.g. FastEthernet0 / 0 on a Cisco router).

One of the best-known MIBs is MIB-II, described in RFC 1213. Figure 3.4 this depicts a part of the OID tree for MIB-II.

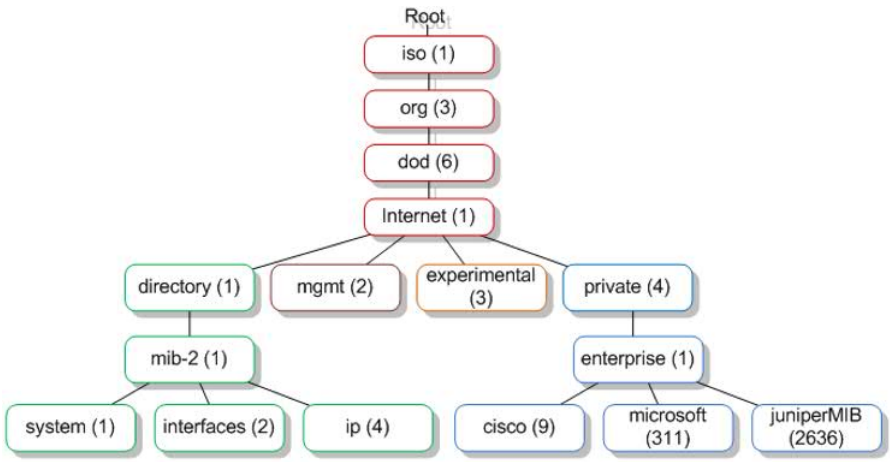


Figure 3.4. *The structure of the MIB-II. For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip*

3.4.2.3. *The different versions of SNMP*

SNMP comes in three main versions: SNMP version 1, SNMP version 2c, and SNMP version 3.

– **SNMPv1**: this is the original version and it is recommended that this not be used on a network as it has security gaps.

– **SNMPv2c**: this is an updated version of the initial protocol and offers certain improvements. However, the security that it provides is based only the community string, which is simply a plaintext password (non-encrypted), vulnerable to hacking. SNMPv2c has two types of community strings:

- **read-only (RO)**: this option provides read-only access to MIB objects. This is the recommended option for secured configuration;

- **read-write (RW)**: this option gives Read and Write access to MIB objects. This method provides the ability to modify the configuration of a network element.

– **SNMPv3**: this version has signification improvements, aimed at addressing the security vulnerabilities present in the earlier versions. The concept of the community chain gave way to new security features. However, even though this version offers better security, SNMPv2c still remains the most frequently used version.

3.4.2.4. *SNMP messages*

SNMP messages makes it possible to carry out the following operations:

– **searching for data related to the SNMP agent**: SNMP makes it possible to search for data that is linked to an agent using the messages:

- **GET**: this makes it possible to extract a value from a MIB element;

- **GetNext**: it makes it possible to retrieves the next value of the MIB element;

- GetBulk: (from version SNMPv2c and higher) this operation is used by the SNMP manager to efficiently retrieve large amounts of data from the SNMP agent;

– **the modification of data connected to the SNMP agent**: SNMP makes it possible to modify data connected to the agent by using the message:

- **SET**: this makes it possible to define a value for a MIB element;

– **Sending alerts and notifications**: SNMP also provides different notification (rerouting) operations that can be used by SNMP to warn the SNMP manager about an important event:

- **Trap**: this notification is used to send a message that does not need a read-receipt from the SNMP agent to the SNMP manager (NMS) when a preset condition is fulfilled;

- **Inform**: is used to send a message with read-receipt to the SNMP manager now. This feature was introduced in SNMPv2c to address the read-receipt problem when using Trap.

3.4.3. *SNMP configuration*

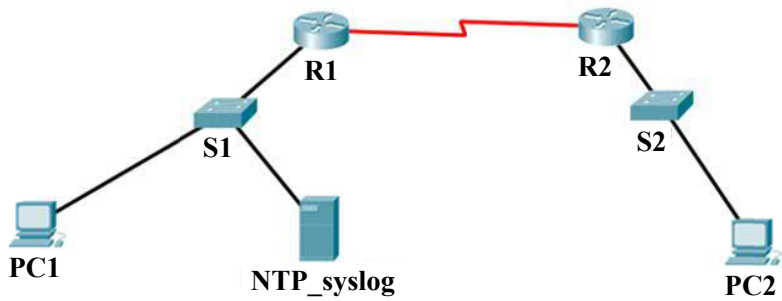
To configure a router to use SNMP, proceed as follows:

Command	Description
Router(config)**#snmp-server community** *name_community* [ro|rw]	Configures the "community" identifier and its access level (read only or read/write).
Router(config)#**snmp-server enable traps** *name_traps*	Activates an SNMP "trap".
Router(config)#**snmp-server host** *IP_address_of_agent name_community*	Supervises a device.
Router#**show snmp**	Verifies the SNMP configuration.

3.5. Exercises for application

EXERCISE 3.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet Mask	Gateway
R1	G0/0	192.168.0.1	/24	–
	S0/0	192.168.2.1	/30	–
R2	G0/0	192.168.1.1	/24	–
	S0/0	192.168.2.2	/30	–
PC1	NIC	192.168.0.2	/24	192.168.0.1
NTP_syslog Server	NIC	192.168.0.3	/24	192.168.0.1
PC2	NIC	192.168.1.2	/24	192.168.1.1

Objectives

– Securing passwords;

– Putting in place connection restrictions;

– Securing the control plane;

– Configuring the NTP;

– Configuring the syslog protocol.

Software to be used

– Packet Tracer.

Part A: set up the basic device configuration

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interfaces.

2. Configure routing with the OSPF protocol.

2.1. Enable OSPF on both routers using the value 1 as the process ID.

2.2. Set the RID value to 1.1.1.1 for R1 and 2.2.2.2 for R2.

2.3. Add all networks to zone 0.

2.4. Check the connectivity between PC1 and PC2.

2.5. Use the **"show ip ospf interface"** command to display the authentication type configured for the s0/0 interface.

R1# **show ip ospf interface s0/0**

Serial0 is up, line protocol is up
Internet Address 192.168.2.1/24, Area 0
…
…
Suppress hello for 0 neighbor(s)
Simple password authentication enabled

2.6. Explain the meaning of the underlined line:

.....

Part B: securing passwords

1. Set a minimum password length of 8 characters.

R1(config)# **security passwords min-length 8**

2. Configure the password for the privileged mode.

R1(config)# enable secret Ci$c0ena

3. Configure the console, auxiliary ports and virtual access lines.

3.1. Set a password for the console port and set the inactivity interval to 5 minutes.

R1(config)# **line console 0**
R1(config-line)# **password Ci$c0con**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **login**
R1(config-line)# **logging synchronous**

3.2. Set a password on the VTY lines and set the inactivity interval to 2 min.

R1(config)# **line vty 0 4**
R1(config-line)# **password Ci$c0vty**
R1(config-line)# **exec-timeout 2 0**
R1(config-line)# **login**

3.3. Disable the auxiliary port.

R1(config)# **line aux 0**
R1(config-line)# **no exec**

4. Encrypt all passwords.

R1(config)# **service password-encryption**

Part C: securing access to VTY lines using ssh

1. Configure the *ssh* connections.

Use the following options to configure the ssh connections:

– the domain name: ***tri.local***;

– the user name: ***sshadmin*** with the password: ***Ci$c0ssh***;

– the RSA encryption key is ***1024 bit***;

– the SSH version used is ***version 2***;

– the wait time is ***90 seconds***;

– the number of login attempts is ***3***;

– allow ***ssh*** and ***VTY*** sessions.

2. Configure the connection parameters.

Use the "**login block-for**" command to block the connection for ***60 seconds*** if two connection attempts have failed within 30s.

R1(config)#**login block-for 60 attempts 2 within 30**

Part D: securing the control plane

1. Review the definition of the control plane.

.....

2. Configure MD5 authentication for the OSPF protocol.

2.1. Activating MD5 authentication on R1.

R1(config)#**interface S0/0**
R1(config-if)#**ip ospf message-digest-key 1 md5 Ci$c0ospf**
R1(config-if)#**exit**
R1(config)#**router ospf 1**
R1(config-router)#**area 0 authentication message-digest**

2.2. Repeat the same configuration on R2.

2.3. Reuse the "show ip ospf interface" command to display the authentication type configured for the s0/0 interface.

```
R1# show ip ospf interface s0/0
  Serial0 is up, line protocol is up
    Internet Address 192.168.2.1/24, Area 0
  …
  …
    Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
  Youngest key id is 1
```

2.4. Explain the meaning of the underlined lines:

……

Part E: configuring the NTP

1. Revise the role of NTP.

……

2. Configuring the NTP server.

Activate the **NTP service** on the **NTP_Syslog** server.

3. Display the system date.

3.1. Display the system date on R1.

```
R1# show clock detail
```

3.2. Based on the output of the previous command, fill in the following table:

Date	
Time	
Time zone	
Time source	

4. Configure R1 and R2 as NTP clients of the NTP_Syslog Server.

```
R1(config)# ntp server 192.168.0.3
R1(config)# ntp update-calendar
```

5. Verify the NTP configuration on R1.

5.1. Display the system date on R1.

R1# **show clock detail**
19:50:47.118 UTC Fri Jul 6 2018
Time source is NTP

5.2. Display the NTP configuration settings.

R1#**show ntp status**
Clock is **synchronized**, stratum **2**, reference is **192.168.0.3**
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is DEBF99EF.000001B3 (10:58:55.435 UTC Wed Jul 4 2018)
clock offset is 0.00 msec, root delay is 0.00 msec (millisecond)
root dispersion is **0.02 msec**, peer dispersion is **0.02 msec**.

6. Configure the authentication on the NTP server.

Enable authentication with the following settings on the NTP__Syslog Server:

– Key: 1;

– password: **NTPpa00.**

7. Configure authentication on R1 and R2.

R1(config)# **ntp authenticate**
R1(config)# **ntp trusted-key 1**
R1(config)# **ntp authentication-key 1 md5 NTPpa00**

Part F: configuring the Syslog protocol

1. Revise the role of the syslog protocol.

.....

2. Activate the timestamps on the debug and log messages.

R1(config)# **service timestamps log datetime msec**

3. Identify the address of the Syslog server or its host name.

R1# **logging host 192.168.0.3**

4. Activate the despatch of messages to be logged.

R1(config)# **logging on**

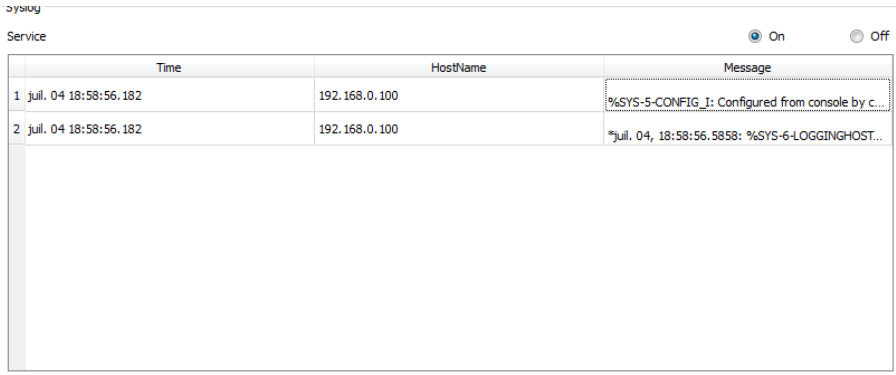
5. Set the severity level of the messages sent to the syslog server at the value 7 (debugging).

R1(config)# **logging trap debugging**

6. Display the logging status.

R1# **show logging**

7. Check that the messages have been properly saved on the Syslog server.



8. Analyze a message displayed on the NTP_Syslog Server.

Fill in the table based on the following message:

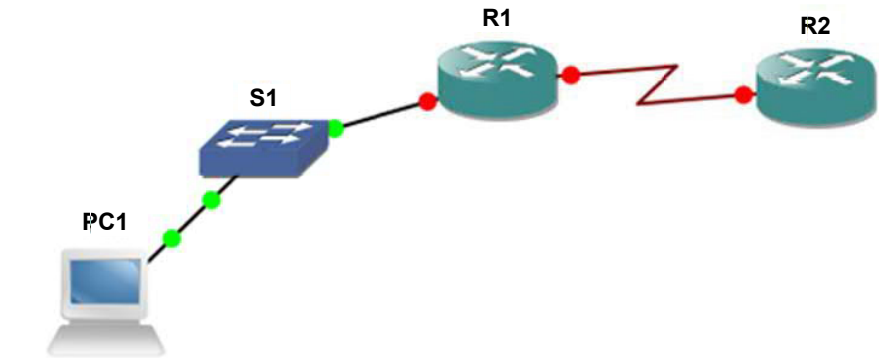
<189> *Mar 1 00:18:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up 192.168.100.1 04/07 22:27:59.280

Seq num	
Timestamp	

Facility	
Severity	
Mnemonic	
Message	

EXERCISE 4.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address / subnet mask	Operating system	Gateway
R1	G0/0	192.168.0.1/24	c2600-adventerprisek9-mz.124-1	–
	S0/0	192.168.2.1/30		–
R2	S0/0	192.168.2.2/30	c2600-adventerprisek9-mz.124-1	–
PC1	NIC	192.168.0.2/24	Windows 7 or later	192.168.0.1

Objectives

– Securing passwords;

– putting in place connection restrictions;

– securing the control plane;

– configuring the NTP;

– configuring the syslog protocol;

– configuring SNMP.

Software to be used

– GNS3.

Part A: setting up the basic device configuration.

1. Configure the basic settings on the devices.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. 128 Set the clock value to 128 000 for the serial interfaces.

2. Use EIGRP to configure the routing.

2.1. Enable EIGRP on both routers using the value 1 as SA ID.

2.2. Set the RID value to 1.1.1.1 for R1 and 2.2.2.2 for R2.

2.3. Add all the networks to EIGRP.

2.4. Test connectivity between all network elements.

Part B: securing passwords

1. Set a minimum password length of 8 characters.

2. Set the password "Ci$c0ena" for the privileged mode.

3. Configure the console, auxiliary ports and virtual access lines.

3.1. Set "**Ci$c0con**" as the console port password and set the inactivity interval to 5 minutes.

3.2. Set "**Ci$c0vty**" as the password on the VTY lines and set the inactivity interval to 2 minutes.

3.3. Disable the auxiliary port.

4. Encrypt all passwords.

```
R1(config)# service password-encryption
```

Part C: securing access to VTY lines using ssh

1. Configure ssh connections.

Use the following options to configure the ssh connections:

– the domain name: ***tri.local***;

– the user name: ***sshadmin*** with the password: ***Ci$c0ssh***;

– the RSA encryption key is ***1024 bit***;

– the SSH version used is ***version 2***;

– the wait time is ***90 seconds***;

– the number of login attempts is ***3***;

– allow the ***ssh*** and ***telnet*** sessions.

2. Configure the connection parameters.

Use the **"login block-for"** command to configure the connection being stopped for ***60 seconds*** if two connection attempts have failed within ***30 seconds***.

Part D: securing the control plane

1. Configure MD5 authentication for EIGRP.

1.1. Set the EIGRP key on R1.

```
R1(config)#key chain EIGRP-SECRET
R1(config-keychain)# key 1
R1(config-keychain-key)#  key-string Ci$eigrp
```

1.2. Repeat the same configuration on R2.

1.3. Set up EIGRP authentication.

```
R1(config)#interface s0/0
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP-SECRET
```

1.4. Repeat the same configuration on R2.

1.5. Check that an EIGRP neighborhood link is established between R1 and R2.

```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec)       (ms)      Cnt Num
0   192.168.2.2          s0/0                12 00:01:10 2000  5000  0  2
```

1.6. Ensure that authentication has been established using MD5 encryption:

```
R1#debug eigrp packets
```

*Mar 2 13:06:02.998: **EIGRP: received packet with MD5 authentication, key id = 1**

Part E: configuring the NTP

1. Set the R1 router system time.

R1# clock set *the_current_date*

2. Configurer R1 comme serveur NTP.

```
R1(config)# ntp master 5
```

NOTE.– The number 5 (the number of strata) indicates the number of NTP section that are remote from an authoritative time source.

3. Configuring R2 as an NTP client.

```
R2(config)# ntp server 192.168.2.1
R2(config)# ntp update-calendar
```

4. Checking the NTP configuration.

4.1. Display the system date on R2.

R2# **show clock detail**

4.2. Check the NTP association.

R2# **show ntp associations**

address ref clock st when poll reach delay offset disp

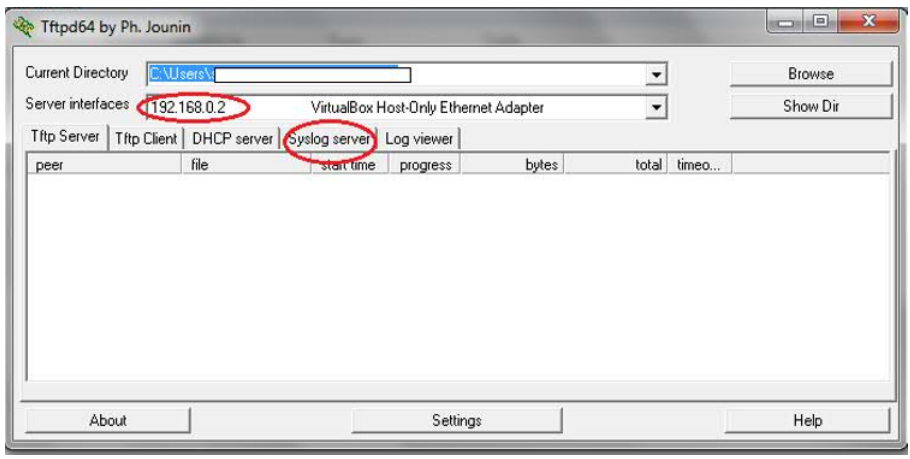
*~**192.168.2.1** 127.127.1.1 5 11 64 177 11.312 -0.018 4.298

* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

Part F: configuring the Syslog Protocol

1. Installing the Syslog server.

Download and install the tftpd32 server[1].



2. Activate the timestamps on the debug and log messages.

R1(config)# **service timestamps log datetime msec**

3. Configure the IP address of the syslog server.

R1# **logging host 192.168.0.1**

1 http://tftpd32.jounin.net/.

4. Activate the despatch of messages to be logged.

R1(config)# **logging on**

5. Display the logging status.

R1# **show logging**

…

No active filter modules.

Trap logging: **level informational**, 49 message lines logged

Logging to 192.168.0.1 (**udp port 514**, audit disabled,

link up),

6 message lines logged,

0 message lines rate-limited,

0 message lines dropped-by-MD,

…

6. Analyze the logging state.

From the output stat of the previous command, fill in the below table:

The IP address of the Syslog server	
The configured severity level	
The port used by the Syslog service	

7. Display the different severity levels available.

R1(config)#**logging trap?**

<0-7>	Logging severity level	
alerts	Immediate action needed	(severity=1)
critical	Critical conditions	(severity=2)
debugging	Debugging messages	(severity=7)
emergencies	System is unusable	(severity=0)
errors	Error conditions	(severity=3)
informational	Informational messages	(severity=6)
notifications	Normal but significant conditions	(severity=5)
warnings	Warning conditions	(severity=4)

8. Review the advantages and disadvantages of configuring the messages sent to the Syslog server, at severity level 7 (logging trap 7).

.....

9. Setting the severity level to 4 (warnings).

R1(config)# **logging trap warnings**

10. Disable and reactivate the S0/0 interface.

R1(config-if)#**shutdown**
R1(config-if)#**no shutdown**

11. Verify that the messages have been correctly recorded on the Syslog server.

<187>68: *Mar 1 00:13:28.837: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up 192.168. 0.1 07/07 22:35:33.869

Based on this message, fill in the following information:

Seq num	
Timestamp	
Facility	
Severity	
Mnemonic	
Message	

Part G: configuring SNMP

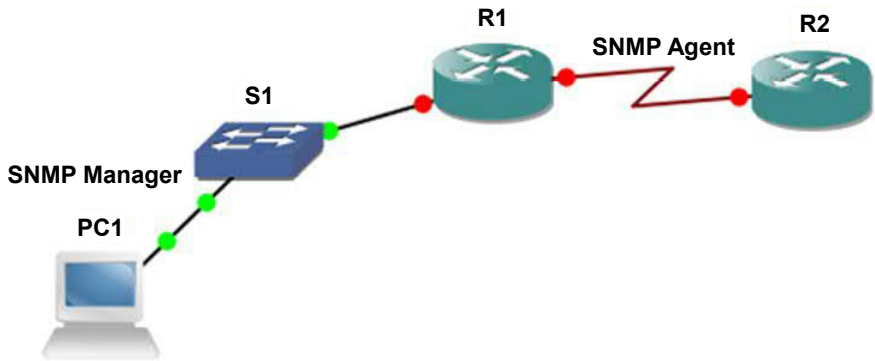
1. Review the role of SNMP.

.....

2. Review the components of an SNMP system.

.....

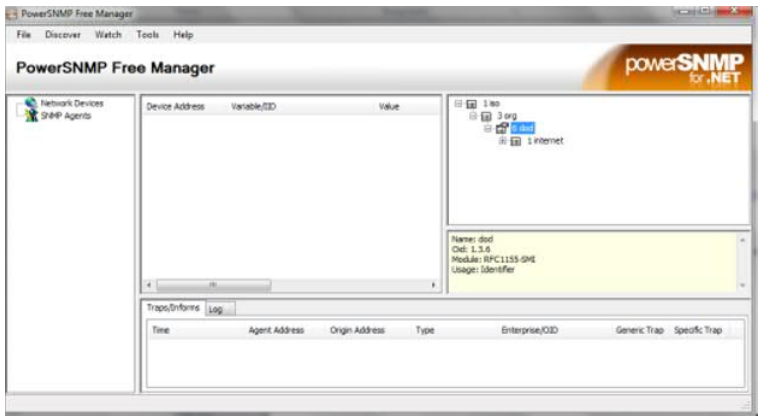
3. Configure the SNMP manager and SNMP agents.



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

3.1. Install the SNMP manager program.

Download and install the **PowerSNMP software**[2].



3.2. Configure the SNMP parameters on R1.

R1(config)#**snmp-server community tri rw**
R1(config)#**snmp-server host 192.168.0.2 tri**
R1(config)# **snmp-server host 192.168.0.2 version 2c tri**

3.3. Display the available "trap" list.

2 http://www.dart.com/snmp-free-manager.aspx.

R1(config)#**snmp-server enable traps?**

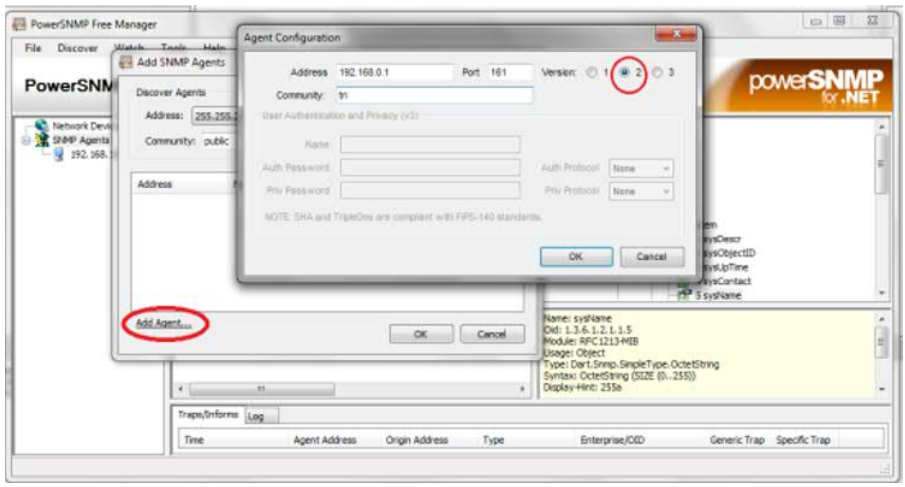
atm	Enable SNMP atm traps
bgp	Enable BGP traps
bstun	Enable SNMP BSTUN traps
bulkstat	Enable Data-Collection-MIB Collection notifications
cnpd	Enable NBAR Protocol Discovery traps
config	Enable SNMP config traps
config-copy	Enable SNMP config-copy traps
cpu	Allow cpu related traps
dial	Enable SNMP dial control traps

…

3.4. Enable all “traps” on the SNMP agent.

R1(config)#**snmp-server enable traps**

3.5. Link the SNMP manager to the SNMP agent.



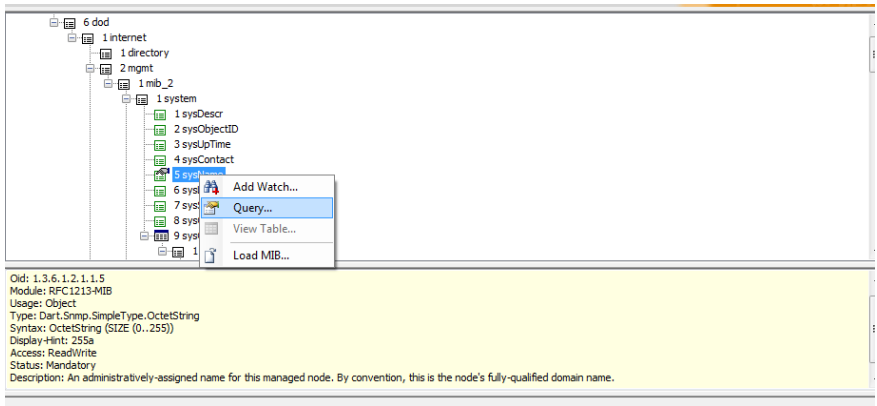
3.6. Review the definition of the following three SNMP messages:

– **SET:** .....

– **GET:** .....

– **Trap:** .....

3.7. Send a “**GET”** request to receive the “**sysName”** value of the SNMP agent.



3.8. Write the following elements for this SNMP request:

the OID value of this request: .....

– the type of access: .....

– the value of this SNMP request: .....

NOTE.– Not all elements of the basic version of the MIB, which is installed by default are accessible by the **"get"** command.

3.9. Display information related to a recorded trap.

4

Securing Access Using AAA

This chapter will focus on the following topics:

– AAA security strategy:

- authentication,
- authorization,
- traceability;

– the AAA authentication types:

- local AAA authentication,
- AAA authentication based on a server;

– AAA authorizations:

- introduction,
- configuring AAA authorizations;

– AAA traceability:

- introduction,
- configuration of AAA traceability.

4.1. Introduction

AAA (Authentication, Authorization, Accounting) is a security policy implemented in some Cisco routers that performs three functions: authentication, authorization, and traceability. With:

Computer Network Security, First Edition. Ali Sadiqui.

– **authentication**: this consists of verifying the identity of the user or the machine;

– **authorization**: this consists of determining user rights on different resources;

– **traceability**: this consists of preserving information on the use of resources by the user.

AAA users may be created on a local host on the router or the switch, just as they can be created on an external server (which has the added advantage of centralizing access configuration).

4.2. AAA authentication

4.2.1. *Local AAA authentication*

Local authentication enables simple and quick management of user accounts. However, this proves inefficient when there is a large number of users.

The local authentication process can be summarized as follows:

1) the user establishes a connection with the router;

2) the router prompts the users to enter a username and password. The user authentication is then validated from a local database.

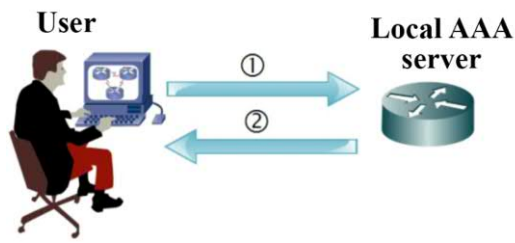


Figure 4.1. *The local AAA authentication process*

To configure a router to use local AAA authentication, proceed as follows:

Command	Description
Router(config)# **username** *username* **privilege** *level* **secret** *password*	Creates a user in the local database and allocates a password to the user.
Router(config)# **aaa new-model**	Creates a new AAA model.

Router(config)# **aaa authentication login** { **default** | *list-name* } { *method1* [*method2* ...]}	Defines the authentication method to be used when accessing **console**, **VTY** or **aux** lines. The authentication method includes **local**, **local-case** and **Enable**.
Router(config)# **aaa authentication username-prompt** *text-string*	Replace the "**Username**" message with another message. If this contains spaces, they must be surrounded by double quotation marks.
Router(config)# **aaa authentication password-prompt** *text-string*	Replace the "**Password**" message with other text.
Router(config)# **aaa local authentication attempts max-fail** *number*	Secure the AAA accounts by locking accounts that have exceeded the pre-defined maximum number of failed attempts. The account remains locked until it is activated by an administrator using the command: **clear aaa local user lockout**.

4.2.2. *AAA authentication based on a server*

AAA users can reside on an external server. It is possible to use two types of servers based on the Radius or Tacacs + protocols:

– **the radius protocol**: an open protocol based on the UDP;

– **the Tacacs+ protocol**: a proprietary protocol based on TCP.

The differences between the two protocols include:

	Tacacs+	**Radius s**
Protocol	TCP on port 49	UDP on ports: – 1812 or 1645 for authentication and authorization; – 1813 or 1646 for traceability
Encryption	Encrypts all information	Only encrypts the passwords
AAA architecture	The AAA strategies are independent	Combines authentication and traceability
Challenge/response	Bidirectional	Unidirectional
Proprietor	Cisco system	Open source

AAA strategies enable the integration of users in the "Active directory" database in order to benefit from centralized management.

Authentication using a server may be summarized as follows:

1) the user establishes a connection with the router via a username and password;

2) the router passes along the user's identifiers to an external AAA server;

3) the AAA server validates the data;

4) the router sends back the result of the connection and validates the data.

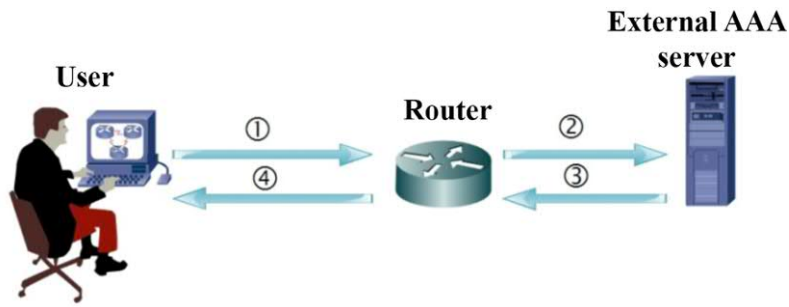


Figure 4.2. *Authentication based on a server*

In order to configure a router to use AAA authentication on a server, proceed as follows:

Command	Description
R1(config)# **tacacs-server host** { *host-name* | *host-ip-address* } [**key** *string*] [**port** [*integer*]] [**single-connection**] [**timeout** [*seconds*]]	Configures the IP address (or hostname) of the TACACS+ server. The other parameters are optional.
R1(config)# **radius-server host** { *host-name* | *host-ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**key** *password*]	Configures the IP address (or hostname) of the RADIUS server. The other parameters are optional.

Optionally, servers may be grouped together to accelerate the process of authenticating users or to ensure load redundancy or balancing.

Command	Description
Router(config)# **aaa group server radius** *group-name*	Groups existing RADIUS host servers and uses them.
Router(config-sg-radius)# **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]	Configures the IP address of the RADIUS server for the group server.
Router(config)# **aaa group server tacacs+** *group-name*	Groups together the existing TACACS+ host servers.
Router(config-sg-tacacs+)# **server** *server-ip*	Configures the IP address of the TACACS+ server for the group server.

4.3. AAA authorizations

AAA authorization strategies define the access parameters for a user on a router or in a network.

Command	Description
Router(config)# **aaa authorization** { **exec** | **network** | **commands** *level* } { **default** | *list-name* } { *method1* [*method2* ...]}	Defines the authorization strategy to be used at the time the following modes are accessed: – **exec**, which allows a user to run a command in this mode; – **network**, which sets authorized access requests related to the network, such as PPP; – **commands**, which sets authorized commands for a specific level of privilege.

4.4. AAA traceability

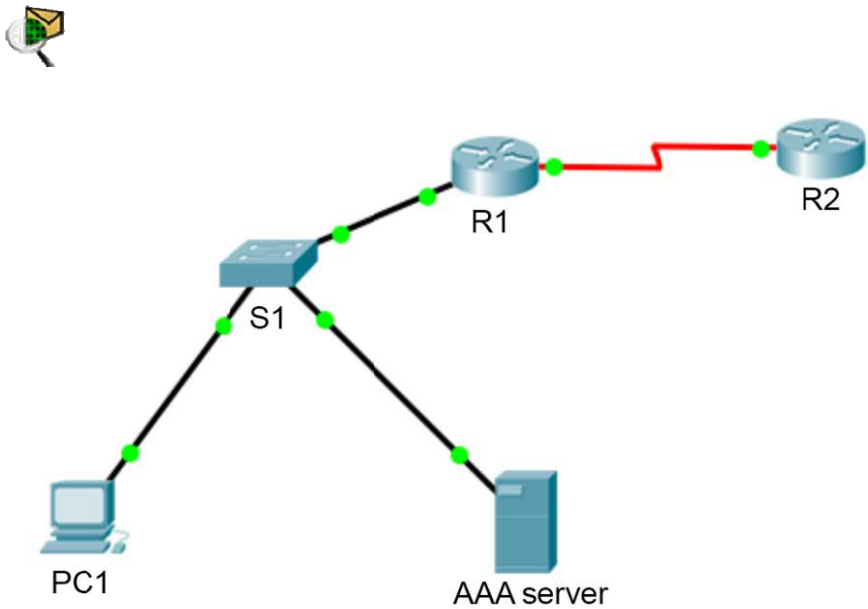
AAA traceability makes it possible to log all actions carried out by a user in the events log. By doing this, it will be possible to consult the logs to verify user actions or to identify the author of a given action in order to rapidly intervene in the case of a problem. AAA supports six different types of traceability: **system**, **network**, **exec**, **commands**, **connection** and **resource**.

Command	Description
Router(config)# **aaa accounting** { **system** | **network** | **exec** | **commands** *level* } { **default** | *list-name* } { **start-stop** | **wait-start** | **stop-only** | **none** } [*method1* [*method2*]]	Defines the traceability method used for a specific service. It follows up on the requested services: – **system**: preserves a trace of all the actions carried out at the level of the system; – **network**: preserves a trace of all the actions carried out at the level of the network, such as PPP; – **exec**: preserves a trace of all the actions carried out at the "**exec**" level; – **commands**: carries out a follow-up on all the commands at a specific privilege level.

4.5. Exercises for application

EXERCISE 5.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	G0/0	192.168.0.1	/24	–
	S0/0	192.168.2.1	/30	–
R2	S0/0	192.168.2.2	/30	–
PC1	NIC	192.168.0.2	/24	192.168.0.1
AAA server	NIC	192.168.0.3	/24	192.168.0.1

Objectives

– Securing passwords;

– securing the control plane;

– securing management access using AAA.

Software to be used

Packet tracer.

Part A: setting up the basic device configuration.

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interfaces.

2. Use EIGRP to configure the routing.

2.1. Enable EIGRP on both routers using the value 1 as SA ID.

2.2. Set the RID value to 1.1.1.1 for R1 and 2.2.2.2 for R2.

2.3. Add all the networks to EIGRP.

2.4. Test connectivity between all network elements.

Part B: securing passwords

1. Set a minimum password length of 8 characters.

2. Set the password "Ci$c0ena" for the privileged mode.

3. Configure the console, auxiliary ports and virtual access lines.

3.1. Set "Ci$c0con" as the console port password and set the inactivity interval to 5 minutes.

3.2. Set the password "**Ci$c0vty**" on the VTY lines and set the inactivity interval to 2 minutes.

3.3. Disable the auxiliary port.

4. Encrypt all passwords.

```
R1(config)# service password-encryption
```

Part C: securing the control plane

Configure MD5 authentication for EIGRP.

1. Configure the EIGRP key on R1.

```
R1(config)#key chain EIGRP-SECRET
R1(config-keychain)# key 1
R1(config-keychain-key)#  key-string Ci$eigrp
```

2. Repeat the same configuration on R2.

3. Implement EIGRP authentication.

```
R1(config)#interface s0/0
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP-SECRET
```

4. Repeat the same configuration on R2.

5. Verify that a neighborhood EIGRP link has been established between R1 and R2.

```
R1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q
Seq
(sec)         (ms)       Cnt Num
0   192.168.2.2             s0/0            12 00:01:10 2000  5000  0  2
```

6. Verify that the authentication has been carried out using MD5 encryption.

```
R1#debug eigrp packets
 *Mar 2 13:06:02.998: EIGRP: received packet with MD5
authentication, key id = 1
```

Part D: securing management access using AAA

1. Review the advantages of managing access using AAA.

.....

2. Configure the local AAA authentication for the access console using the local database.

2.1. Activate the AAA service.

```
R1(config)# aaa new-model
```

2.2. Configure the authentication method to only use the local database.

```
R1(config)# aaa authentication login default local none
```

2.3. Create an **Admin** user with the password "**@dmin012**".

```
R1(config)#username Admin privilege 15 secret @dmin012
R1(config)#exit
R1#exit
```

2.4. Connect to the Admin account, via Telnet.

3. Create an AAA authentication profile for Telnet using the local database.

3.1. Delete the configuration for the older authentication mode.

R1(config)# **no aaa authentication login default local none**

3.2. Create an authentication name for Telnet access to the router.

R1(config)# **aaa authentication login TELNET_CON local**

NOTE.– The "**local**" parameter is added to use the local database in case there is a connection failure with the "AAA" server.

3.3. Define the authentication name for Telnet access.

R1(config)# line vty 0 4
R1(config-line)# **login authentication TELNET_CON**

3.4. Connect to the Admin account via the console.

PC1> telnet 192.168.0.1

3.5. How is it possible to still connect to R1?

.....

4. Configure authentication using a local AAA server.

4.1. On the AAA server:

Activate the AAA service;

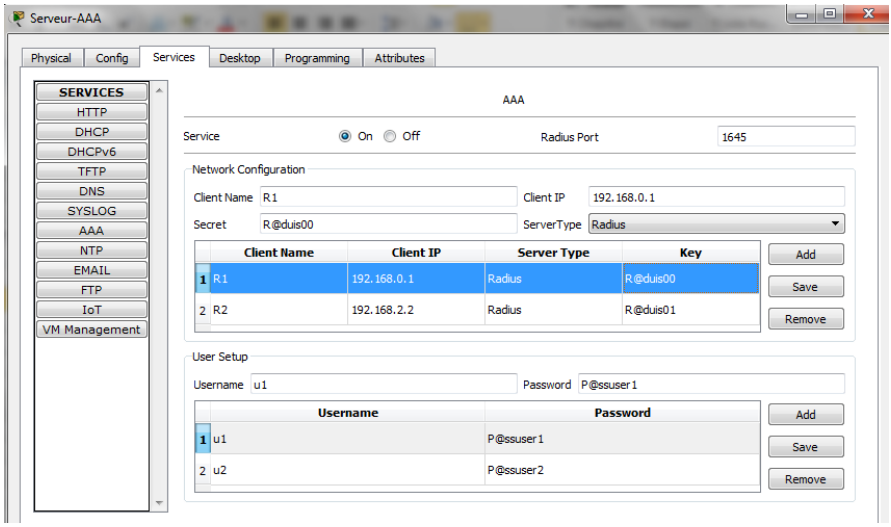
Create a client, "**R1**" with the password "**R@duis00**";

Create a client, "**R2**" with the password "**R@duis01**";

Define the IP address **192.168.0.1** for client **R1** and **192.168.2.2** for client **R2**;

Set the type of AAA server to **Raduis**;

Create two users: **u1** with the password "**P@ssuser1**" and **u2** with the password "**P@ssuser2**".



4.2. Configure the routers to use the AAA server.

R1(config)# **radius-server host 192.168.0.3 key R@duis00**

R1(config)# **aaa authentication login TELNET_CON group radius local**

4.3. Connect to R1, via Telnet, using the Admin account.

PC1> **telnet 192.168.0.1**

4.4. Why is it no longer possible to connect to R1?

.....

4.5. Connect to R1, via Telnet, using the account u1.

4.6. Configure R2 to use AAA authentication.

R2(config)# **radius-server host 192.168.0.3 key R@duis01**

R2(config)# **aaa authentication login TELNET_CON group radius local**

R2(config)# **line vty 0 4**

R2(config-line)# **login authentication TELNET_CON**

4.7. Connect to R2, via Telnet, using the same account, u1.

PC1> **telnet 192.168.2.2**

4.8. What is the advantage of using an AAA server?

.....

NOTE.– In this exercise, we limit ourselves to the AAA authentication. However, the reader can learn more by adding the parts related to AAA authorizations and AAA traceability using, for example, the Cisco Secure ACS server.

5

Using Firewalls

This chapter will focus on the following topics:

– the role a firewall plays;

– the types of firewalls:

  - NAT firewall,

  - packet-filtering firewall,

  - stateful firewall,

  - application firewall;

– setting up a firewall;

– different firewall strategies;

– ACL-based firewalls:

  - IPv4 ACLs,

  - IPv6 ACLs;

– zone-based firewalls:

  - the types of security zones in a network,

  - rules applied to inter-zone traffic,

  - configuring a ZFW.

Computer Network Security, First Edition. Ali Sadiqui.

5.1. Introducing firewalls

A firewall is a software or hardware system put in place between a reliable network and an unreliable one. The main purpose of putting in place a firewall is to filter out and prevent unwanted traffic from crossing the firewall barrier. In order to do this, a firewall must comply with the following recommendations:

– it must be resistant to attacks;

– it must be the only transit point between two networks;

– it must ensure that the organization's access control strategy is applied.

5.2. Types of firewalls

There are different kinds of firewalls. Some of these are:

– **NAT firewall**: this hides a private IP address by translating it into a public IP address;

– **packet-filtering firewall**: this makes it possible to filter packets from Layers 3 or 4 of the OSI model. This kind of firewall is simple to configure but is also vulnerable to identity-theft attacks;

– **stateful firewall**: this carries out the same function as a packet-filtering firewall and also keeps track of the state of network connections (i.e. the TCP and UDP sequence numbers), thereby making it more secure;

– **application firewall (proxy firewall)**: This is usually a server that carries out this type of filtering of information located in layers 3, 4, 5 and 7.

5.3. Setting up a firewall

The best practices for setting up a firewall include:

– place the firewall at the security boundaries to separate different domains of communication;

– only allow the traffic of necessary services;

– monitor firewall logs;

– put in place a variety of firewall technologies in order to provide comprehensive multilayer access control;

– do not rely on only a firewall for security;

– ensure that physical access to the firewall is monitored;

– practice change management for firewall configuration.

5.4. Different firewall strategies

In general, access rules are implemented using an ACLs (ACL). When you define access rules, you can use several criteria as your starting point:

– **rules based on the service**: these determine the type of services that may be accessed by incoming or outgoing traffic. The firewall may filter traffic depending on the IP address and the TCP port number.

– **rules based on direction**: these determine the direction in which requests towards a specific service may be initiated and authorized.

– **rules based on behavior**: these control the manner in which specific services will be used. For example, the firewall may filter emails to eliminate spam.

5.5. ACL-based firewalls

5.5.1. *Introduction*

An Access Control List is a sequential set of authorization or denial instructions that are applied to addresses or higher layer protocols. ACLs make it possible to control incoming or outgoing traffic in a network.

5.5.2. *The location of ACLs*

ACLs may be put in place in two directions:

– **incoming ACLs**: the router processes incoming packets before sending them onto the output interface.

– **outgoing ACLs**: the router directs incoming packets towards the output interface and then processes them by applying outgoing ACLs.

5.5.3. *IPv4 ACLs*

Routers support two types of IPv ACLs.

– **Standard ACLs:**

- filter IP packets based only the source IP address;

- can be numbered or named;

- the range of valid numbers extends from 1–99 and 130–1999.

– **Extended ACLs:**

- filter IP packets based on the source and destination IP addresses, the source and destination UDP and TCP ports and the ICMP message types etc.;

- can be numbered or named;

- valid number ranges include 100–199 and 2000–2699.

– To configure standard ACLs, proceed as follows:

Command	Description
R1(config)# access-list *number* [**deny**|**permit**] **source** [*generic mask*]	Creates a numbered standard ACL.
R1(config)# ip access-list standard *name_ACL*	Creates a standard named ACL.
R1(Config-if)# ip access-group [*number* | *name* [**in** | **out**]]	Activates an ACL on an interface.

– To configure extended ACLs, proceed as follows:

Command	Description
R1Config)# access-list *number* { **deny** | **permit** } **protocol source** [*generic mask*] **destination** [*generic mask*]	Creates a numbered extended ACL.
R1(config)# ip access-list extended *name_ACL*	Create a named extended ACL.
R1 (config-if)# ip access-group {*number*|*name*} {in|out}	Activates an ACL on an interface.

5.5.4. *IPv6 ACLs*

– The list of IPv6 Access Control Lists are similar to IPv4 Access Control Lists, with some specific features presented below:

IPv4 Access Control Lists	IPv6 Access Control Lists
Standard Numbered Named **Extended** Numbered Named	**Named only** Function as IPv4 extended ACL access control lists.
Use a generic mask	No generic mask.
The IP access-group command makes it possible to apply an IPv access control list to an IPv4 interface	IPv6 uses the ipv6 traffic-filter command to perform the same task on IPv6 interfaces.
There is an implicit deny any or deny any instruction	**permit icmp any any nd-na** **permit icmp any any nd-ns**

– To configure IPv6, ACLs, proceed as follows:

Command	Description
R1(config)# ipv6 access-list *name*	Creates an IPv6 ACL.
R1(config-ipv6-acl) # {**deny**|**permit**} **protocole** *ipv6-source/CIDR* [{**eq**|**neq**|**gt**|**lt**|**range**} **port**] *ipv6-destination/CIDR* [{**eq**|**neq**|**gt**|**lt**|**range**} **port**]	Configures an IPv6 ACL.
R1(config)#interface *type number* **R1(config-if)#ipv6 traffic-filte** *name*_ACL {**in**|**out**}	Activates an IPv6 ACL on an interface.

5.5.5. *ACL recommendation*

When implementing ACLs it is important to consider the following points:

– the instructions in an ACL are processed in sequential order, taking into account their order;

– the most specific instructions must be placed in the first lines in an ACL;

– by default, new instructions in an existing ACL are added to the last lines;

– it must be ensured that the last instruction is a refusal of any other unspecified traffic;

– only a single ACL is authorized per interface, per protocol or per direction;

– the packets generated by the routers are not processed by outgoing ACLs;

– standard ACLs must be placed as close to the destination as possible;

– extended ACLs must be placed as close to the source as possible.

NOTE.– You can now attempt Exercise 6.

5.6. Zone-based firewalls

5.6.1. *Introduction*

A Zone-based Policy Firewall (ZFW) is a firewall solution based on an IOS router. This allows a network to be protected against external threats based on the separation of the different network types into distinct zones and enables the specification of the kind of traffic that may pass from one zone to another. One of the chief advantages of this solution includes the simplicity of defining access strategies.

5.6.2. *Types of security zones in a network*

In general, there are three kind of security zones that may be applied to an organization's network:

– **the internal zone**: this is the production network in an organization. This is a zone whose access must be strictly controlled. Direct, uncontrolled access from another zone must not be permitted;

– **the external zone**: as a general rule, this corresponds to the Internet. This is a non-secured zone which presents a constant source of danger to the organization's internal network;

– **the DMZ (demilitarized) zone:** this is a zone that is used to enable Internet-based access to certain servers (web messaging services etc.) while avoiding any direction connection with the internal network. This zone presents several security breach risks and requires strict access control for the following traffic:

- incoming traffic from the internet to the hosts in the DMZ zone;

- outgoing traffic from the hosts in the DMZ zone towards the internet;

- incoming traffic from the internal network to the hosts in the DMZ zone;

- outgoing traffic from the hosts in the DMZ zone towards the internal network.

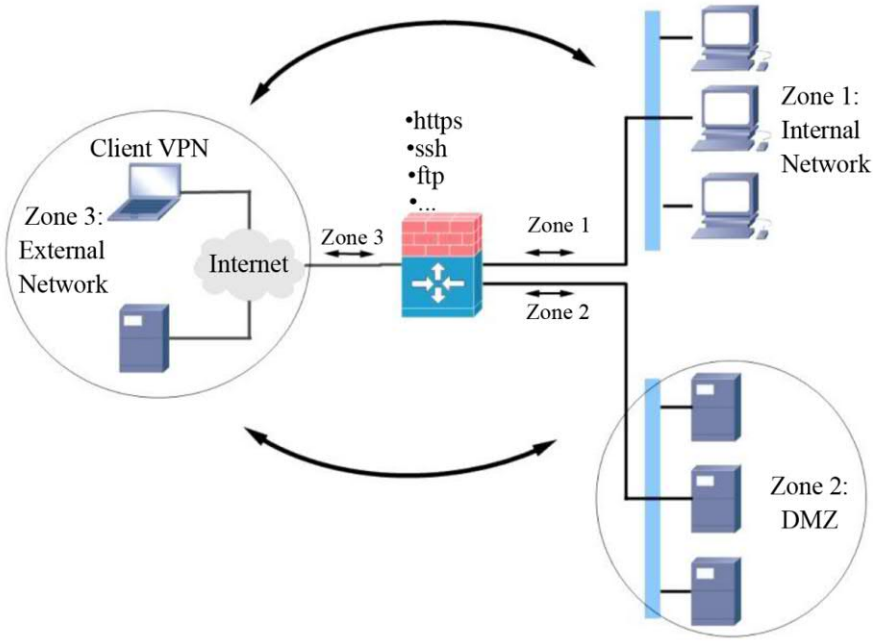


Figure 5.1. *The separation of the different types of networks into distinct zones*

5.6.3. *Rules applied to interzone traffic*

The following rules are applied to a ZFW when routing traffic:

– a security zone must be created before it can be assigned interfaces;

– an interface may be assigned to a single security zone;

– by default, traffic is authorized between interfaces that belong to the same zone;

– a security policy must be pre-configured in order to authorize traffic to pass between two zones. Three actions can be taken:

- **Pass**: traffic is allowed to transit from one zone to another;

- **Inspect**: allows traffic and inspects return traffic;

- **Drop**: delete the traffic;

– Any traffic towards a router interface (“self-zone”) is authorized unless explicitly prohibited.

5.6.4. *Terminology*

Access policies for a ZFW require three essential components:

– **Class-Map**: allows traffic to be identified based on certain criteria;

– **Policy-Map**: allows the application of a previously created "Class-Map" strategy;

– **Service-Policy:** allows you to define where to apply the Policy-Map created previously.

5.6.5. *Configuring a ZFW*

A ZFW can be configured following the below steps in sequence:

1) create zones;

2) create class-maps to identify authorized traffic;

3) create Policy-Maps to apply the Class-Maps;

4) define pairs of zones;

5) apply policy mappings to the zone pairs;

6) assign interfaces to the zones.

5.7. Creating zones

Command	Description
Router(config)# **zone security** *zone-name*	Creating a security zone.

5.8. Creating Class-Maps

Command	Description
Router(config)# **class-map type inspect** { **match-any** | **match-all** } *class-map-name*	Creates Class-Map and defines these options. **match-any**: the packets must satisfy one of the match criteria. **match-all**: the packets must satisfy all match criteria.
Router(config-cmap)# **match protocol** *protocol*	Defines the match criteria based on a protocol.

5.9. Creating the Policy-Map to apply the Class-Maps

Command	Description
Router(config)# **policy-map type inspect** *policy-map-name*	Creates a Policy-Map and defines these options.
Router(config-pmap)# **class type inspect** *class-map-name*	Associates this with one (or more) Class-Map(s).
Router(config-pmap-c)#{**drop** | **inspect** | **pass** }	Defines the action to be performed.

5.10. Defining the zone pairs

Command	Description
Router(config)# **zone-pair security** *zone-pair-name* **source** { *source-zonename* | **self** | **default** } **destination** { *destination-zone-name* | **self** | **default** }	Creates a pair of zones that allows the application of a unidirectional "Policy-Map" between both zones.

5.11. Applying the policy maps to the zone pairs

Command	Description
Router(config-sec-zone-pair)# **service-policy type inspect** *policymap-name*	Applies the Policy-Map strategy to the zone pair.

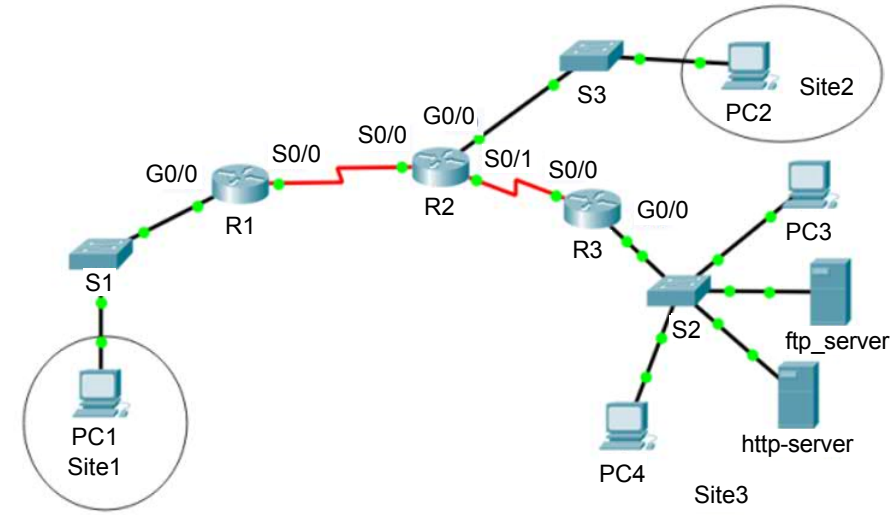
5.12. Assigning interfaces to zones

Command	Description
Router(config)# **interface** *type number* Router(config-if)# **zone-member security** *zone-name*	Associates an interface with a specific security zone.

5.13. Exercises for application

EXERCISE 6.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	G0/0	192.168.0.1	/24	–
	S0/0	192.168.100.1	/30	–
R2	G0/0	192.168.1.1	/24	–
	S0/0	192.168.100.2	/30	–
	S0/1	192.168.200.1	/30	–
R3	G0/0	192.168.2.1	/24	–
	S0/0	192.168.200.2	/30	–
PC1	NIC	192.168.0.2	/25	192.168.0.1
PC2	NIC	192.168.1.2	/26	192.168.1.1
PC3	NIC	192.168.2.4	/24	192.168.2.1
PC4	NIC	192.168.2.5	/24	192.168.2.1
ftp_server	NIC	192.168.2.2	/24	192.168.2.1
http-server	NIC	192.168.2.3	/24	192.168.2.1

Objectives

– Securing passwords;

– configuring an IPv4 ACL;

– configuring an IPv6 ACL.

Software to be used

Packet tracer.

Part A: establishing the basic device configuration.

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interface.

2. Configure the routing using the OSPF protocol.

2.1. Enable OSPF on both routers using the value 1 as the process ID.

2.2. Set the RID value to 1.1.1.1 for R1, 2.2.2.2 for R2 and 3.3.3.3 for R3.

2.3. Add all networks to the OSPF protocol.

2.4. Test connectivity between all network elements.

Part B: securing passwords

1. Set a minimum password length of 8 characters.

2. Set the password “Ci$c0ena” for the privileged mode.

3. Configure the console, auxiliary ports and virtual access lines.

3.1. Set “Ci$c0con” as the console port password and set the inactivity interval to 5 minutes.

3.2. Set "Ci$c0vty" as the password on the VTY lines and set the inactivity interval to 2 minutes.

3.3. Disable the auxiliary port.

4. Encrypt all passwords;

R1(config)# **service password-encryption**

Part C: configuring an IPv4 ACL

1. Review the valid range of numbers for numbered extended ACLs.

.....

2. On R3, create a numbered extended ACL that authorizes access to the http-server from station PC1. To do this create an ACL with the following options:

– the extended list number is **100**

– the action to be defined is **permit**;

– the protocol to be used is **TCP**;

– the source is a **host** with the IP address **192.168.0.2** (PC1);

– the destination is a **host** with the IP address **192.168.2.2** (http-server);

– the port to be used is **80**.

Write the ACL to be used:

.....

3. Add a rule to the extended ACL already created to allow denial of access to the http-server from the "site 2" network. To do this, configure ACL 100 with the following options:

– the action to be defined is **deny**;

– the protocol to be used is **TCP**;

– the source is **network** with the network address **192.168.1.0 / 26** (site 2);

– the **generic mask** is obtained by subtracting mask 255.255.255.255 from the network mask:

255.255.255.255 – 255.255.255.192 = **0.0.0.63**

– the destination is a **host** with the IP address **192.168.2.3** (http-server);

– the port to be used is **80**.

Write the command to be used:

.....

4. Add a rule to the previous ACL allowing all IP traffic with the http-server. To do this, configure the ACL 100 with the following options:

– the action to be defined is **permit**;

– the protocol to be used is **IP**;

– the source to be used is **any**;

– the destination is a **host** with the IP address **192.168.2.3** (http-server).

Write the command to be used:

.....

5. Add a rule to the previous ACL allowing the denial of ICMP traffic between PC1 and PC4. To do this, configure ACL 100 with the following options:

– the action to be defined is **permit**;

– the protocol to be used is **ICMP**;

– the source to use is a **host** with the IP address **192.168.0.2** (PC1);

– the destination is a **host** with the IP address **192.168.2.4** (PC4).

Write the command to be used:

.....

6. Apply the access control list 100 to the G0/0. / 0 interface.

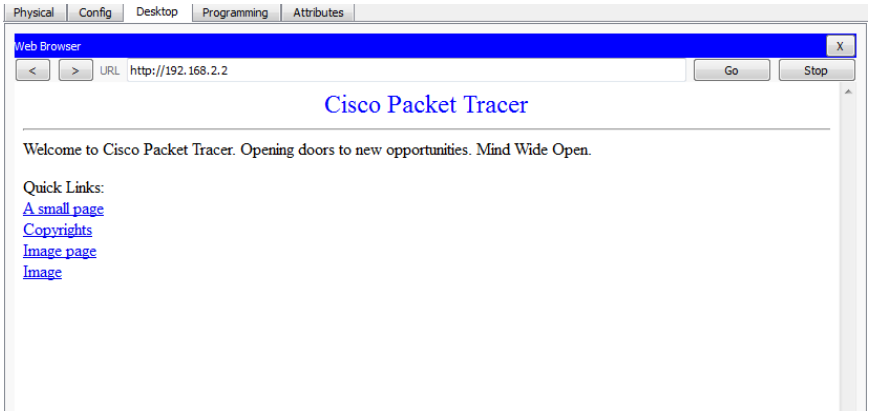
Write the command to be used:

.....

NOTE.– As a general rule, extended ACLs should be placed near the source. However, as ACL 100 affects traffic coming from two networks, “Site 1” and “Site 2”, the best placement would be on the output of interface G0/0.

7. Test the ACL created previously.

– Check that it is possible to access the **http** service from **PC1**.



– Check that the **http** service cannot be accessed from **PC2**.

– Check that it is possible to send a **ping** request to **http-server** from **PC2**.

– Check that it is not possible to send a **ping** request to **PC3** from **PC1**.

– Check that it is possible to send a **ping** request to **PC4** from **PC1.**

8. Delete the created ACL.

R3(config)#**no access-list 100**

9. On R3, create and test an extended ACL named "ACL_HTTP" which makes it possible to fulfil the security requirements stated earlier.

9.1. Create the extended ACL.

R3(config)#**ip access-list extended ACL_HTTP**
R3(config-ext-nacl)#

9.2. Allow http access from PC1 to http-server

R3(config-ext-nacl)# **permi tcp host 192.168.0.2 host 192.168.2.3 eq www**

9.3. Block http traffic from network “site 2” to the http-server.

R3(config-ext-nacl)# **deny tcp 192.168.1.0 0.0.0.63 host 192.168.2.3 eq www**

9.4. Allow all IP traffic with the http-server.

R3(config-ext-nacl)#**permit ip any host 192.168.2.3**

9.5. Display the ACL_HTTP ACL rules.

R3#**sh IP access-lists ACL_HTTP**

9.6. Applying the ACL_HTTP ACL to the G0/0. / 0 interface.

R3#**IP access-group ACL_HTTP out**

9.7. Test the effect of ACL_HTTP ACL.

10. On R3, create an extended ACL named “ACL_FTP” which makes it possible to fulfil the following security requirements:

– allow **ftp** access from **PC2** to **ftp_server**;

– block **ftp** traffic from “site 1” network to **ftp_server_http**;

– allow all **IP** traffic with **ftp_server**.

10.1. Display the ACL_FTP ACL rules.

10.2. Apply the ACL_FTP ACL to the G0/ 0 interface.

10.3. Test the effect of the ACL_FTP ACL.

PC2:\>**ftp 192.168.2.3**
Trying to connect...192.168.2.3
Connected to 192.168.2.3
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:**** (cisco)
230- Logged in
(passive mode On)
ftp>

Part D: configuring an IPv6 ACL

IPv6 addressing table

Device	Interface	IP address	Gateway
R1	G0/0	2001:DB8:AAAA:A::1/64	–
	S0/0	2001:DB8:AAAA:D::1/64	–
R2	G0/0	2001:DB8:AAAA:B::1/64	–
	S0/0	2001:DB8:AAAA:D::2/64	–
	S0/1	2001:DB8:AAAA:E::1/64	–
R3	G0/0	2001:DB8:AAAA:C::1/64	–
	S0/0	2001:DB8:AAAA:E::2/64	–
PC1	NIC	2001:DB8:AAAA:A::2/64	FE80::1
PC2	NIC	2001:DB8:AAAA:B::2/64	FE80::1
PC3	NIC	2001:DB8:AAAA:C::4/64	FE80::1
PC4	NIC	2001:DB8:AAAA:C::5/64	FE80::1
ftp_server	NIC	2001:DB8:AAAA:C::2/64	FE80::1
http-server	NIC	2001:DB8:AAAA:C::3/64	FE80::1

1. Create a new template with the same topology as in the previous exercise

2. Configure the basic parameters on R1, R2 and R3.

2.1. Configure the host name as indicated in the topology.

2.2. Apply the IP addresses to the router's interfaces according to the addressing table.

NOTE.– The local link addresses of the routers will be set to FE80: 1/64.

2.3. Set the clock value to 128 000 for the serial interface.

3. Configure the routing using the OSPF protocol.

3.1. Enable OSPF on both routers using the value 1 as the process ID.

3.2. Set the RID to 1.1.1.1 for R1, to 2.2.2.2 for R2 and to 3.3.3.3 for R3.

3.3. Add all networks to the OSPF protocol.

3.4. Test connectivity between all network elements.

4. On R3, create and activate an extended ACL named "ACL_HTTP" which makes it possible to meet all the security requirements defined in Part 1.

Write the command to be used:

.....

.....

.....

5. On R3, create an extended ACL called "ACL_FTP" which makes it possible to meet the security requirements defined in Part 1.

.....

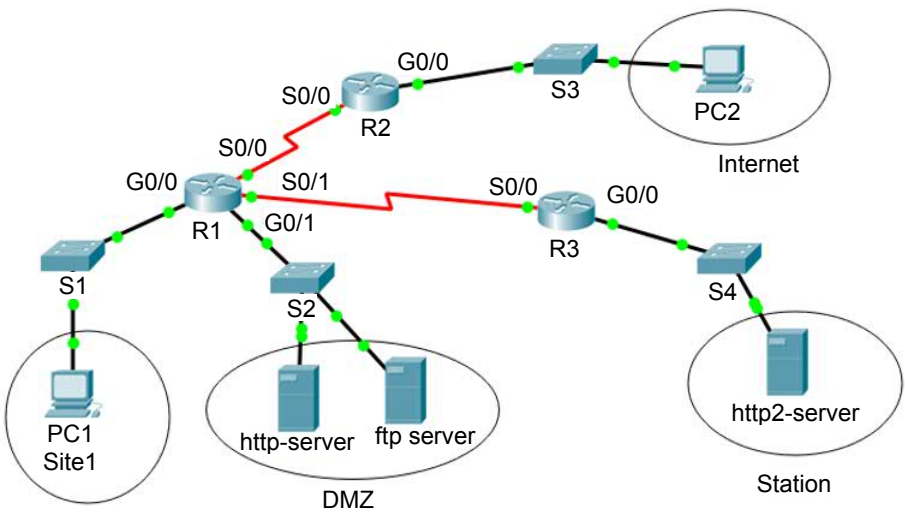
.....

.....

6. Test the effect of the ACLs created.

EXERCISE 7.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	G0/0	192.168.0.1	/24	–
	G0/1	192.168.1.1	/24	–
	S0/0	192.168.100.1	/30	–
	S0/1	192.168.200.1	/30	–
R2	G0/0	192.168.10.1	/24	–
	S0/0	192.168.100.2	/30	–
R3	G0/0	192.168.20.1	/24	–
	S0/0	192.168.200.2	/30	–
PC1	NIC	192.168.0.2	/24	192.168.0.1
PC2	NIC	192.168.10.2	/24	192.168.10.1
ftp_server	NIC	192.168.1.2	/24	192.168.1.1
http-server	NIC	192.168.1.3	/24	192.168.1.1
http2-server	NIC	192.168.20.2	/24	192.168.20.1

Objectives

Configuring a zone-based firewall.

Software to be used

Packet tracer.

Part A: establishing the basic device configuration.

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interface.

2. Configure the routing using the OSPF protocol.

2.1. Enable OSPF on the routers using the value 1 as the process ID.

2.2. Set the RID value to 1.1.1.1 for R1, to 2.2.2.2 for R2 and to 3.3.3.3 for R3.

2.3. Add all networks to the OSPF protocol.

2.4. Test connectivity between all network elements.

Part B: configuring a zone-based firewall

1. Review the definition of the DMZ zone.

.....

.....

2. Creating security zones on R1.

2.1. Create the internal zone with the name IN-ZONE.

```
R1(config)# zone security IN-ZONE
R1(config-sec-zone) exit
```

2.2. Create the DMZ zone with the name DMZ-ZONE.

```
R1(config)# zone security DMZ-ZONE
R1(config-sec-zone) exit
```

2.3. Create the external zone with the name OUT-ZONE.

```
R1(config)# zone security OUT-ZONE
R1(config-sec-zone) exit
```

2.4. Create the external zone with the name HEAD-ZONE.

```
R1(config)# zone security HEAD-ZONE
R1(config-sec-zone) exit
```

3. Create Class-Maps to identify authorized traffic.

3.1. Create a CMAP-IN-TO-DMZ Class-Map.

R1(config)#**class-map type inspect match-any CMAP-IN-TO-DMZ**

3.2. Allow http and ftp and icmp protocols.

R1(config-cmap)#**match protocol http**
R1(config-cmap)#**match protocol ftp**
R1(config-cmap)#**match protocol icmp**
R1(config-cmap)#**exit**
R1(config)#**exit**

3.3. Create a CMAP-IN-TO-HEAD Class-Map.

R1(config)#**class-map type inspect match-any CMAP-IN-TO-HEAD**

3.4. Allow http and icmp protocols.

R1(config-cmap)#**match protocol http**
R1(config-cmap)#**match protocol icmp**
R1(config-cmap)#**exit**
R1(config)#**exit**

3.5. Create a CMAP-OUT-TO-DMZ Class-Map.

R1(config)#**class-map type inspect match-any OUT -TO-DMZ**

3.6. Allow only the http protocol.

R1(config-cmap)#**match protocol http**
R1(config-cmap)#**exit**
R1(config)#**exit**

4. Create the Policy-Maps for applying the access rules to the Class-Map.

4.1. Review the definition of the three rules applied to inter-zone traffic.

– Pass: .....

– **Inspect**: .....

– **Drop**: .....

4.2. Create a Policy-Map to apply the Class-Map CMAP-IN-TO-DMZ.

R1(config)# **policy-map type inspect PMAP-IN-TO-DMZ**
R1(config-pmap)# **class type inspect CMAP-IN-TO-DMZ**
R1(config-pmap-c)# **pass**

4.3. Similarly, create the following Policy-Maps:

– **PMAP-OUT-TO-DMZ** for the Class-Map **CMAP-OUT-TO-DMZ**;

– **PMAP- IN-TO-HEAD** for the Class-Map **CMAP- IN-TO-HEAD.**

5. Define the zone pairs.

5.1. Create a zone pair that applies the PMAP-IN-TO-DMZ policy between IN-ZONE and DMZ-ZONE.

R1(config)#**zone-pair security IN-to-DMZ source IN-ZONE destination DMZ-ZONE**
R1(config-sec-zone-pair)# **service-policy type inspect PMAP-IN-TO-DMZ**

5.2. Similarly, create the following zone pairs:

– **OUT-to-DMZ** that applies the **PMAP-OUT-TO-DMZ** strategy;

– **IN-to-HEAD** that applies the **PMAP-IN-TO-HEAD** strategy.

6. Assign the interfaces to the zones.

R1(config)#interface G0/0
R1(config-if)#zone-member security **IN-ZONE**
R1(config)#interface G0/1
R1(config-if)#zone-member security **DMZ-ZONE**
R1(config)#interface S0/0
R1(config-if)#zone-member security **OUT-ZONE**
R1(config)#interface S0/1
R1(config-if)#zone-member security **HEAD-ZONE**

7. Verify the configuration of R1.

Using the "show running-config" command, verify all the parameters of your configuration.

8. Test the configuration of your firewall.

– Ensure that it is possible to access the **http-server** from **PC1** and **PC2**.

– Check that it is possible to access **http2-server** only from PC1**.**

– Check that it is possible to access the ftp-server service only from **PC1**.

PC1:\>**ftp 192.168.1.3**

– Check that it is possible to send a **ping** request to **http-server** from **PC1**.

– Check that it is not possible to send a **ping** request to **http-server** from **PC2**.

– Check that it is possible to send a **ping** request to **PC2** from **PC1**.

6

Putting in Place an Intrusion Prevention System (IPS)

This chapter will focus on the following topics:

– the role played by a detector;

– the differences between an IDS and an IPS;

– the types of IPS:

  - host-based IPS,

  - network-based IPS;

– modes of using an IPS:

  - promiscuous mode,

  - inline mode;

– the types of alarms;

– modes of detecting malicious traffic:

  - signature-based detection,

  - strategy-based detection,

  - anomaly-based detection,

  - reputation-based detection;

– severity levels of signatures;

– monitoring and management of alarms and alerts;

Computer Network Security, First Edition. Ali Sadiqui.

– the list of actions to take during an attack;

– the configuration of the IOS IPS.

6.1. Introduction to a detector

A **detector** is a network device that analyzes network traffic in order to classify it as normal or malicious, based on predefined rules.

An **Intrusion Detection System (IDS)** is a detector that can analyze packets travelling over one or more network connections in order to detect suspicious activity. Its role is limited to alerting the system administrator to the trace of any abnormal activity on a host or on the network. It does not prevent intrusion attempts.

An **Intrusion Prevention System (IPS)** is a detector that can detect and prevent any potential attack on a host or on the network.

6.2. The differences between an IDS and an IPS

The following table presents some characteristics of the two detectors: **IPS** and **IDS**.

	IDS	**IPS**
Processing packets	Receives only one copy of the original packets for processing.	All packets are processed by the system before reaching the network or host.
Impact on latency	There is no delay in the original traffic.	There is a slight delay before the traffic is sent on to the network.
Impact caused if the system is out of service	No negative impact.	All traffic passing through the system may be negatively affected.
Ability to protect the network	No protection against malicious traffic.	An IPS can protect traffic based on a set of pre-established rules.

NOTE.– Section 6.3 will focus on IPS detectors.

6.3. Types of IPS

Depending on where they are positioned in a network, the IPS may be placed to protect a host (Host-IPS or HIPS) or the entire network (Network-IPS or NIPS). Each type presents advantages and disadvantages.

	Advantages	Disadvantages
Host-IPS	– Can protect a specific host. – Can protect the Operating System and applications.	– Depends on an Operating System. – Must be installed on all hosts.
Network-IPS	– A less expensive solution. – Independent of the Operating System.	– Impossible to examine encrypted traffic.

6.4. Cisco IP solutions

The IPS solutions offered by Cisco are designed so that they can be adapted to different environments and offer high availability and efficiency.

Deployment options include dedicated equipment, IPS modules for switches and routers, and software-based solutions.

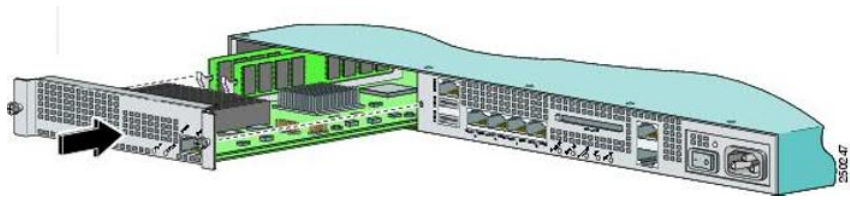


Figure 6.1. *The AIP-SSM module (a modular IPS) that can be integrated into a router[1]. For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip*

6.5. Modes of deploying IPS

An IPS may be deployed in two modes:

– **promiscuous mode**: the IPS is limited to analyzing network traffic and reporting anomalies (i.e. the IPS plays the role of an IDS);

1 Cisco Networking Academy, the official Cisco training site, can be found at the following address: https://www.netacad.com.

– **inline mode**: the traffic is directed towards the IPS in order to be analyzed. The IPS blocks part of this traffic based on pre-configured parameters.

6.6. Types of alarms

Attacks on a network may generate four types of alarms, coded as follows:

True positive	An alarm triggered by an intrusion that occurred and was detected by the IPS.
True negative	No intrusion took place and no action was taken by the IPS.
False positive	An alarm is triggered by normal traffic or an insignificant action.
False negative	No alarm was triggered when an intrusion took place.

An administrator is required to ensure that the "false positive" alarms are adjusted and that the "false negative" alarms are corrected.

NOTE.– You can now attempt Exercise 8.

6.7. Detecting malicious traffic

6.7.1. *Modes of detection*

An IPS may detect malicious traffic using several methods, including **signature**-based detection, **strategy**-based detection, **anomaly**-based detection and **reputation**-based detection.

6.7.2. *Signature-based detection*

6.7.2.1. *Definition of a signature*

A signature is a set of rules configured on an intrusion prevention system that allows it to detect intrusions. Cisco has grouped together signatures with similar characteristics into categories for easy management and analysis.

6.7.2.2. *Types of signatures*

There are two types of signatures:

– **atomic**: an attempt has been made to access a specific port on a specific host and the malicious content is in a single packet;

– **composite**: a sequence of operations distributed over multiple hosts over an arbitrary period.

6.7.2.3. *Characteristics of this detection mode*

In general, signature-based detection is the most commonly used method to identify malicious software in the Cisco intrusion-prevention/detection systems.

Advantages:

– easy to configure and implement;

– by default, an IPS has several pre-installed signatures;

– other, additional signatures, can be downloaded and implemented to mitigate new types of attacks.

Disadvantages:

– does not detect attacks that fall outside the predefined rules.

– may generate “false positive” alarms;

– signatures must be periodically updated.

6.7.3. *Other modes of detecting malicious traffic*

6.7.3.1. *Strategy-based detection*

Strategies are created and configured onto the IPS based on the network security policy. Any traffic that is detected as being outside this policy will generate an alarm and/or be blocked.

Advantages:

– simple, reliable and highly customizable;

– only allows traffic based on the network security policy, which may prevent unknown attacks.

Disadvantages:

– the strategy must be manually created;

– difficult to apply in the case of large networks.

6.7.3.2. *Anomaly-based detection*

The IPS generally looks for network traffic that deviates from the norm. A statistical reference must be developed to define the normal behavior of network traffic.

Advantage: can detect new types of attacks.

Disadvantages:

– difficult to accurately standardize the traffic on extremely large networks;

– may cause "false positive" alarms if valid network traffic changes significantly.

6.7.3.3. *Reputation-based detection*

Cisco Global Correlation is a feature that allows Cisco IPS detectors to filter network traffic using the "reputation" of the source IP address of a packet.

The reputation of an IP address, among other elements, is computed by the "Cisco SensorBase" service, specialized in this domain, based on this IP address' previous actions. This information is gathered from the flows of over 1.5 million Cisco IPS detectors and firewalls, among other devices, deployed worldwide. This feature supplies the network with valuable information that helps in detecting, preventing and reacting to recently-detected threats.

Advantages:

– makes use of the experience of other existing security systems;

– considered to be an early-warning system.

Disadvantage: requires continuous updates.

6.8. Signature micro-engines

A signature micro-engine is a component in an IPS (or IDS) detector that supports a particular category of signatures. All signatures from a signature micro-engine are scanned in parallel, which increases the efficiency and fluidity of the data.

A signature micro-engine carries out the following operations:

– allocates a set of ranges or acceptable values to a category of signatures;

– uses the router memory to compile, load and merge signatures.

Cisco has defined several categories of signatures used by these micro-engines, including:

Category of signatures	Description
Atomic	Makes it possible to inspect simple packets.
Service	Makes it possible to inspect whether a system is being attacked.
String	Makes it possible to inspect packets for multiple protocols, while specifying an expression that must be verified to trigger the signature.
Multi-string	Makes it possible to inspect packets by specifying a series of expressions that must be verified in order to trigger the signature.

NOTE.– There are other categories of signatures that make it possible to inspect other types of traffic.

6.9. Severity levels of the signatures

Each signature in the IPS signatures database is associated with a severity level. This makes it possible to configure an IPS to take different actions depending on the severity level detected. A signature may be associated with four severity levels.

Severity levels	Description
Information	The activity that triggers a signature is not considered an immediate threat, however the information supplied is useful.
Weak	Abnormal network activity has been detected. This may be perceived as malicious, however it is not likely to be an immediate threat.

Medium	Abnormal network activity has been detected. This may be perceived as malicious and an immediate threat is probable.
High	Attacks that are used to access or provoke a denial of service (DoS) attack are detected and an immediate threat is extremely probable.

6.10. Monitoring and managing alarms and alerts

Alerts generated by an IPS are, in general, sent to a real-time monitoring system to analyze, display and archive information. The surveillance and management of events may be hosted on a single server or on several separate servers for larger deployment. Several protocols are available to generate alarms, especially SDEE (Security Device Event Exchange), Syslog server and SNMP.

6.11. List of actions to be taken during an attack

When an IPS detector detects malicious activity, it can choose one of the following actions:

Action	Description
Deny attacker inline	Blocks packets coming from the attacker's IP address for a specified period.
Deny connection inline	Blocks the current and future packets belonging to this TCP stream.
Deny packet inline	Blocks the packet that triggered the alert.
Log attacker packets	Initiates the logging of packets that contain the IP address of the attacker.
Log pair packets	Initiates the logging of packets that contain the IP address of the attacker as well that of the victim.
Log victim packets	Initiates the logging of packets that contain the IP address of the victim.
Produce alert	Initiates the logging of events as alerts.
Produce verbose alert	Initiates the logging of events as alerts. However, this also includes a copy of the packets that triggered the alert.

Request block connection	Certain detectors may rely on another network element to block traffic in the network from the attacker, at a given moment. This device is called the "blocking device" and may be an IOS router using ACLs, a switch using VACLs, etc. This action causes a request to be sent to the "blocking device" to block this connection.
Request block host	Sends a request to a "blocking device" to block the attacker's host.
Request SNMP trap	Sends an SNMP notification and an alert to the events log.
Reset TCP connection	Resets and terminates a TCP connection.

6.12. Configuration of an IOS IPS

1. To configure a basic IPS using CLI commands, proceed as follows:

Create an IPS configuration directory in the Flash memory.

Command	Description
Router# mkdir flash: dir-name	Creates a configuration directory.

Copy the IPS signatures package into the Flash memory.

Command	Description
Router# copy ftp://myuser:my-pass@ftp-server/IOS-Sxxx-CLI.pkg **flash:** dir-name **idconf**	Copy the signature package from an FTP server into the directory in Flash.
Router# copy tftp://tftp-server/IOS-Sxxx-CLI.pkg **flash:** dir-name **idconf**	Copy the signature package from a TFTP server into the Flash directory.
Router# copy usbflash0:/IOS-S xxx -CLI.pkg **flash:** dir-name **idconf**	Copy the signature package from a USB into the Flash directory.

Create an IPS rule and specify the location of the IPS signature file.

Command	Description
Router(config)# ip ips name ips-name **[***name acl* **]**	Creates a name for the IPS rule. NOTE.– the use of ACLs is optional. It makes it possible to filter the traffic that will be analyzed.
Router(config)# ip ips config location flash: dir-name	Specifies the location of the IPS signature file.

Activate the SDEE protocol and logging.

Command	Description
Router(config)# ip http server	Activates the http server (required when using SDEE).
Router(config)# ip ips notify sdee	Activates the SDEE event notification.
Router(config)# ip ips notify log	Activates logging.

Modify the signature categories.

Parameterization of signatures per category:

Command	Description
Router(config)# ip ips signature-category	Enters into the configuration mode for IPS signature categories.
Router(config-ips-category)# category { all | ios_ips [basic | advanced]}	Specifies the signature category to be modified.
Router(config-ips-categoryaction)# retired { false | true }	Indicates whether a signature or signature category is to be loaded or not in the router memory. **– True**: removes all signatures within this category from the memory. **– False**: compiles the signature category in memory and uses it to analyze traffic.
Router(config-ips-categoryaction)# event-action action	Modifies the actions to be taken for a specified signature category. These actions include the following: **– deny-attacker-inline**; **– deny-connection-inline**; **– deny-packet-inline**; **– produce-alert**; **– reset-tcp-connection**.
Router(config-ips-categoryaction)# alert-severity { high | medium | low | informational }	(Optional) Modify the severity level of an alert for a signature or specific signature category.

Modify a signature.

Command	Description
R1(config)#ip ips signature-definition **R1(config-sigdef)#signature***ID_of_signature ID_of_sub-signature* **R1(config-sigdef-sig)#status** **…** **R1(config-sigdef-sig)#engine** **…**	This command uses several parameters, in particular: **Signature ID-**: a unique numerical value assigned to a signature. The list of signature IDs is available on the Cisco website. **Sub-signature ID:** a unique numerical value assigned to a sub-signature. **Engine**: makes it possible to define the engine used by the signature and the functional characteristics. **Status**: indicates whether the signature is active or removed.

Activates the IPS rules on an interface.

Apply the IPS rule to a desired interface and specify the direction:

Command	Description
Router(config-if)# ip ips ips-name { in | out }	Applies an IPS rule to an interface – **IN**: only inspects incoming traffic; – **OUT**: only inspects outgoing traffic.

6.13. Recommended practices

The best practices for implementing IPS include:

– implement IPS to analyze traffic sent towards critical network components such as servers, routers etc.;

– reconfigure IPS, when necessary, to take into account changes in flow or topology;

– it is recommended that you use dedicated devices for IPS tasks instead of using IPS that are based on modules or on the features of the IOS system;

– use automated signature updates instead of applying them manually;

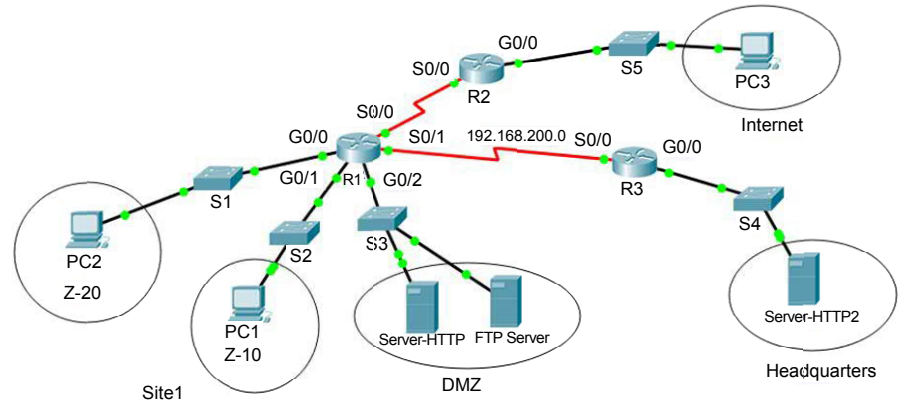
– make use of global correlation to improve your resistance to possible attacks;

– use a combination of intrusion detection technologies to reinforce security.

6.14. Exercises for application

EXERCISE 8.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	G0/0	192.168.0.1	/25	–
	G0/1	192.168.0.129	/25	–
	G0/2	192.168.1.1	/24	–
R1	S0/0	192.168.100.1	/30	–
	S0/1	192.168.200.1	/30	–
R2	G0/0	192.168.10.1	/24	–
	S0/0	192.168.100.2	/30	–
R3	G0/0	192.168.20.1	/24	–
	S0/0	192.168.200.2	/30	–
PC1	NIC	192.168.0.2	/25	192.168.0.1
PC2	NIC	192.168.0.130	/25	192.168.0.129
PC3	NIC	192.168.10.2	/24	192.168.10.1
FTP_server	NIC	192.168.1.2	/24	192.168.1.1
Server-HTTP	NIC	192.168.1.3	/24	192.168.1.1
Server-HTTP2	NIC	192.168.20.2	/24	192.168.20.1

Objectives

Configuring a zone-based firewall.

Software to be used

Packet tracer.

Part A: setting up the basic device configuration

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interfaces.

2. Configure the routing using the OSPF protocol.

2.1. Enable OSPF on the routers using the value 1 as the process ID.

2.2. Set the RID value to 1.1.1.1 for R1, to 2.2.2.2 for R2 and to 3.3.3.3 for R3.

2.3. Add all networks to the OSPF protocol.

2.4. Test connectivity between all network elements.

Part B: configuring a zone-based firewall

1. Create security zones on R1.

Create the following security zones:

Name of the security zone	Description
IN-ZONE-Z10	Network for Service 1
IN-ZONE-Z20	Network for Service 2
DMZ-ZONE	Network for the DMZ zone
OUT-ZONE	Internet network
HEAD-ZONE	The headquarters network

2. Create ACLs that define the internal traffic to be monitored.

2.1. Create a numbered ACL that authorizes http, FTP and icmp streams.

R1(config)# **access-list 101 permit tcp 192.168.0.0 0.0.0.127 host 192.168.1.2 eq www**
R1(config)# **access-list 101 permit tcp 192.168.0.0 0.0.0.127 host 192.168.1.2 eq ftp**
R1(config)# **access-list 101 permit icmp 192.168.3.0 0.0.0.127 any**

2.2. Creates a numbered ACL that allows the FTP stream.

R1(config)# **access-list 102 permit tcp any host 192.168.1.2 eq ftp**
R1(config)# **access-list 102 permit icmp any host 192.168.1.2**

2.3. Create a numbered ACL that allows http and icmp streams towards the headquarters.

R1(config)# **access-list 103 permit tcp 192.168.0.0 0.0.0.255 host 192.168.20.2 eq www**
R1(config)# **access-list 103 permit icmp 192.168.0.0 0.0.0.255 host 192.168.20.2**

3. Create Class-Maps to identify authorized traffic.

3.1. Create a CMAP-IN-TO-DMZ Class-Map and identify authorized traffic.

R1(config)#class-map type inspect match-any CMAP-IN-TO-DMZ
R1(config-cmap)# **match access-group 101**
R1(config-cmap)# **exit**

3.2. Create a CMAP-IN-TO-HEAD Class-Map and identify authorized traffic.

R1(config)#class-map type inspect match-any CMAP-IN-TO-HEAD
R1(config-cmap)# **match access-group 103**
R1(config-cmap)# **exit**

3.3. Create a CMAP-OUT-TO-DMZ Class-Map.

R1(config)#class-map type inspect match-any OUT -TO-DMZ

R1(config-cmap)# **match access-group 102**
R1(config-cmap)# **exit**

4. Create the Policy-Map to apply the Class-Maps.

4.1. Create a Policy-Map to apply the CMAP-IN-TO-DMZ Class-Map.

R1(config)# policy-map type inspect PMAP-IN-TO-DMZ
R1(config-pmap)# class type inspect CMAP-IN-TO-DMZ
R1(config-pmap-c)# pass

4.2. Similarly, create the following Policy-Maps:

PMAP-OUT-TO-DMZ for the **CMAP-OUT-TO-DMZ Class-Map**

PMAP- IN-TO-HEAD for the **CMAP-IN-TO-HEAD Class-Map**

5. Define the zone pairs.

Create the following zone pairs:

Name of the zone pair	Source	Destination	Strategy to apply
IN-to-DMZ	IN-ZONE-Z10	DMZ-ZONE	PMAP-IN-TO-DMZ
OUT-to-DMZ	OUT-ZONE	DMZ-ZONE	PMAP-OUT-TO-DMZ
IN1-to-HEAD	IN-ZONE-Z10	HEAD-ZONE	PMAP- IN-TO-HEAD
IN2-to-HEAD	IN-ZONE-Z20	HEAD-ZONE	PMAP- IN-TO-HEAD

6. Assign the interfaces to the zones.

Name of the interface	Name of the security zone
G0/0	IN-ZONE-Z20
G0/1	IN-ZONE-Z10
G0/2	DMZ-ZONE
S0/0	OUT-ZONE
S0/1	HEAD-ZONE

7. Verify the configuration of R1.

Using the “show running-config” command, verify all the parameters of your configuration.

8. Test the configuration of your firewall.

– Check that it is possible to access the **Server-HTTP** from **PC2** and **PC3**.

– Check that it is only possible to access **Server-http2** from PC1.

– Check that it is only possible to access the **Server-ftp** service from PC1.

PC1:\>**ftp 192.168.1.3**

– Check that it is possible to send a **ping** request to **Server-HTTP** from **PC1**.

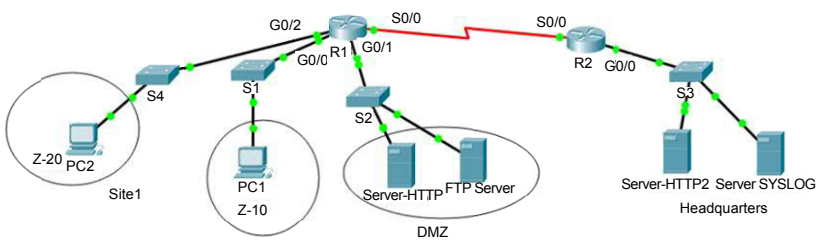
– Check that it is possible to send a **ping** request from **PC1** from to **PC3**.

9. Modify the parameters of your R1 firewall.

Add the modifications required to **authorize** and **inspect** the traffic between Z-20 and the **http-Server.**

EXERCISE 9.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	G0/0	192.168.0.1	/25	–
	G0/2	192.168.0.129	/25	–
	G0/1	192.168.1.1	/24	–
	S0/0	192.168.100.1	/30	–
R2	G0/0	192.168.10.1	/24	–
	S0/0	192.168.100.2	/30	–
PC1	NIC	192.168.0.2	/25	192.168.0.1
PC2	NIC	192.168.0.130	/25	192.168.0.129
FTP_server	NIC	192.168.1.2	/24	192.168.1.1
Server-HTTP	NIC	192.168.1.3	/24	192.168.1.1
Server-HTTP2	NIC	192.168.10.2	/24	192.168.10.1
Server-SYSLOG	NIC	192.168.10.3	/24	192.168.10.1

Objectives

– Configure a zone-based firewall;

– configure an IPS using the CLI command.

Software to be used

Packet tracer.

Part A: establishing the basic device configuration.

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interfaces.

1.4. Set the system date and time.

2. Configure the routing using the OSPF protocol.

2.1. Enable OSPF on the routers using the value 1 as the process ID.

2.2. Set the RID value to 1.1.1.1 for R1 and 2.2.2.2 for R2.

2.3. Add all networks to the OSPF protocol.

2.4. Test connectivity between all network elements.

Part B: configuring a zone-based firewall

1. Create security zones on R1.

Create the following security zones:

Name of the security zone	Description
IN-ZONE-Z10	Network for Service 1
IN-ZONE-Z20	Network for Service 2
DMZ-ZONE	Network for the DMZ zone
HEAD-ZONE	The headquarters network

2. Create ACLs that define the internal traffic to be monitored.

2.1. Create a numbered ACL (101) that authorizes the http, FTP and icmp streams between Z-10 and the DMZ-zone servers.

2.2. Create a numbered ACL (102) that allows the FTP flow between Z-20 and the FTP server for the DMZ.

2.3. Create a numbered ACL (103) that allows all http and icmp streams towards the headquarters.

3. Create Class-Maps to identify authorized traffic.

3.1. Create a CMAP-IN-TO-DMZ Class-Map and identify authorized traffic.

3.2. Create a CMAP-IN-TO-HEAD Class-Map and identify authorized traffic.

3.3. Create a CMAP-OUT-TO-DMZ Class-Map.

4. Create the Policy-Map to apply the Class-Maps.

4.1. Create a Policy-Map to apply the CMAP-IN-TO-DMZ Class-Map.

4.2. Similarly, create the following Policy-Maps:

PMAP-OUT-TO-DMZ for the **CMAP-OUT-TO-DMZ Class-Map**

PMAP- IN-TO-HEAD for the **CMAP- IN-TO-HEAD Class-Map**

5. Define the zone pairs.

Create the following zone pairs:

Name of the zone pair	Source	Destination	Strategy to apply
IN-to-DMZ	IN-ZONE-Z10	DMZ-ZONE	PMAP-IN-TO-DMZ
IN1-to-HEAD	IN-ZONE-Z10	HEAD-ZONE	PMAP-IN-TO-HEAD
IN2-to-HEAD	IN-ZONE-Z20	HEAD-ZONE	PMAP-IN-TO-HEAD

6. Assign the interfaces to the zones.

Name of the interface	Name of the security zone
G0/0	IN-ZONE-Z10
G0/2	IN-ZONE-Z20
G0/1	DMZ-ZONE
S0/0	HEAD-ZONE

7. Verify the configuration of R1.

Using the "show running-config" command, verify all the parameters of your configuration.

8. Test the configuration of your firewall.

Part C: configuring an IPS using CLI commands

1. Review the definition of an IPS signature.

.....

.....

2. Create a configuration directory.

R2# **mkdir ipsDir**

R2# **config terminal**

R2(config)#**ip ips config location ipsDir**

3. Create an IPS rule.

R2(config)#**ip ips name ipsRule**

4. Enable logging to the Syslog server.

R2(config)#**service timestamps log datetime msec**
R2(config)#**logging on**
R2(config)#**logging 192.168.10.3**
R1(config)#**ip ips notify log**

5. Configure the IPS to use the signature categories.

5.1. Remove all signatures

R2(config)#**ip ips signature-category**
R2(config-ips-category)#**category all**
R2(config-ips-category-action)#**retired true**
R2(config-ips-category-action)#**exit**

5.2. Only activate the signatures from the category "ios_ips basic".

R2(config-ips-category)#**category ios_ips basic**
R2(config-ips-category-action)#**retired false**
R2(config-ips-category-action)#**exit**
R2(config-ips-category)#**exit**
Do you want to accept these changes? [confirm]

6. Apply the IPS rule to an interface.

R2(config)#**interface S0/0**
R2(config-if)#**ip ips ipsRule in**

7. Modify the signature parameters.

7.1. Display the information associated with the signature "ICMP Echo Request" (IDsig: 2004, IDsubsig: 0).

```
R2#show ip ips signature sigid 2004 subid 0
…
Action=(A)lert, (D)eny, (R)eset, Deny-(H)ost, Deny-(F)low
Trait=alert-traits          EC=event-count          AI=alert-interval
GST=global-summary-threshold  SI=summary-interval   SM=summary-mode
SW=swap-attacker-victim       SFR=sig-fidelity-rating Rel=release
 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW
SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
 2004:0     N* Nr   A     INFO     0     1    0    200   30  FA  N 100 S1
    sig-name: ICMP Echo Request
    sig-string-info: My Sig Info
    sig-comment: Sig Comment
    Engine atomic-ip params:
        fragment-status:
        icmp-type: 8
        l4-protocol: icmp
```

7.2. Select the signature “ICMP Echo Request”.

```
R2(config)#ip ips signature-definition
R2(config-sigdef)#signature 2004 0
```

7.3. Enable the signature.

```
R2(config-sigdef-sig)#status
R2(config-sigdef-sig-status)#retired false
R2(config-sigdef-sig-status)#enabled true
R2(config-sigdef-sig-status)#exit
```

7.4. Change the action for the signature to “produce-alert”.

```
R2(config-sigdef-sig)#engine
R2(config-sigdef-sig-engine)#event-action produce-alert
R2(config-sigdef-sig-engine)#exit
```

R2(config-sigdef-sig)#**exit**
R2(config-sigdef)#**exit**
Do you want to accept these changes? [confirm]

8. Check the IPS configuration is done.

R2#**show ip ips all**
IPS Signature File Configuration Status
Configured Config Locations: ipsDir
Last signature default load time:
…
IPS Syslog and SDEE Notification Status
Event notification through syslog is enabled
IPS Signature Status
Total Active Signatures: 1
Total Inactive Signatures: 0
IPS Packet Scanning and Interface Status
IPS Rule Configuration
IPS name ipsRule
IPS fail closed is disabled
..
Interface Configuration
Interface Serial0/0
Inbound IPS rule is not set
Outgoing IPS rule is ipsRule
IPS Category CLI Configuration:
Category all
Retire: True
Category ios_ips basic
Retire: False

9. Check that your configuration works.

9.1. Review the definition of an IDS.

……

……

9.2. Send out a "ping" from PC2 to Server-http2.

9.3. Check that the following message was added to the Server-SYSLOG:

%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.0.2 -> 192.168.10.2:0] RiskRating:25

9.4. Why can R2 be considered as an IDS and not an IPS?

……

……

9.5. Modify the "ICMP Echo Request" signature to refuse ICMP packets.

R2(config)#ip ips **signature-definition**
R2(config-sigdef)#**signature 2004 0**
R2(config-sigdef-sig)#**engine**
R2(config-sigdef-sig-engine)#**event-action produce-alert**
R1(config-sigdef-sig-engine)#**event-action deny-packet-inline**
R2(config-sigdef-sig-engine)#**exit**
R2(config-sigdef-sig)#**exit**
R2(config-sigdef)#**exit**
Do you want to accept these changes? [confirm]

9.6. Send out a "ping" from PC2 to Server-http2. Why was this command unsuccessful?

……..

9.7. Verify that a message has been added to the Server-SYSLOG.

9.8. Why can we now consider R2 as an IPS?

……..

……..

7

Securing a Local Network

This chapter will focus on the following topics:

– the types of attacks on Layer 2:

- MAC address flooding attacks;
- MAC address spoofing attack;
- DHCP starvation attack;
- VLAN hopping attack;
- STP-based attacks;

– best security practices to protect Layer 2:

- configuring port security;
- configuring the DAI feature;
- configuring the “portfast” feature;
- configuring the “bpdu guard” feature;
- configuring the “guard root” feature.

7.1. Introduction

A LAN, generally comprising one or more Layer 2 switches may be the target of several attacks based on any gaps that may exist in Layer 2. An attacker may attempt to interrupt, copy, redirect or compromise Level 2 data transmission and, consequently, may affect any type of protocol used on the upper layers.

Computer Network Security, First Edition. Ali Sadiqui.

7.2. Types of attacks on Layer 2

In this chapter we will study several security threats that target Layer 2 of an OSI model and discuss countermeasures that can be used to protect against these risks. This is part of securing the "**data plane**".

7.2.1. *MAC address flooding attacks*

Overview of the attack

An attacker connects to a switch port and floods it using a large number of frames with fake source MAC addresses. Once the switch table is saturated, the switch acts as a hub. The attacker can then capture sensitive data from the network.

Countermeasures

The "**port security**" feature is a countermeasure that can prevent MAC address flooding attacks.

Command	Description
Switch(config-if)# switchport mode access **Switch(config-if)# switchport port-security**	Enables port security and assign the current MAC address to the port. The default port security values are: – only one MAC address can be assigned; – the violation action is set to the deactivation of the port.
Switch(config-if)# **switchport port-security maximum** *value*	Defines the maximum possible number of MAC addresses secured for the interface.
Switch(config-if)# switchport port-security mac-address *mac-address*	Manually assigns the MAC addresses that can connect to this port.
Switch(config-if)# switchport port-security violation { protect | restrict | shutdown |shutdown vlan }	Configures the action that must be taken when the number of MAC addresses exceeds the pre-defined maximum.
Switch(config)# errdisable recovery interval *seconds*	Configures the period of deactivation of a port.

7.2.2. *MAC spoofing attack*

Overview of the attack

A MAC address spoofing (ARP spoofing) attack consists of sending false ARP messages within a local network, with the aim of deviating and intercepting network traffic.

Countermeasures

The "**DAI**" (Dynamic ARP Inspection) feature is used to prevent ARP spoofing attacks. It makes it possible to verify the mapping between the IPv4 addresses and the MAC addresses. In case of any anomaly from an unreliable port, the spoofed ARP packets will be ignored.

Command	Description
switch(config)#ip arp inspection vlan vlan	Enables dynamic ARP inspection (DAI) on a specific VLAN.
switch(config)#interface g0/0 **switch(config-if)#ip arp inspection trust**	Configures a port to be a reliable port.

7.2.3. *The DHCP starvation attack*

Overview of the attack

A DHCP starvation attack consists of broadcasting a large number of DHCP requests with spoofed source MAC addresses. Once the number of IP addresses available in the DHCP server is exhausted, the attacker may introduce their DHCP server to respond to new DHCP requests on the network. The attacker can now capture sensitive data using a man-in-the-middle (MITM) attack.

Countermeasures

The "**DHCP snooping**" feature is used to prevent attacks of this type by filtering unreliable DHCP messages.

Command	Description
S1(config)#**ip dhcp snooping**	Enables the "**DHCP snooping**" feature on all VLANs.
S1(config)#**ip dhcp snooping vlan** *vlan*	Enables the "**DHCP Snooping**" feature on a specific VLAN.
S1(config)#**interface g0/0** S1(config-if)#**ip dhcp snooping trust**	Configures a reliable port.
S1#**show ip dhcp snooping**	Displays the "**DHCP snooping**" configuration.

7.2.4. *VLAN hopping attacks.*

VLAN hopping attacks consist of connecting to a particular VLAN and attempting to access network traffic belonging to other VLANs. By using VLAN hopping, an attacker may capture another VLAN's network traffic or send data from one VLAN to another.

There are two types of VLAN hopping attacks, namely: "Switch spoofing" and "Double Tagging" attacks.

7.2.4.1. *Switch spoofing attack*

Overview of the DTP protocol

DTP is the protocol used to dynamically create trunks (aggregated links) between two switches. This may be configured in three modes: "Dynamic Desirable", "Dynamic Auto" or "Trunk".

Overview of the attack

This attack consists of connecting to the interface of a switch and generating DTP messages from a program to create a "trunk" link between the attacker's computer and the switch. The attacker can now capture data from all other VLANs.

This attack can also take place through the introduction of a "spoofed switch", configured for using the DTP protocol.

Countermeasures

The following features are used to prevent this kind of attack:

Command	Description
S1(config)#**interface range gigabitethernet 0/0 - 20** S1(config-if-range)#**switchport mode access**	Configures the ports of a switch connected to hosts as access ports.
S1(config-if)# **switchport mode trunk**	Explicitly enables the aggregation links.
S1(config-if)# **switchport nonegotiate**	Disables DTP and prevents DTP messages from being generated.
S1(config)#**interface range gigabitethernet 0/26 - 32** S1(config-if)# **switchport access vlan** *Vlan* S1(config-if)# *shutdown*	Assigns the unused ports to a dedicated VLAN and disables them.

7.2.4.2. *Double tagging attack*

Overview of the attack

This attack consists of connecting to an interface that belongs to a native VLAN on a “trunk” port and sending a frame by inserting the fields related to the VLAN twice in an Ethernet frame.

Indeed, a double-tagging attack takes place in three steps:

1) the attacker generates and sends a 802.1Q frame, marked by double tags, to switch 1:

- the first tag carries the native VLAN identifier of the “trunk” port;
- the second tag carries the VLAN identifier of the target host.

Data	Native VLAN ID	Target VLAN ID

Figure 7.1. *Frame 802.1Q, marked by two tags*

2) switch 1 will remove the native VLAN tag. The attacker’s frame will now only contain the VLAN tag for the target host.

Data	Target VLAN ID

Figure 7.2. *Frame 802.1Q marked by the VLAN tag on the host target*

3) switch 2 will send the frame to the port of the target host.

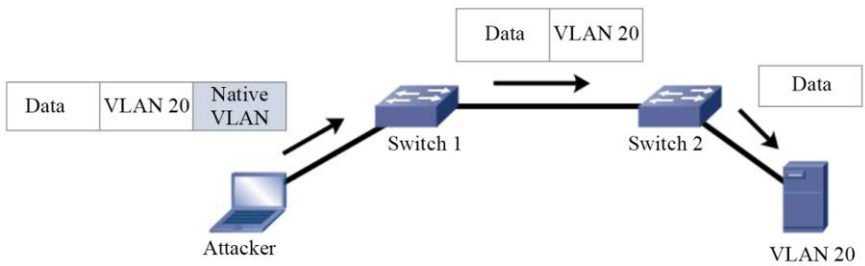


Figure 7.3. *The steps in a double-tagging attack*

NOTE.–

– In figures 7.1, 7.2 and 7.3, the "data" field represents the information connected to an Ethernet frame, in addition to the other information from the packet and without taking into account the order of their succession in a 802.1Q frame.

– This type of attack is unidirectional and only works if the hacker is connected to a port in the same VLAN as the native trunk port VLAN.

Countermeasures

The "**native VLAN"** feature is used to prevent this kind of attack.

Command	Description
Switch(config-if)# **switchport trunk native vlan** *vlan*	Create a dedicated VLAN for native VLAN traffic separated from user traffic.

7.2.5. *STP-based attacks*

Overview of the STP

STP is a network protocol that makes it possible to create a loopless network topology by blocking certain paths in the LAN, consisting of multiple switches. Its function can be summarized as follows:

– selecting a "root bridge" switch for each VLAN;

– defining "root ports" that allow interconnection between the "root" switch and other switches;

– defining ports authorized to transmit data;

– blocking certain ports on the switches.

Overview of the attack

This attack consists of introducing a "spoofed switch", which will attempt to position itself as the "root bridge" by sending false "PDU" messages that contain a minimal "BID". This will have the effect of modifying the STP topology and changing the role of the ports. From now on, the attacker can use the ports which were blocked earlier, in order to capture all the traffic passing through the network.

Countermeasures

The "**guard root**" feature is used to prevent this kind of attack:

Command	Description
S1(config-if)# **spanning-tree guard root**	Protects against the replacement of the original “root bridge” by another switch.

NOTE.–

– “**bpdu guard”** and “**guard root**” are similar, but have different impacts:

– **bpdu guard** disables the ports when receiving bpdu messages if the “portfast” option is activated on the port. You must manually reactivate the port or configure a “deactivation time”.

– **guard root** allows bpdu messages to travel across a port to maintain STP topology, unless another switch attempts to become the “root bridge”. The port is reactivated when the other switch stops its attempts.

7.3. The best security practices for protecting Layer 2

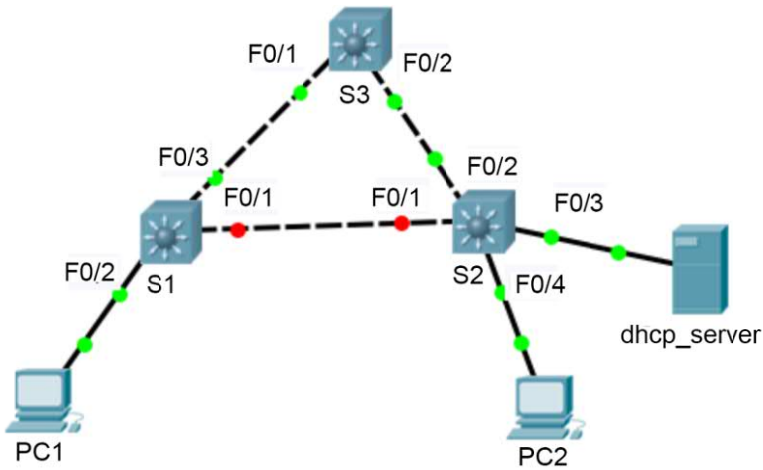
The best practices to protect Level 2, for each type of attack, include:

Type of attack	Description	Countermeasures
MAC address attacks	– MAC address flooding – MAC address spoofing	– Using port security for access ports. – Configure the **DAI** feature**.**
STP attacks	– Modification of STP topology	– Configuring the **portfast** feature. – Configuring the **bpdu guard** feature. – Configure the **guard root** feature.
VLAN hopping attacks	– Using DTP – Double tagging attack	– Disable DTP on the access ports. – Explicitly configure the “trunk” ports. – Always use a dedicated native VLAN. – Deactivate all unused ports and place them in an unused VLAN. – Avoid using VLAN 1.

7.4. Exercises for application

EXERCISE 10.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
S1	VLAN1	192.168.0.2	/24	192.168.0.1
S2	VLAN1	192.168.0.3	/24	192.168.0.1
S3	VLAN1	192.168.0.4	/24	192.168.0.1
PC1	NIC	192.168.0.5	/24	192.168.0.1
PC2	NIC	192.168.0.6	/24	192.168.0.1
dhcp-server	NIC	192.168.0.7	/24	192.168.0.1

Objectives

– Securing passwords;

– Putting in place connection restrictions;

– Securing the local network against Level 2 attacks.

Software to be used

– Packet Tracer.

Part A: establishing the basic device configuration.

1. Configure the names of the host as indicated in the topology.

2. Apply the IP addresses to the device interfaces according to the addressing table.

Part B: securing passwords

On switch S1

1. Set the password "Ci$c0ena" for the privileged mode.

2. Configure the console ports and virtual access lines.

2.1. Set "Ci$c0con" as the password for the console port and set the inactivity interval to 5 minutes.

2.2. Set "Ci$c0vty" as the password on the VTY lines and set the inactivity interval to 2 minutes.

3. Encrypt all passwords.

Part C: securing access to VTY lines using ssh

1. Configure *ssh* connections.

On switch S1

– Use the following options to configure the ssh connections:

– domain name: ***tri.local***;

– the user name: ***sshadmin*** with the password**: Ci$c0ssh;**

– the RSA encryption key is ***1024 bits***;

– the SSH version used is ***version 2***;

– the wait time is ***90s***;

– the number of login attempts is ***3***;

– only authorize ***ssh*** sessions.

2. Configure the connection parameters.

Use the "**login block-for**" command to configure the connection being blocked for ***60s*** if two connection attempts have failed within ***30s***.

Part D: securing the local network against Layer 2 attacks

On switch S2

1. Secure LAN against MAC address flooding attacks.

1.1. Explain this type of an attack.

.....

.....

1.2. Set the maximum number of secured MAC addresses to be 2 on the FastEthernet ports 0/4 to 0/16.

S2(config)# **int rang f0/4-16**
S2(config-if)# **switchport mode access**
S2(config-if)# **switchport port-security**
S2(config-if)# **switchport port-security maximum 2**

1.3. Block the frames received on the ports in case of access violation.

S2(config-if)# **switchport port-security violation protect**

1.4. Manually assign the MAC address of the Server_dhcp to port f0/3.

S2(config)# **int f0/3**
S2(config-if)# **switchport mode access**
S2(config-if)# **switchport port-security**
S2(config-if)# **switchport port-security mac-address** *mac-address_server_dhcp*

1.5. Deactivate the unused *FastEthernet* ports *0/17* to *0/24*.

S2(config)# **int rang f0/17-24**

S2(config-if)# **shutdown**

1.6. Display the security of the interfact ports f0/4 and give explanations for the elements in bold.

S2#**show port-security interface f0/4**
Port Security: Enabled
Port Status: Secure-up
Violation Mode: protect
Aging Time: 0 mins
Aging Type: Absolute
SecureStatic Address Aging: Disabled
Maximum MAC Addresses: 2
Total MAC Addresses: 1
Configured MAC Addresses: 1
Sticky MAC Addresses: 0
Last Source Address:Vlan: 001b.5325.256f:1
Security Violation Count: 0

.....

.....

.....

2. Secure the LAN against DHCP starvation attacks.

2.1. Explain this type of attack.

.....

.....

2.2. Configure the port f0/3 as a port connected to a reliable DHCP server.

S2(config)#**interface f0/3**
S2(config-if)#**ip dhcp snooping trust**

2.3. Display the “dhcp snooping” parameters.

S2#**show ip dhcp snooping**

2.4. Test the working of the DHCP server. Stations PC1 and PC2 must be capable of having dynamic IP addresses after DHCP configuration.

3. Secure the LAN against VLAN hopping attacks

3.1. Explain this type of attack.

.....

.....

3.2. Disable the use of the DTP protocol on the ports f0/1 and f0/2.

S2(config)# **int rang f0/1-2**
S2(config-if)# **switchport nonegotiate**

3.3. Configure the two ports in trunk mode.

S2(config-if)# **switchport mode trunk**

3.4. Direct untagged traffic towards the native VLAN 99.

S2(config)#**vlan 99**
S2(config-vlan)#**name 99**
S2(config-vlan)#exit
S2(config)# **int rang f0/0-1**
S2(config-if)# **switchport trunk native vlan 99**

3.5. Display the parameters of the interface f0/1.

S2#**show interfaces trunk**
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q **trunking** **99**
..
S2#**show interface fa0/1 switchport**
Name: Fa0/1
….
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Inactive)

4. Secure the LAN against STP-based attacks.

4.1. Explain this type of attack.

……..

……..

4.2. Configure the switch S2 as the “root bridge”.

S2(config)#**spanning-tree vlan 1 root primary**

4.3. Protect the replacement of the “root bridge” on ports f0/1 and f0/2.

S2(config)# **int rang f0/1-2**
S2(config-if-range)# **spanning-tree guard root**

4.4. Enable the “portfast” option on the f/3 port.

S2(config-if)#**spanning-tree portfast**

4.5. Enable the “bpduguard” option on the same port.

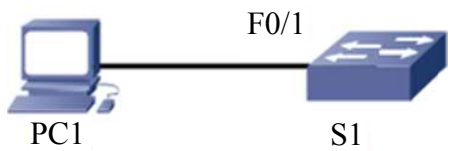
S2(config-if)#**spanning-tree bpduguard enable**

4.6. Display the STP parameters for the f0/1 interface.

S2#sh running-config | begin interface FastEthernet0/1
interface FastEthernet0/1
spanning-tree **portfast**
spanning-tree bpduguard enable
spanning-tree guard root

EXERCISE 11.–

Topology



Addressing table

Device	Interface	IP address / subnet mask	Operating system	Gateway
S1	VLAN1	172.16.0.1/24	c3725-adventerprisek9-mz.124-15.T14	192.168.0.1
PC1	NIC	172.16.0.2/24	Windows 7 or later	192.168.0.1

Objectives

– Secure passwords;

– Simulate attacks on Layer 2.

Software to be used

– GNS3.

Part A: establishing the basic device configuration.

1. Configure the host name as indicated in the topology.

2. Apply the IP addresses to the device interfaces according to the addressing table.

Part B: securing passwords (optional)

On switch S1

1. Set a minimum password length of 8 characters.

2. Set the password "Ci$c0ena" for the privileged mode.

3. Configure the console ports and virtual access lines.

3.1. Set "Ci$c0con" as the password for the console port and set the inactivity interval to 5 minutes.

3.2. Set "Ci$c0vty" as the password on the VTY lines and set the inactivity interval to 2 minutes.

4. Encrypt all passwords.

5. Configure the VTY connections.

On switch S1

– Use the following options to configure the ssh connections:

– domain name: ***tri.local***;

– the user name: ***sshadmin*** with the password: ***Ci$c0ssh***;

– The RSA encryption key is ***1024 bits***;

– the SSH version used is ***version 2***;

– the wait time is ***90s***;

– the number of login attempts is ***3***;

– allow the ***ssh*** and ***telnet*** sessions.

Part C: simulating attacks on layer 2

Download and install the **hyenae**[1] tool.

1. Simulate a MAC address flooding attack.

Objective

1.1. Send a ping between S1 and Host1.

```
S1#ping 172.16.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/20/36 ms
```

1.2. Display the S1 switch table.

```
S1#sh mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
cc01.0d68.0000         Self         1     Vlan1
0200.4c4f.4f50         Dynamic      1     FastEthernet0/0
```

With cc01.0d68.0000 being the MAC address of VLAN1. This value is not necessarily the same when carrying out this exercise.

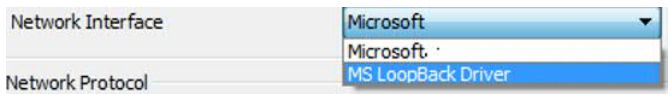
Write the address of your VLAN1:

……..……

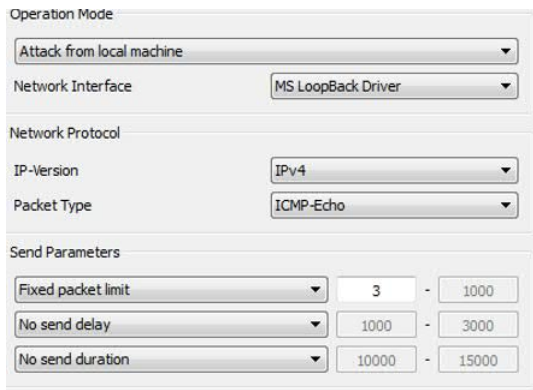
1 https://sourceforge.net/projects/hyenae/.

1.3. Configure an "ICMP-echo" attack using the following parameters:

– ensure that the selected interface is correct;



Configure the following settings as given below:

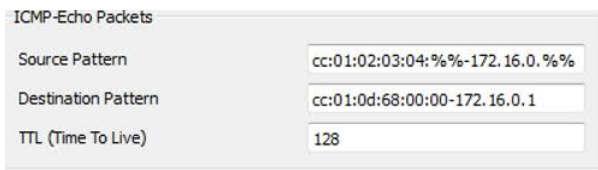


Note that:

- the "**Packet-type"** parameter must be set to an "**ICMP-echo"** attack;

- the "**Fixed packet limit"** must be set to three packets;

– configure the following settings as given below:



Note that:

- the **Destination Pattern** setting must include your VLAN1's MAC address and IP address:

- the two digits of the MAC address must be separated by ":";

- the "%" character indicates that the program will randomly generate values.

1.4. Launch the "ICMP-echo" attack by pressing the "Execute" button:

```
S1#sh mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
cc01.0d68.0000       Self          1     Vlan1
cc01.0203.0411       Dynamic       1     FastEthernet0/0
cc01.0203.04dc       Dynamic       1     FastEthernet0/0
cc01.0203.043a       Dynamic       1     FastEthernet0/0
```

1.5. Launch the "ICMP-echo" attack to fill the switch table with 10 random MAC addresses. To do this, set the following options:

– the "Fixed packet limit" parameter must be set to 10 packets;

– the "Fixed send delay" must be set to 100 ms.

1.6. Verify the result.

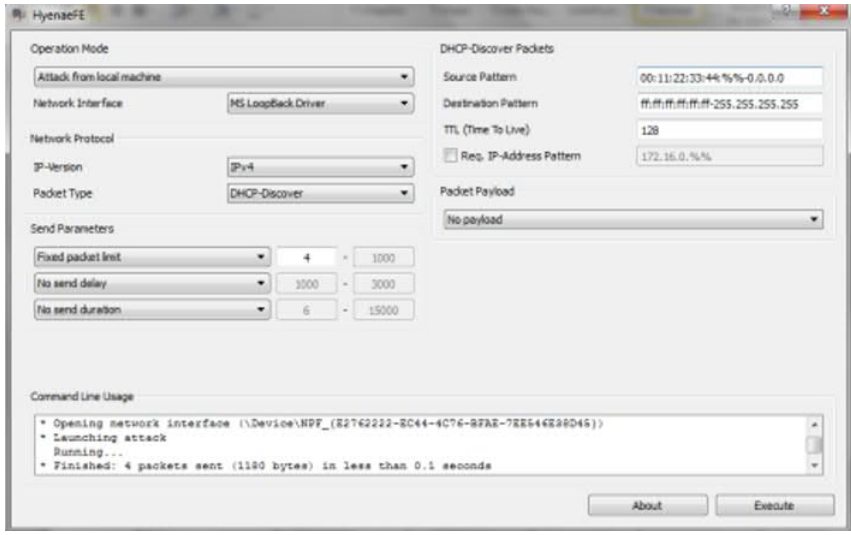
```
S1#sh mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
cc01.0d68.0000       Self          1     Vlan1
cc01.0203.0411       Dynamic       1     FastEthernet0/0
cc01.0203.04dc       Dynamic       1     FastEthernet0/0
cc01.0203.043a       Dynamic       1     FastEthernet0/0
cc01.0203.043d       Dynamic       1     FastEthernet0/0
cc01.0203.04d        Dynamic       2     FastEthernet1
cc01.0203.0460       Dynamic       1     FastEthernet0/0
cc01.0203.04bf       Dynamic       1     FastEthernet0/0
cc01.0203.0495       Dynamic       1     FastEthernet0/0
cc01.0203.04ed       Dynamic       1     FastEthernet0/0
cc01.0203.041e       Dynamic       1     FastEthernet0/0
0200.4c4f.4f50       Dynamic       1     FastEthernet0/0
```

2. Simulate the "DHCP starvation" attack.

2.1. Configure the DHCP service on the S1 switch.

```
S1(config)#ip dhcp excluded-address 172.16.0.1 172.16.0.9
S1(config)#ip dhcp pool pool1
S1(dhcp-config)#network 172.16.0.0 255.255.255.0
S1(dhcp-config)#default-router 172.16.0.1
S1(dhcp-config)#exit
```

2.2. Configure a "DHCP-Discover" attack using the following parameters:



2.3. Launch the attack by pressing the "Execute" button and check the result:

S1#**sh ip dhcp binding**

Bindings from all pools not associated with VRF:

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.16.0.10	0100.1122.3344.93	Mar 01 2002 12:28 AM	Automatic
172.16.0.11	0100.1122.3344.e2	Mar 01 2002 12:28 AM	Automatic
172.16.0.12	0100.1122.3344.9b	Mar 01 2002 12:28 AM	Automatic
172.16.0.13	0100.1122.3344.ce	Mar 01 2002 12:28 AM	Automatic

3. Secure the S1 F0/1 port.

Enable port security on S1 and redo the TP. Ensure that attacks can no longer occur.

8

Cryptography

This chapter will focus on the following topics:

– basic concepts in cryptography;

– different classifications in cryptography:

  - traditional cryptography,

  - modern cryptography,

  - symmetric and asymmetric encryption;

– key management:

  - Diffie-Hellman key exchange;

– hash functions;

– HMAC codes;

– asymmetric cryptography:

  - numerical signatures,

  - public key infrastructure.

8.1. Basic concepts in cryptography

8.1.1. *Definition*

Cryptography is a computer science discipline that makes it possible to protect messages that are judged to be confidential. If the message is intercepted by an unauthorized person, it should be incomprehensible and difficult to decipher.

Computer Network Security, First Edition. Ali Sadiqui.

The four objectives of cryptography are:

– **authentication**: verifying the identity of the source and destination before beginning transmission;

– **integrity**: ensuring that the data transmitted has not been modified during the transmission;

– **confidentiality**: ensuring that only authorized persons can consult the data;

– **non-repudiation**: ensuring that a message transmitted between two people cannot be questioned by one of the two parties.

8.1.2. *Terminology*

– **Plain text**: denotes all data that we wish to transmit before modification. Plain text may include text, images, videos, audio etc.

– **Encryption**: transforms plain text into incomprehensible data.

– **Encrypted text**: refers to text obtained after applying the encryption algorithm on the plain-text, also **cryptogram**.

– **Decryption**: refers to the recovery of plain text from encrypted text.

– **Encrypt**: denotes a sequence of operations to encrypt and decrypt the data.

– **Key**: refers to a parameter that allows the encryption and decryption of the data.

– **Cryptanalysis**: refers to all the techniques and methods used to try to recover the plaintext from the encrypted text.

8.2. The different classifications of cryptology

Cryptography is an ancient technique that is used, in particular, to ensure the confidentiality of text messages deemed critical. With the advent of computers nowadays, the field of cryptography has developed enough to allow the encryption of any type of data, in addition to providing encryption algorithms that are difficult to break.

Figure 8.1 presents the main features of the different classifications of cryptology.

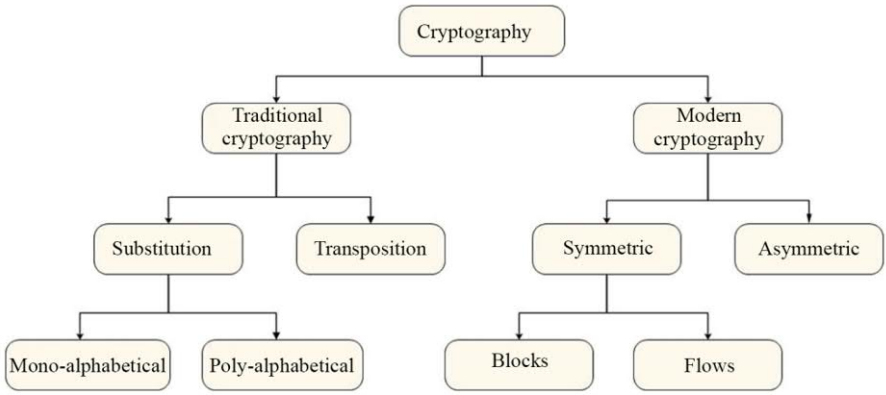


Figure 8.1. *The different classifications in cryptology*

8.2.1. *Traditional cryptography*

The encryption methods commonly used by this cryptography include:

8.2.1.1. *Substitution encryption*

There are two kinds of substitution encryption:

– **mono-alphabetic substitution**: this consists of replacing a character by only one other character to avoid ambiguity during decryption. The oldest and best-known encryption methods in this category we find:

- the Caesar cipher: based on a simple shifting of letters;

- the *Atbash* cipher: based on writing the alphabet in reverse.

NOTE.– To make this method harder to decipher, it is possible to choose only certain letters to be replaced. The exact substitution method can be called an encryption key.

– **the polyalphabetic substitution** consists of replacing one character with another, which is chosen dynamically, determined by the encryption key, instead of being chosen in a fixed manner.

Example: let us encrypt the word “ABCABD” using the key “123” which indicates that the first character will be shifted by one space, the second by two and the third by three spaces and so on. This will give the following result: “BDFBDG”.

8.2.1.2. *Transposition encryption*

Among other things, this method uses the rearrangement of the order of letters following well-defined rules.

Example: let us encrypt the text “ISTA BAB TZIMI” using the key “7514263”, using transposition encryption.

In order to do this, we create the following table:

– the first line consists of the key values;

– we then fill the table by filling in the letters of the message to encrypt. The last line may remain incomplete.

Result:

7	5	1	4	2	6	3
I	S	T	A	B	A	B
T	I	Z	I	M	I	

The result is the concatenation of characters following the order of the columns from 1 to 7: TZBM BAIS IAII T.

NOTE.– In some cases the encryption case may be defined as a series of characters. In this case, each character will be associated with a numerical value and the previous procedure will then be applied.

8.2.2. *Modern cryptography*

8.2.2.1. *Block cipher*

A block cipher XE consists of dividing data into chunks, whose size is generally fixed (between 32 and 512 bits), and which are then encrypted one after another. The general principle underlying a block cipher can be summarized as follows:

1) replacing the characters using a binary code;

2) dividing this chain into blocks of a given length.

3) encrypting a block bit by bit based on a key;

4) repeat Step 3 as many times as needed;

5) move on to the next block.

A non-exhaustive list of block cipher algorithms includes:

– Digital Encryption Standard (**DES**);

– Advanced Encryption Standard (**AES**);

– Triple Digital Encryption Standard (**3DES**);

– Blowfish;

– International Data Encryption Algorithm (**IDEA**).

8.2.2.2. *Stream cipher*

A stream cipher consists of continuously acting on the data without needing to gather a block of data to start the operation. This type of encryption is often used for real-time communication as it has the property of being faster. A non-exhaustive list of block ciphers includes the RC4 **and SEAL standards.**

8.2.3. *Symmetric and asymmetric encryption*

8.2.3.1. *Symmetric encryption*

– In symmetric encryption, the same key is used for encryption and decryption, resulting in the need to keep the key confidential.

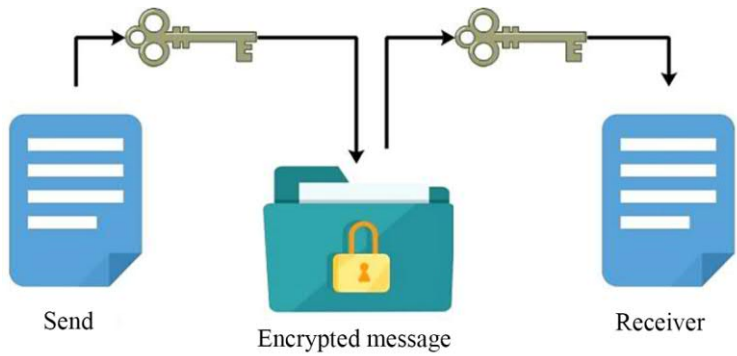


Figure 8.2. *Symmetric encryption*

– A non-exhaustive list of symmetric encryption algorithms includes:

- DES;

- 3DES;

- **AES**;

- **IDEA**;

- **RC2, RC4, RC5, RC6**;

- **Blowfish**.

– Symmetric encryption algorithms are most commonly used for data protection as they offer a quick processing-time and a reasonably high level of security in the presence of a large key. However, its vulnerability lies in the method used to exchange the shared key.

8.2.3.2. *Asymmetric encryption*

– In asymmetric encryption (or public key encryption) a different key is used for the encryption and decryption of data and it is impossible to generate one from the other.

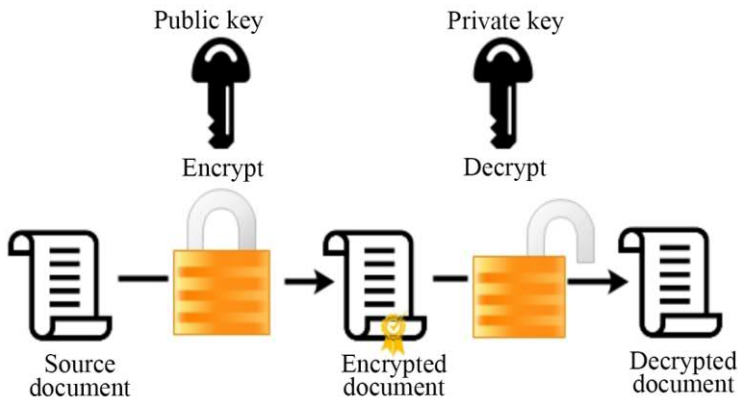


Figure 8.3. *Asymmetric encryption*

Asymmetric encryption algorithms include:

– **RSA**: named for the initials of its creators: Rivest, Shamir and Adleman;

– **DH**: DH (Diffie-Hellman) is an asymmetric encryption algorithm that enables two hosts to exchange shared, secret keys over an unreliable network. This protocol is often combined with symmetric algorithms such as 3DES and AES;

– **DSA**: the digital signature algorithm developed by the National Security Agency of the United States.

– Asymmetric algorithms are slower compared to symmetric algorithms. They are typically used in cases of low-volume encryption, such as digital signatures and key exchange.

NOTE.– A more detailed account of asymmetric encryption is provided later in this chapter (see section 8.6).

8.3. Key management

8.3.1. *Introduction*

The objectives of cryptography rely to a great extent on the protection of encryption keys. It is very important to put in place an efficient and reliable management for securely storing and distributing encryption keys. This management is vital for the success of any encryption project.

There are two approaches to key management to help address this problem:

– **manual management**: consists of manually configuring, on each device, all the parameters of a secured link including encryption keys. This approach has proven to be relatively practical in a static and small environment. However, it is not appropriate for a large network;

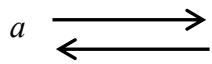
– **automatic management**: this consists of using a protocol (e.g. ISAKMP) to dynamically configure all parameters of a secured link.

8.3.2. *Diffie-Hellman key exchange*

Diffie-Hellman (DH) is a method that allows two network elements to put in place a system by which they can exchange their secret keys in a protected manner. This method makes it possible to create a new, common secret key based on the two initial secret keys, without using a secure channel to exchange them.

Functioning

Step	U1	U2
1	The two users choose together: – a prime number ***p***; – an integer ***g***, such that $\mathbf{1 \leq g \leq p-1}$. Note: this exchange does not need to be secure.	

2	**U1** chooses a random value ***A***	**U2** chooses a random value ***B***
3	**U1** calculates the value: $a = g^A (mod\ p)$	**U2** calculates the value: $b = g^B (mod\ p)$
4	**U1** and **U2** exchange the values of ***a*** and ***b.***  **Note:** this exchange does not need to be secure.	
5	**U1** calculates the value: $K = b^A (mod\ p)$	**U1** calculates the value: $K = a^B (mod\ p)$
Both users then share an identical secret key **K** without sharing the values A ***and*** B.		

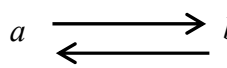
NOTE.

– ***A*** and ***B*** can take the values of the secret keys associated with **U1** and **U2**.

– It is theoretically impossible to find the values ***A*** and ***B*** from the values ***p***, ***g***, ***a***, ***b*** and **K.**

– In practice, the numbers used are numbers with 300 digits raised to the power of 100 digits, which is very strong.

Example

Step	**U1**	**U2**
1	***p*** = ***23*** ***g*** = 7	
2	***A=3***	***B=6***
3	$a = 7^3 (mod\ 23) = 21$	$b = 7^6 (mod\ 23) = 4$
4	**U1** and **U2** exchange the values of ***a*** and ***b.*** 	
5	$K = 4^3 (mod\ 23) = 18$	$K = 21^6 (mod\ 23) = 18$
The two users then share an identical secret key **18**.		

NOTE.– You can now attempt Exercise 3.

8.4. Hash functions

Hash functions are one-way functions used to ensure data integrity. A hash function processes a block of data which may be large or diversified in nature, to return a small hash value, called the "message digest" which is of fixed size. A hash function is characterized by the following properties:

– it is impossible to reconstruct a message from its hash value;

– modifying a message always results in another hash value.

It is impossible for two different messages to have the same hash value.

The list of most commonly used hash functions includes:

– **MD5**: enables the creation of 128-bit message digests;

– **SHA-1**: allows the creation of 160-bit message digests;

– **SHA-2**: enables the creation of 224-bit and 512-bit message digests.

8.5. HMAC codes

Hash-based Message Authentication Code (HMAC) allows you to calculate a message digest by using existing hash functions combined with a shared secret key. This makes it possible to ensure the authentication as well as integrity of the data.

Cisco uses two HMAC functions:

– HMAC-MD5 with a shared key, based on the MD hashing algorithm;

– HMAC-SHA-1 with shared key, based on the SHA-1 hashing algorithm.

8.6. Asymmetric cryptography

8.6.1. *Introduction*

Asymmetric cryptography is a procedure that is based on a pair of keys (public key and private key) for the encryption and decryption of data. Both keys can encrypt the data. However, the complementary key is necessary to decrypt the data.

Asymmetric cryptography is based on complex mathematical algorithms and, thus, takes longer to computer than symmetric algorithms.

Asymmetric cryptography is used to ensure confidentiality and authentication.

8.6.2. *How it works*

Confidentiality	**Confidentiality → public key (encryption) + private key (decryption)** – The public key is used to encrypt; the corresponding private key is used to decipher. – Given that the private key is only present on a single system, this process guarantees confidentiality. – This scenario is often used for key exchange.
Authentication	**Authentication → private key (encryption) + public key (decryption)** – The private key is used to encrypt; the corresponding public key is used for decryption. – Given that the private key is present on only one system, authentication is guaranteed when its public key decrypts the message.

Figure 8.4. gives an overview of the procedure that ensures **confidentiality**.

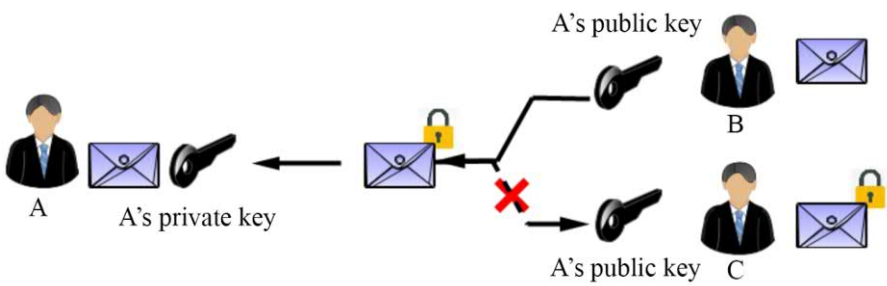


Figure 8.4. *Only A can read the message sent by B*

Figure 8.5. presents the procedure that ensures **authentication**.

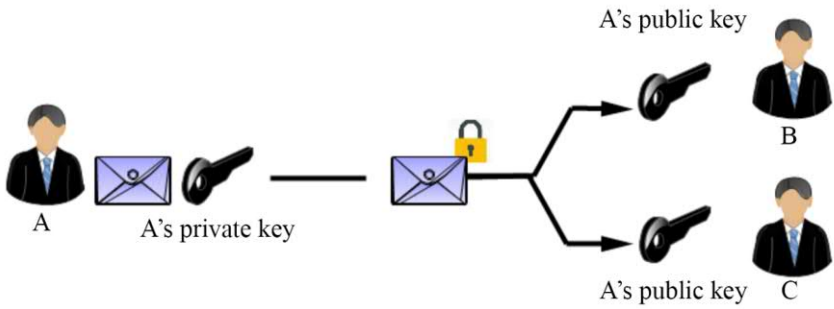


Figure 8.5. *Only A can have sent this message*

8.6.3. *Digital signatures*

8.6.3.1. *Introduction*

A digital signature can ensure the integrity of an electronic document and authenticate the author of the document. It is characterized by the following properties:

– it cannot be falsified;

– it is part of the signed document and cannot be moved to another document;

– a signed document cannot be modified further.

A digital signature offers three security functions:

– the authenticity of the signatory: the identity of the signatory has been approved definitively;

– integrity of the data: digital signatures guarantee that the document has remained intact from the time of transmission;

– non-repudiation: the signatory cannot repudiate the signature on the document.

8.6.3.2. *How it works*

The process of validating a signed document, sent by User A to User B, can be summarized as follows:

Step 1: signing the document

The first user, "A", will:

1) generate a private key **Kpr** and a public key **Kpb**;

2) calculate the hashing value of the document using a hash function **H**;

3) encrypt the hash value using their private key **Kpr**;

4) send the following information to the recipient, “B”:

- the public key **Kpb**;
- the document;
- the function H;
- the encrypted hash value.

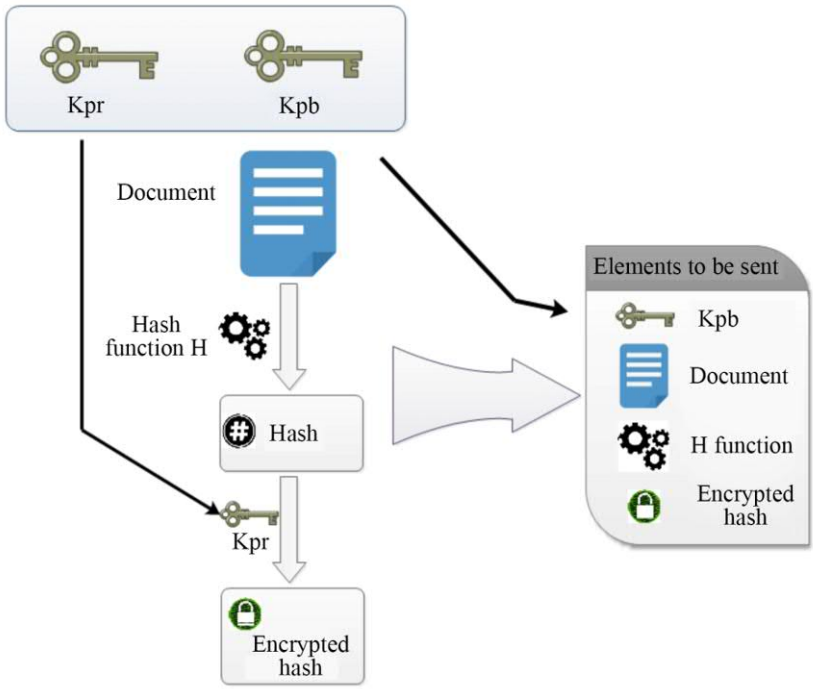


Figure 8.6. *The signature of the document*

Step 2: the verification of the signed document

The second user, “B” will then:

1) decrypt the hash value using the public key **Kpb**;

2) calculate the hash value of the document using the hash function **H**;

3) compare the message digest generated by the document and the message digest previously decrypted using the public key **Kpb**. If the two message digests are identical, the signature is valid.

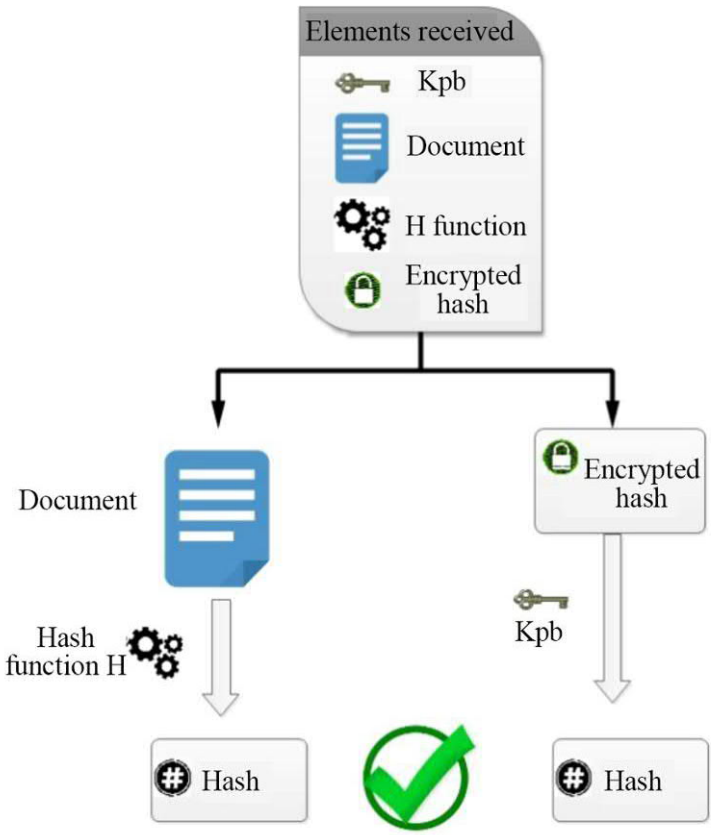


Figure 8.7. *Verifying the signed document*

8.6.4. *Public key infrastructure*

8.6.4.1. *Introduction*

A Public Key Infrastructure (PKI) is a set of services that can ensure the confidentiality, integrity and authentication of data in an organization, and is based on the fundamental principles of asymmetric encryption. PKI solutions are based on digital certificates and the guarantee of a reliable third party.

8.6.4.2. *Terminology*

Concepts	Definitions and characteristics
Certification Authority (CA)	– A Certification Authority is a reliable organization that makes it possible to associate public keys with users, companies, devices etc. – This authority is given the responsibility of digitally signing and publishing these public keys and guaranteeing their authenticity. – A certification Authority may be a private organization (e.g. VeriSign, Cisco etc.) or a public organization.
A certificate	– An electronic document that associates a user name or organization name with a public key. – Digital certificates are digitally signed by a certification authority. – In addition to the public key of the concerned entity, a digital certificate contains information on the validity period of the certification, the algorithm used to sign the certificate etc.
The certificate revocation list (CRL)	– A CRL is a list of certificates that are no longer valid. – A certificate may become invalid for several reasons: - the expiry of its validity date; - the comprising of the private or public key associated with the certificate; - a change in at least one field included in the name of the certificate holder; - Others.

8.6.4.3. *PKI standards*

The most widely used PKI norms include:

– **X.509**: this is a standard created by the organization ITU-T, which defines a basic standard format for public key certificates, the Certificate Revocation Lists (CRL) and other attributes of a certificate;

– **public key cryptographic standards (PKCS)**: these are a set of specifications designed by the "RSA" laboratories for putting in place public key cryptography techniques. The most commonly adopted PKCS in the IT world include:

PKCS Standard	Description
PKCS#1	RSA cryptography standard
PKCS#3	Diffie-Hellman key exchange standard
PKCS#5	Password-based encryption standard
PKCS#7	Cryptographic message syntax standard
PKCS#8	Private key information syntax standard
PKCS#10	Certificate request standard

8.6.4.4. *PKI topologies*

A PKI infrastructure can be implemented using three topologies:

– **simple topology**: in this topology, a single certification authority (the root certification authority) is responsible for issuing all certificates to the end users. This model offers the advantage of being simple. However, it also presents the following drawbacks:

- it is difficult to manage a topology in a large environment;

- requires strictly centralized administration;

- has a critical vulnerability in the use of a single-signature private key. If this key is compromised or stolen, the entire infrastructure will collapse.

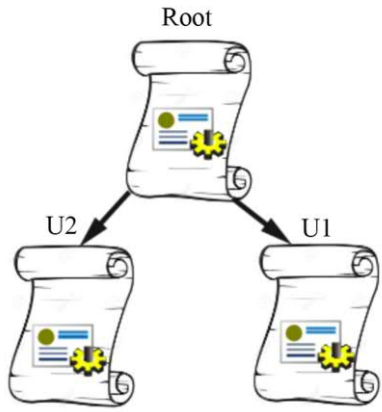


Figure 8.8. *The simple PKI topology*

– **hierarchical topology**: in this topology, a CA can issue certificates directly to end users or delegate this task to subordinate CAs. These subordinate CAs can, in

turn, issue certificates to end users or other certification authorities. The chief advantages of a hierarchical topology are its scalability and simplified management.

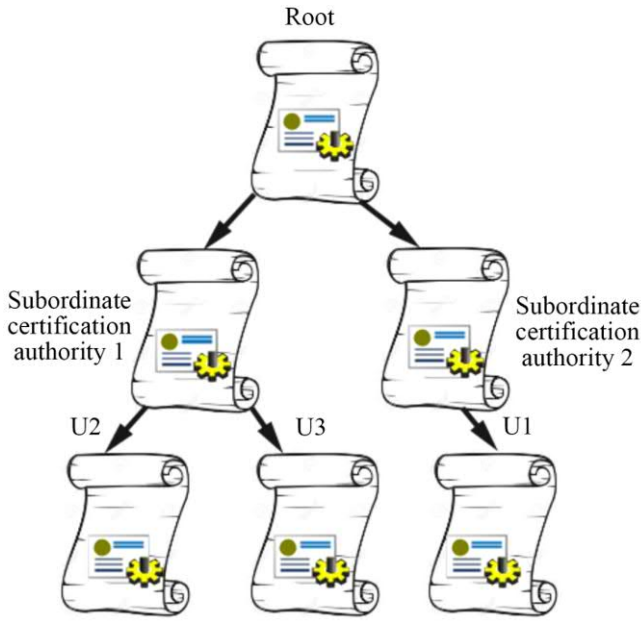


Figure 8.9. *Hierarchical PKI topology*

– **cross topology**: in this topology, multiple Root Certification Authorities establish horizontal trust relationships, mutually validating their certificates.

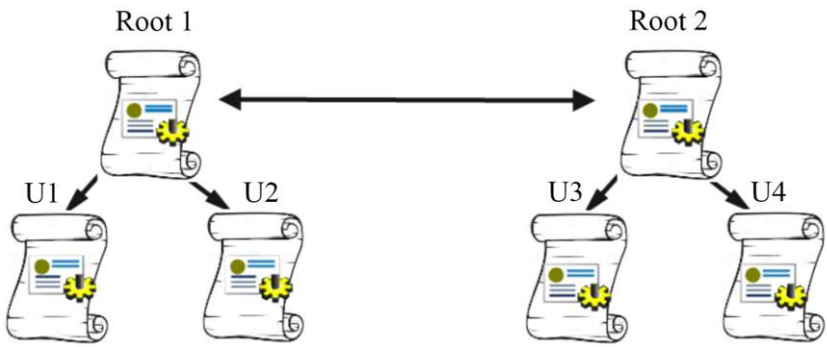


Figure 8.10. *Cross topology*

8.7. Exercises for application

ETL 3.–

Part A: traditional cryptography

1. Use mono-alphabetic substitution to encrypt data.

1.1. Encrypt the text "OFPPT ISTA TRI" using mono-alphabetic encryption with a shift of three characters (the encryption key is equal to 3).

Plain-text	O	F	P	P	T	I	S	T	A	T	R	I
Shift	3	3	3	3	3	3	3	3	3	3	3	3
Encrypted text												

1.2. Encrypt the text "The Office of Vocational Training and Work Promotion" using mono-alphabetic encryption with a shift of 5 characters.

1.3. Decrypt the following text "PEGVCTXSKVETLMIGPEWWMUYI" knowing that it was encrypted using mono-alphabetic encryption with a shift of 4 characters (add spaces).

2. Encrypt with poly-alphabetic substitution.

2.1. Encrypt the text "OFPPT ISTA TRI" using poly-alphabetic encryption with an offset of "132" or (bdc) (the encryption key is 132).

Plain-text	O	F	P	P	T	I	S	T	A	T	R	I
Shift	1	3	2	1	3	2	1	3	2	1	3	2
Encrypted text												

2.2. Encrypt text "Office of Vocational Training and Promotion of Work" using poly-alphabetic encryption with a shift of "202".

2.3. Decrypt the following text "MDGSBTURKSDTILIDOETVMRXI" knowing that it was encrypted using poly-alphabetic encryption with a shift of "134" or (BDE) (add spaces).

3. Encrypt using transposition.

Encrypt the text “OFPPT ISTA TRI” using transposition encryption with the key “52143”.

Part B: modern cryptography

1. Symmetric encryption.

1.1. Review the principle.

.....

.....

1.2. What is the principal weakness of symmetric encryption?

a) The encryption time, considered to be high.
b) The vulnerability of symmetric encryption algorithms.
c) The method for exchanging the shared key.
d) The impossibility of encrypting data other than text.

1.3. Which of the following is not a symmetric algorithm?

a) DES.
b) 3DES.
c) AES.
d) RSA.
e) RC6.
f) Blowfish.

1.4. If 10 people need to communicate using symmetric key cryptography, how many keys are needed?

a) 100.
b) 1000.
c) 9.
d) 10.

1.5. In _____, the key is called the shared secret key.

a) Symmetric encryption.
b) Asymmetric encryption.
(c) (a) and (b).
(d) Neither (a) nor (b).

1.6. What is one of the main drawbacks of using a symmetric algorithm?

a) It does not offer better access control.
b) It is a slower process.
c) It does not provide non-repudiation of the delivery.
d) It is more difficult to implement.

2. Asymmetric encryption.

2.1. Review the principle.

.....

.....

2.2. A pair of keys is used in _____.

a) Symmetric encryption.
b) Asymmetric encryption.
(c) (a) and (b).
(d) Neither (a) nor (b).

2.3. In asymmetric key encryption, the sender uses the _____ key to encrypt the data.

a) Private.
b) Public.
c) Both.
(d) Neither (a) nor (b).

2.4. In asymmetric key encryption, the receiver uses the _____ key to decrypt the data.

a) Private.
b) Public.

c) Both.

(d) Neither (a) nor (b).

2.5. Which statement describes asymmetric encryption algorithms?

a) They have keys ranging in length from 64 to 256 bits.

b) They include DES, 3DES and AES.

c) They are also called shared secret algorithms.

d) They are relatively slow because they are based on algorithms with complicated calculations.

2.6. In what situation is it highly recommended to use an asymmetric encryption algorithm?

a) Logging into a local computer.

b) Making purchases on the Internet.

c) Downloading music via FTP.

d) Sending a large amount of data between two corporate sites.

2.7. In asymmetric key cryptography, what is the public key?

a) The encryption key only.

b) The decryption key only.

c) Both keys.

d) Neither key.

2.8. Which of the following is not an asymmetric algorithm?

a) RSA.

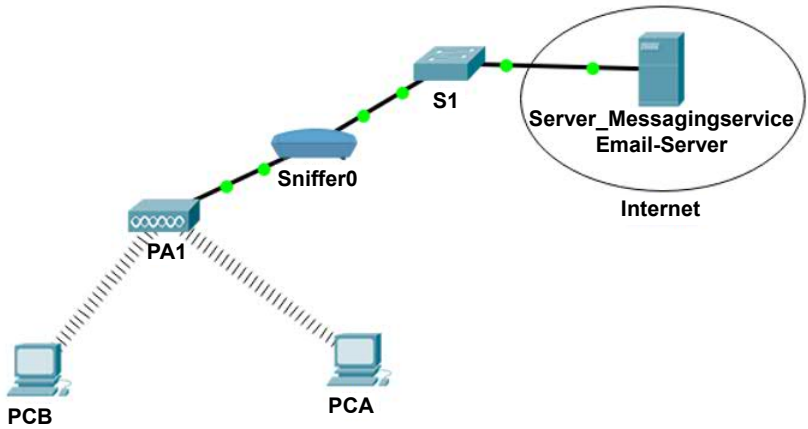
b) DH.

c) DSA.

d) 3DES.

EXERCISE 12.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
PCA	NIC	192.168.0.2	/24	–
PCB	NIC	192.168.0.3	/24	–
Email-Server	NIC	192.168.0.10	/24	–

Objectives

– Use symmetric and asymmetric encryption.

Software to be used

– Packet Tracer.

Part A: establishing the basic device configuration.

Apply the IP addresses to the device interfaces according to the addressing table and check the connectivity between components.

Part B: using symmetric and asymmetric encryption

1. Analyze the risk of sending a clear message.

1.1. Review the role of a Sniffer.

……

……

1.2. Review the principle of the “Man-in-the-middle” attack.

……

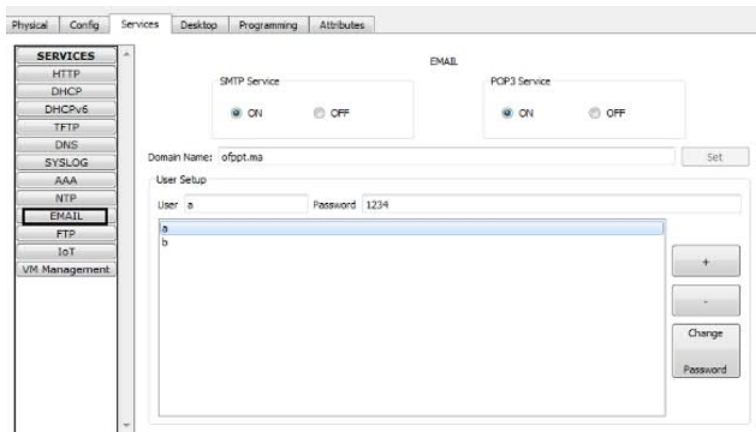
……

1.3. Parameterize and test the Sniffer.

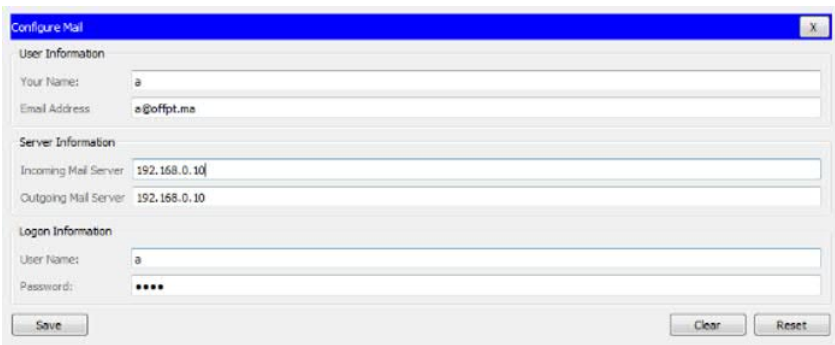
On the Sniffer, filter only the ICMP, POP3 and SMTP packets. Send a **ping** between PCA and PCB and check that this package appears on the Sniffer screen.

1.4. Configure the E-Mail service on the server, on PCA and PCB.

– Configure the E-mail-server as follows:



– Configure the email application on PCA as follows:



– Similarly, configure the E-Mail application on PCB with the options b, b@ofppt.ma, and the account b with its password.

1.5. Send an email message from PCA to PCB.

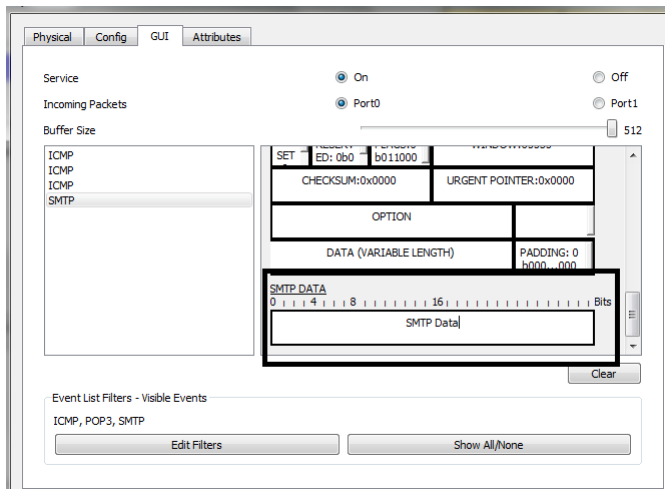
Using the email application on PCA, send the following message:

– to: b@ofppt.ma;

– subjet: Plain-text test

– message: a secret message from A to B.

1.6. Verify that the message has been intercepted by the Sniffer.



1.7. Why would a hacker be able to read the message intercepted by the Sniffer?

……

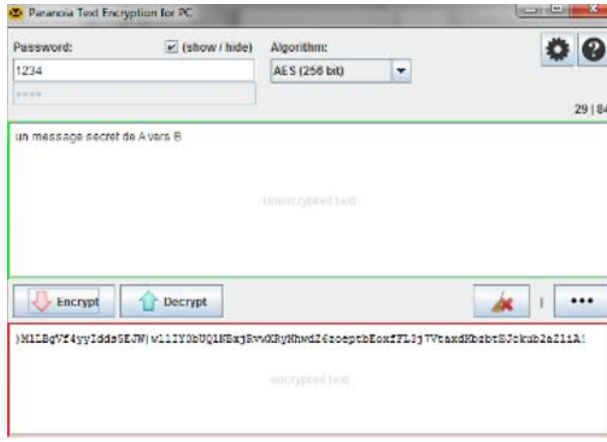
……

2. Secure the sent message using symmetric encryption.

2.1. Download and install the tool "Paranoia Text Encryption for PC"[1].

2.2. Encrypt the previous message using the following parameters:

1 https://paranoiaworks.mobi/ptepc/.



2.3. Define the parameters for this encryption:

– **the plain text**: ....

– **the encryption algorithm**: .....

– **the number of bits in the key**: .....

– **the encryption key**: .....

– **the encrypted text**: ....

– **the type of encryption**:..... ..

2.4. Replace the "plain-text" contents of the previous message with the "encrypted message" and resend it.

2.5. Why is it impossible for a hacker to decrypt the message, even if they know the encryption algorithm, the number of bits in the key as well as the encrypted text?

……...

……...

2.6. What is the other name given to the "encryption key" in symmetric encryption?

……..

……..

2.7. Propose a secure method to exchange the "encryption key" between A and B.

……..

……..

3. Secure a message using asymmetric encryption.

3.1. Download and install the "AEP file encryption" tool[2].

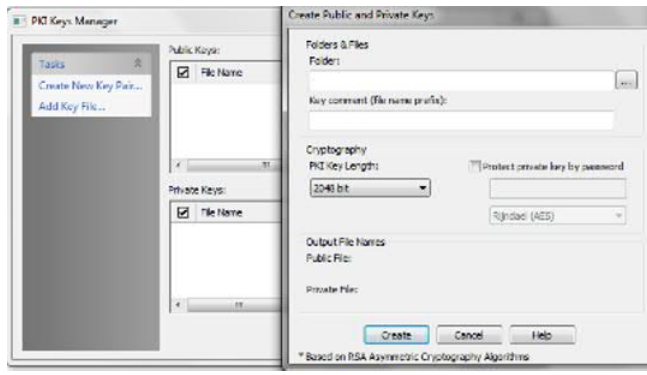
3.2. Review the principle of asymmetric encryption.

……..

……..

3.3. Create the pair of keys for account A.

From the *Tools / RSA Key Generator/* menu, click on "Create new Key Pair".



Choose a folder on the desktop and fill in the comment with "A" then click on "Create" and confirm.

3.4. Define the parameters for this encryption:

– **the encryption algorithm**: .....

– **the number of bits in the key**: .....

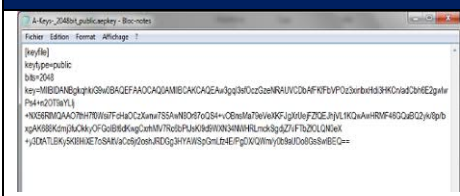
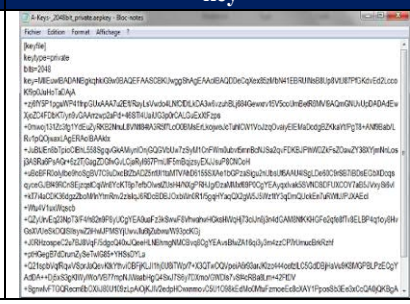
2 http://www.aeppro.com/download/latest.shtml.

– **the name of the file name containing the public key:** .....

– **the name of the file name containing the private key**: .....

– **the type of encryption:** .....

3.5. Display the contents of both keys using the “Notepad” software.

Example of the content of the public key	Example of the content of the private key
	

3.6. To encrypt messages exchanged between users A and B (using PCA and PCB), tick the appropriate key to use:

Key to be used / User	Must use key _____ to send encrypted data				Must use key _____ to decrypt the data received.			
	Public for A	Private for A	Public for B	Private for B	Public for A	Private for A	Public for B	Private for B
A								
B								

3.7. Which of these objectives of cryptography was (were) satisfied by applying the method used in question 3.6?

a) Authentication.

b) Integrity.

c) Confidentiality.

d) Non-repudiation.

3.8. Tick the correct key to us to digitally sign messages exchanged between users A and B:

Key to use / User	Must use key _____ to send signed data			
	Public for A	Private for A	Public for B	Private for B
A				
B				

3.9. Which of these objectives of cryptography was (were) satisfied by applying the method used in question 3.8?

a) Authentication.

b) Integrity.

c) Confidentiality.

d) Non-repudiation.

4. Secure a message using hash functions.

4.1. Download and install the "**HashTool**" program[3].

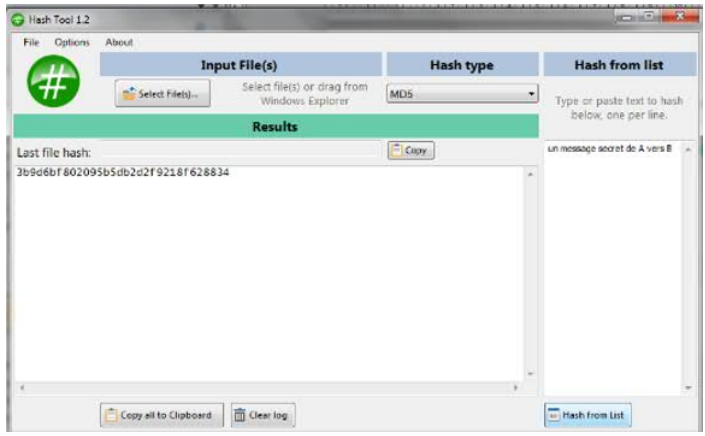
4.2. Review the definition of a hash function.

.....

.....

4.3. In the dedicated zone, paste the text "A secret message from A to B" and compute the hash value.

3 https://md5-hash.soft112.com.



Fill in the following values:

– the **text to be secured**: .....

– the **hash function used**: .....

– the **hash value**: .....

4.4. Using the same hash function and after making the required changes to the original text, write the first 10 digits of the hash value of the following texts:

Text	**Modification**	**The first 10 digits of the hash value for the following texts**
A secret message from A to B.	Add a full-stop at the end	
A secret message from A to B	Add a space between the words "message" and "secret"	
A secret message from A to B	Add a space at the end of the sentence	
A secret message from A to B	Add a space at the beginning of the sentence	

4.5. Using the same hash function and after making the requested changes to the original file, write the first ten digits of the Hash value of the following image files:

NOTE.– The original file, whose path is *C:\Users\Public\Pictures\Sample Pictures/Chrysanthème.jpg,* can be used as an example.

Image	Modification	The first 10 digits of the hash value of the following text
	No modification	
	Using the Paint software, add a small, nearly-invisible dot and save the file.	
	Resize the file to 99% using Paint and save the file.	

4.6. Which of the objectives of cryptography has been (were) satisfied by applying the procedures used in questions 4.4 and 4.5?

a) Authentication.

b) Integrity.

c) Confidentiality.

d) Non-repudiation.

9

IPsec VPNs

This chapter will focus on the following topics:

– the IPsec protocol:

- objectives of IPsec,
- protocols based on IPsec,
- the IPsec framework,
- the IPsec security association,
- IPsec modes;

– the IKE protocol:

- components of IKE,
- the IKE phases,
- the IPsec framework,
- the IPsec security association,
- the differences between the two IKE versions;

– the configuration of the IPsec VPN.

9.1. The IPsec protocol

9.1.1. *Objectives of IPsec*

IPsec is a security architecture, based on standardized norms, that allows two entities to establish secure communication.

Computer Network Security, First Edition. Ali Sadiqui.

The objectives of the IPsec protocol may be summarized as follows:

– **confidentiality**: this consists of transforming clear text into an encrypted text;

– **data integrity**: uses a hash function or HMAC code to ensure that the data was not modified as it travelled over the network;

– **authentication**: consists of end-to-end authentication of VPNs using a pre-shared key (PSK) or digital signature;

– **antireplay protection**: ensuring that no packet was re-sent during the data exchange.

9.1.2. *Basic IPsec protocols*

The three main components of IPsec are:

– **AH**: this protocol only ensures the integrity of the data and the authentication of the source. AH is appropriate when confidentiality is not required or permitted;

– **ESP**: in addition to the functions offered by AH it offers data confidentiality. It is for these reasons that this is the most widely used protocol;

– **Internet Key Exchange (IKE)**: is a protocol responsible for negotiating a connection before an IPsec transmission is possible.

9.1.3. *The IPsec framework*

IPSec is a norm that uses existing algorithms to implement privacy, integrity, authentication, and key exchange.

The combination of these elements offers the administrator a great deal of flexibility, especially when configuring several connections with different security options.

An IPsec frame contains five basic elements that must be configured to ensure a secured connection.

Figure 9.1 depicts the components of the IPsec configuration.

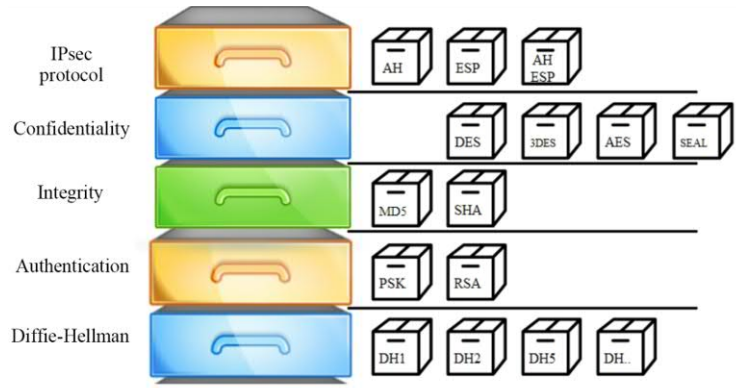


Figure 9.1. *The IPsec framework*

9.1.4. *The IPsec security association*

– An IPsec Security Association (SA) makes it possible to specify the security settings associated with a communication.

– Each SA is identified uniquely by:

- the destination address of the packets;
- the basic IPsec protocol (AH or ESP);
- the SA identifier: the SPI.

– An SA is unidirectional. We thus need two SAs to protect communications in both directions.

All SAs together make up the **Security Policy Database** (SPD).

9.1.5. *IPsec modes*

There are two modes in which IPsec can be used: transport mode and tunnel mode.

– **Transport mode**:

- protects data within a packet. However, the original IP headers remain intact;
- is used for communications between two hosts that support IPsec;
- is generally combined with the GRE protocol to protect traffic.

– **Tunnel mode**:

- the integrality of the original IP packet is protected;

- IPSec encapsulates the original packet, encrypts it, adds a new IP header and then sends it to the other side of the VPN tunnel;

- tunnel mode is most commonly used between IPsec gateways (Cisco routers or ASA firewalls).

9.2. IKE protocol

9.2.1. *Introduction*

Internet Key Exchange (IKE) is a protocol used to dynamically negotiate the security settings associated with IPSec communication. It must be noted that an IPsec implementation can also support the manual management of this exchange of settings. However, the IKE protocol is considered faster and more secure.

IKE is available in two versions. The version v2 offers several advantages, including, among others, the fixing of vulnerabilities in IKEv1 and optimal bandwidth use.

9.2.2. *Components of IKE*

IKE is the combination of three protocols, namely: ISAKMP, SKEME and Oakley. These protocols are grouped together to ensure negotiation and the establishment of a secured communication.

– **ISAKMP**: makes it possible to negotiate SAs between two ends of an IPsec communication.

– **Oakley**: uses the Diffie-Hellman algorithm to carry out key exchanges between both sides of the IPsec connection.

– **SKEME**: defines key exchange techniques that ensure anonymity and non-repudiation.

9.2.3. *IKE phases*

The IKE protocol operates in two main phases to create a secured communication channel between the two IPsec points. The first phase makes it possible to negotiate the tunnel security settings, while the second phase ensures the secured transmission of data.

Figure 9.2. *IKE phases*

NOTE. – We will study how IKEv1 works in this chapter

9.2.3.1. *Phase 1 of IKE*

The characteristics of phase 1 can be summarized as follows:

– the objective is to establish an **ISKMP SA** (or IKE SA). IKE negotiates the security options for the communication such as the encryption algorithm, the hash function, the authentication method and the Diffie-Hellman;

– the SA negotiations are in **both directions**;

– this phase produces three keys. Two keys are used to protect the ISKMP SA messages and the third key is used to produce two other keys used for protecting IPsec exchanges;

– to prove their identity, the sender sends a **hash** of the key associated with the identity and with all previous messages. The identity key is either a **shared secret** or a **pair of private/public keys**;

– the fact that multiple keys are generated guarantees data confidentiality. Even if the shared key is known in the future (or even if the public key used is comprised) the data will always be protected as it is encrypted by the **session key**. The session key is a combination of the identity key with a **random** (**nonce**) value and several other values that are difficult to predict;

– this phase can be established in two modes:

- ***main mode:*** this consists of six messages. It guarantees anonymity on both sides by encrypting the last two messages;

- ***aggressive mode***: this consists of only three messages. It is, therefore, faster, but does not offer the advantages of the Main Mode.

9.2.3.2. *Phase 2 of IKE*

The characteristics of phase 2 can be summarized as follows:

– the objective is to establish an **IPsec SA**;

– the SA negotiations are ***unidirectional.***

The only mode defined for this phase is the ***Quick Mode***.

9.2.3.3. *The differences between the two IKE versions*

The main differences between versions 1 and 2 include:

– **simplified exchange of messages:**

- IKEv1 exchanges nine messages (phase 1 = 6, phase 2 = 3);

- IKEv2 exchanges six messages (phase 1 = 4, phase 2 = 2);

– **security:**

- IKEv1 is susceptible to denial-of-service (DoS) attacks;

- IKEv2 is protected against DoS attacks. A request is only processed if the applicant is identified.

9.3. The site-to-site VPN configuration

9.3.1. *Introduction*

A site-to-site VPN connects two remote LANs in order to securely share resources *via* the internet. It is set up between two sides of a VPN connection in a transparent way for internal hosts.

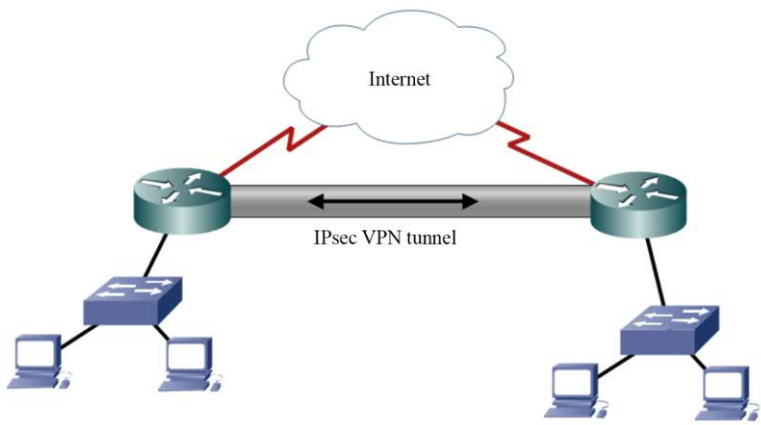


Figure 9.3. *Site-to-Site VPN*

9.3.2. *Configuration of IPsec VPN*

Steps to be followed

To configure a site-to-site VPN using CLI commands, use the following steps:

1) identify the “interesting traffic” by creating an extended ACL;

2) create an IKE policy and configure the required settings for Phase 1;

3) specify the PSK shared key and identify the IP address for the other side of the VPN tunnel;

4) create the IPsec policy required for Phase 2;

5) create the crypto map and configure the specificities of the crypto map;

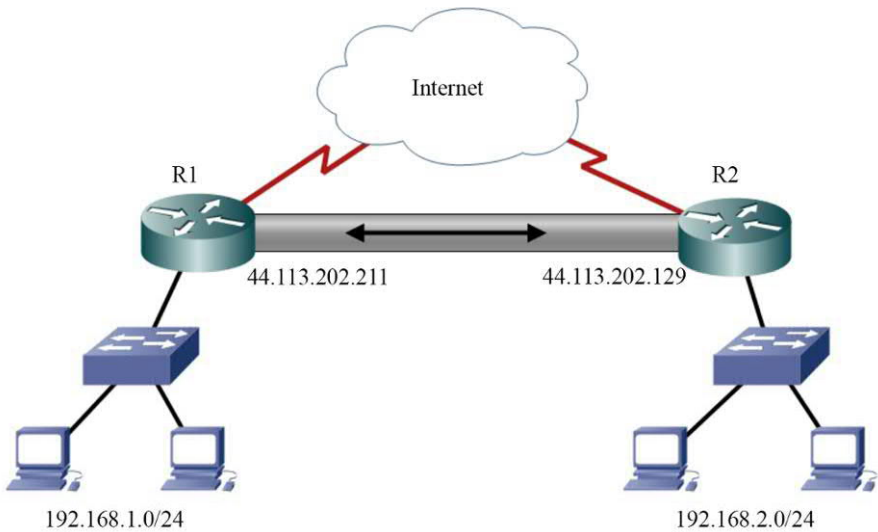
6) apply the crypto map to an interface;

7) verify the VPN tunnel settings.

NOTE.– This order is not essential for all steps.

Example of a configuration

Consider the following network topology:



To configure a VPN link between the two sites, proceed as follows:

1) create an ACL to identify the traffic of interest.

Command	Description
R1(config)# **ip access-list extended** *VPN-ACL*	Creates an extended ACL.
R1(config-ext-nacl)# **permit ip** *192.168.1.0 0.0.0.255 192.168.2.0* 0.0.0.255	Identifies the "interesting traffic".

2) create an IKE policy and configure the settings required for Phase 1.

Command	Description
R1(config)# **crypto isakmp policy** *10*	Creates the IKE policy.
R1(config-isakmp) # **authentication** ***pre-share***	Defines the authentication method.
R1(config-isakmp) # **encr aes** ***128***	Defines the encryption protocol.
R1(config-isakmp) # **hash** ***sha***	Defines the hash function.
R1(config-isakmp) # **group** ***5***	Defines the DH group to be used.
R1(config-isakmp) # **lifetime 86400**	Defines the IKE timeout.

3) specify the shared key (PSK) and identify the IP address on the other side of the VPN tunnel.

Command	Description
R1(config)# **crypto isakmp key** *PassVPN* **address** *44.113.202.129*	Defines the shared key and the IP address for the other side of the VPN tunnel.

4) create the IPsec policy required for Phase 2.

Command	Description
R1(config)# **crypto ipsec transform-set** *R1-to-R2-SET* ***esp- sha-hmac esp-aes 128***	Defines the communication settings for Phase 2.

5) create the encryption map and configure the parameters of the crypto map.

Command	Description
R1(config)# **crypto map** *R1-to-R2-MAP 10* **ipsec-isakmp**	Creates an encryption map connected to IKE policy number 10.
R1(config-crypto-map)# **set transform-set** *R1-to-R2-SET*	Defines the identifier of the IPSec policy required for Phase 2.
R1(config-crypto-map)# **set peer 44.113.202.129**	Sets the IP address for the other side of the VPN tunnel.
R1(config-crypto-map)# **match address** *VPN-ACL*	Sets the ACL ID for the traffic of interest.

6) apply the encryption map to an interface.

Command	Description
R1(config)# **interface** *s0/0/0* R1(config-if)# **crypto map** *R1-to-R2-MAP*	Selects an interface and applies the encryption map.

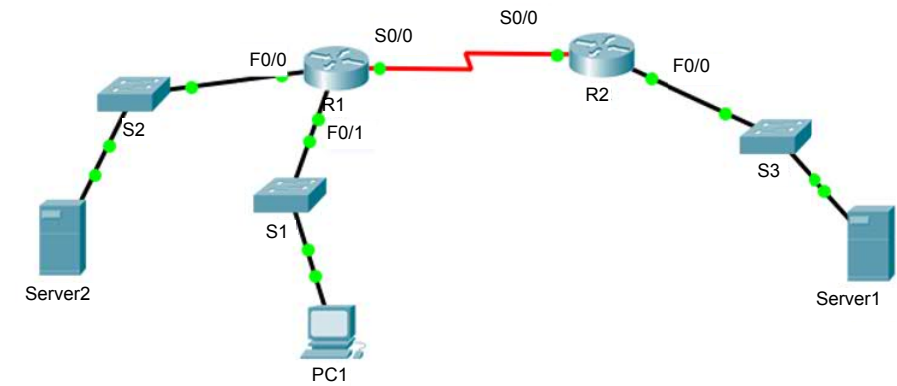
7) verify the VPN tunnel settings.

Command	Description
R1# **show crypto isakmp transform-set**	Displays the configuration for the IPsec policy required for Phase 2.
R1# **show crypto map**	Displays the encryption map configuration.
R1# **show crypto ipsec sa**	Displays the established IPsec tunnels.

9.4. Exercises for application

EXERCISE 13.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	F0/0	192.168.0.1	/24	–
	F0/1	192.168.1.1	/24	–
	S0/0	192.168.10.1	/30	–
R2	S0/0	192.168.10.2	/30	–
	F0/0	192.168.2.1	/24	–
ServerS2	NIC	192.168.0.2	/24	192.168.0.1
PC1	NIC	192.168.1.2	/24	192.168.1.1
ServerS1	NIC	192.168.2.2	/24	192.168.2.1

Objectives

– Securing passwords;

– Configuring a site-to-site IPsec VPN with the Cisco IOS.

Software to be used

– Packet Tracer.

Part A: establishing the basic device settings

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interfaces.

2. Use EIGRP to configure the routing.

2.1. Enable EIGRP on both routers using the value 1 as the AS ID.

2.2. Set the RID value to 1.1.1.1 for R1 and 2.2.2.2 for R2.

2.3. Add all the networks to EIGRP.

2.4. Test connectivity between all network elements.

Part B: securing passwords

On R1

1. Set a minimum password length of 8 characters.

2. Set the password "Ci$c0ena" for the privileged mode.

3. Configure the console, auxiliary ports and virtual access lines.

3.1. Set "Ci$c0con" as the console port password and set the inactivity interval to 5 minutes.

3.2. Set "Ci$c0vty" as the password on the VTY lines and set the inactivity interval to 2 minutes.

3.3. Disable the auxiliary port.

4. Encrypt all passwords.

Part C: configuring a site-to-site IPsec VPN using Cisco IOS

Encrypt the traffic between Server1 and Server2.

1. Identify the "interesting traffic" by creating an extended ACL on R1 and R2.

```
R1(config)# access-list 101 permit ip 192.168.0.0 0.0.0.255 192.168.2.0
0.0.0.255
R2(config)# access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.0.0
0.0.0.255
```

2. Create an IKE policy and configure the settings required for Phase 1.

2.1. What is the role of Phase 1 of the IKE protocol?

.....

.....

2.2. Configure the settings required for Phase 1 on R1.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp) # authentication pre-share
R1(config-isakmp )# encryption aes 256
R1(config-isakmp) # hash sha
```

R1(config-isakmp) # **group 5**
R1(config-isakmp) # **lifetime 3600**
R1(config-isakmp)# **end**

2.3. Based on the previous commands, fill in the following table:

IKE Phase 1 settings	
The ISAKMP **policy ID**	
The authentication **method**	
The **encryption algorithm**	
The **number of bits** used for the encryption key	
The **hash algorithm**	
The **Diffie-Hellman group**	
The **lifetime** of the Security Association	

2.4. Verify the settings of the IKE policy.

R1r#**show crypto isakmp policy**
Global IKE policy
Protection suite of priority 10
encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
Hash algorithm: Secure Hash Standard
Authentication method: Pre-Shared Key
Diffie-Hellman group: #5 (1536 bit)
Lifetime: 3600 seconds, no volume limit

2.5. Repeat the same configuration as above on R2.

3. Specify the PSK shared key and identify the IP address on the other side of the VPN tunnel.

Configure the pre-shared key on both routers.
R1(config)# **crypto isakmp key Tri123 address 192.168.10.2**
R2(config)# **crypto isakmp key Tri123 address 192.168.10.1**

4. Create the IPsec policy required Phase 2.

4.1. What is the role of Phase 2 of the IKE protocol?

……

……

4.2. Create the IPsec policy required for Phase 2 on R1.

R1(config)# **crypto ipsec transform-set 10 esp -aes 256 esp-sha-hmac**

4.3. Based on the previous commands, fill in the following table:

IKE Phase 2 settings	
The identifier for the **transform-set policy.**	
The basic IPsec protocol used.	
The **encryption algorithm**	
The **number of bits** used for the encryption key.	
The **hash algorithm**	

NOTE.– It is possible to modify the lifetime of an IPsec association so that it is different from the lifetime of an ISAKMP association. This can be done using the command:

R1(config)# crypto ipsec security-association lifetime seconds 1800

4.4. Verify the settings of the transform-set policy.

R1#**show crypto ipsec transform-set**
Transform set 10: { { esp -256-aes esp-sha-hmac }
will negotiate = { Tunnel, },

4.5. Repeat the same configuration on R2.

5. Create the crypto map and configure the parameters of the crypto map.

5.1. Create a crypto map on R1.

R1(config)# **crypto map carte_crypto1 10 ipsec -isakmp**
R1(config-crypto-map)# **match address 101**

```
R1(config-crypto-map)# set  peer 192.168.10.2
R1(config-crypto-map)# set  transform-set 10
R1(config-crypto-map)# exit
```

5.2. Based on the previous commands, fill in the following table:

The settings for the crypto map	
The name of the crypto map	
The ISAKMP policy ID	
The ACL identifier for interesting traffic	
The IP address for the other side of the VPN tunnel	
The identifier for the transform-set policy	

5.3. Repeat the same configuration as above on R2.

6. Apply the crypto map to the appropriate R1 and R2 interfaces.

```
R1(config)# interface S0/0
R1(config-if)# crypto map carte_crypto1
R2(config)# interface S0/0
R2(config-if)# crypto map carte_crypto2
```

7. Verify the VPN tunnel settings.

7.1. Verify the crypto map settings.

```
R1#show crypto map
Crypto Map carte_crypto1 10 ipsec  -isakmp
      Peer = 192.168.10.2
      Extended IP access list 101
          access-list 101 permit ip 192.168.0.0 0.0.0.255 192.168.2.0
0.0.0.255
      Current peer: 192.168.10.2
      Security association lifetime: 4608000 kilobytes/3600 seconds
      PFS (Y/N): N
      Transform sets={
            10,
      }
      Interfaces using crypto map carte_crypto1:
            Serial0/0
```

7.2. Display the ISAKMP and IPsec security associations.

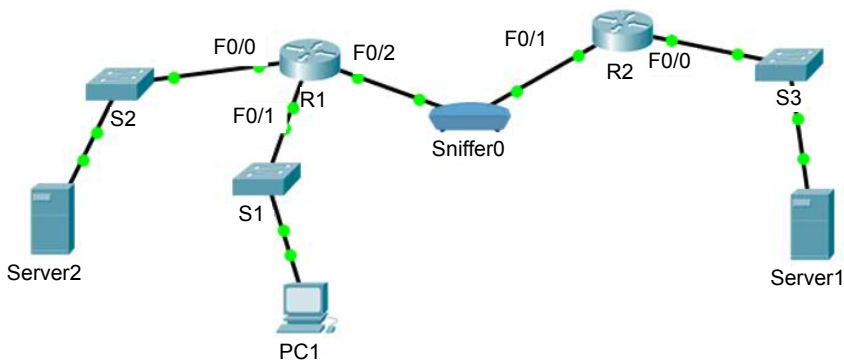
```
R1#show crypto isakmp sa
 IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status

IPv6 Crypto ISAKMP SA
R1# sh          ow crypto ipsec sa
interface: Serial0/0/0
Crypto map tag: carte_crypto1, local addr 192.168.10.1
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168. 0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 192.168.10.2 port 500
PERMIT, flags={origin_is_acl ,}
…
```

7.3. Send out a **ping** between Server2, PC1 and Server1 and once again display the ISAKMP and IPsec security associations.

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id    slot      status
192.168.10.2 192.168.10.1 QM_IDLE        1033       0 ACTIVE
```

7.4. Replace the serial link between the two routers by a FastEthernet (or Ethernet) link and add a Sniffer to capture the frames exchanged between the two routers.



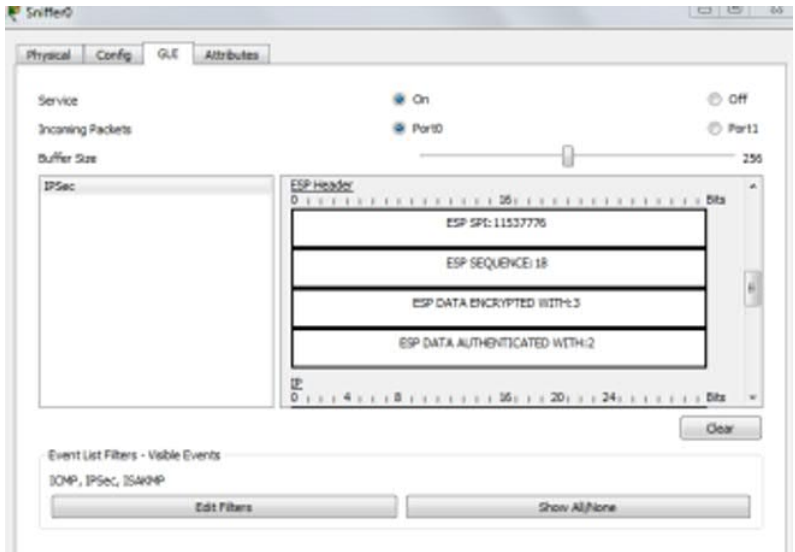
For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

NOTE.– The IP addresses of the FastEthernet interfaces must be identical to those of the IP addresses of the serial interfaces

7.5. Apply the crypto mp to the appropriate R1 and R2 interfaces.

R1(config)# **interface F0/2**
R1(config-if)# **crypto map carte_crypto1**
R2(config)# **interface F0/1**
R2(config-if)# **crypto map carte_crypto2**

7.6. Ping between Server 2 and Server 1 and explain the IPsec frame captured by the Sniffer.



……

……

7.7. Why have security associations been created only for traffic between Server2 and Server1 and not for traffic between PC1 and Server1?

……..

……..

NOTE.– ISAKMP frames can also be captured if, after saving the configuration, one of the two routers is restarted.

10

Studying Advanced Firewalls

This chapter will focus on the following topics:

– CISCO ASA firewalls:

  - ASA models,

  - modes of using ASA equipment,

  - an overview of ASA 5505;

– configuring ASA using CLI:

  - the types of ASA licenses,

  - configuring the interfaces,

  - configuring the DHCP service,

  - configuring ACLs,

  - configuring the NAT service,

  - configuring the AAA;

– configuring Cisco devices using the CCP and ASDM graphic tools;

– the TMG 2010 firewall.

10.1. Cisco ASA firewalls

10.1.1. *Introduction*

A Cisco ASA (Adaptive Security Appliance) is a security device that combines a firewall, an antivirus, an Intrusion Prevention System (IPS) and VPN functionalities.

Computer Network Security, First Edition. Ali Sadiqui.

It thus offers a wide range of technologies and solutions for effective network security.

10.1.2. *ASA models*

– There are different models of ASAs. All the models offer advanced firewall and VPN functionalities. The biggest difference between the models is the maximal flow of traffic that can be managed by each model and the number and the types of interfaces. An ASA model is chosen based on the requirements of an organization, such as the flow, maximal connections per second and the company's budget.

– ASA devices also support virtualization environments. These environments run the same software as the physical device in order to offer the same security features.

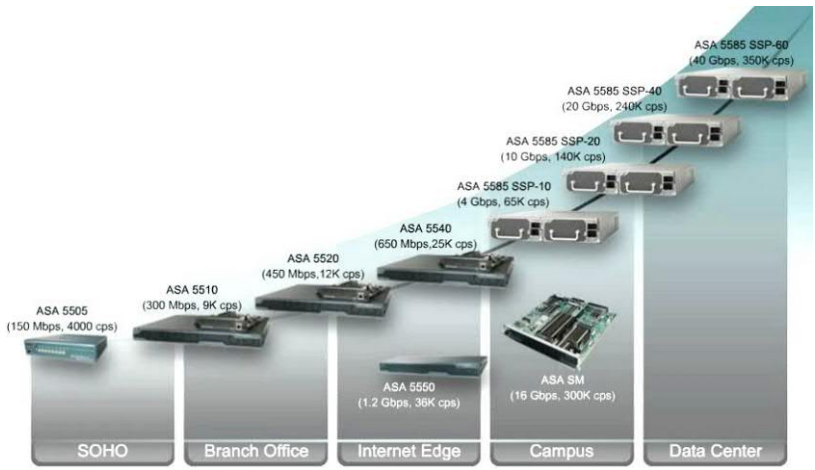


Figure 10.1. *The different ASA models*[1]

NOTE.– In this chapter, we will restrict ourselves to studying the ASA 5505 model and firewall functionalities.

10.1.3. *Modes for using ASA devices*

– **Router mode**:

- this is the conventional mode of deployment;

1 The official Cisco training site, Cisco Networking Academy, https://www.netacad.com.

- this mode supports multiple interfaces and each interface is found on a different sub-network with a separate IP address;

- the ASA reacts like a router in the network and can carry out Network Address Translation (NAT) between connected networks.

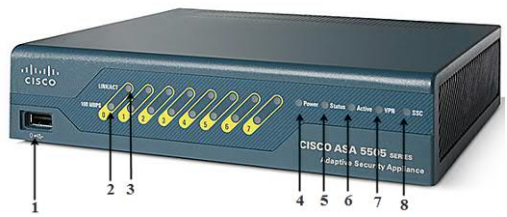
– **Transparent mode**:

- the ASA works as a Layer 2 component;

- this mode supports multiple interfaces, including dynamic routing protocols and VPN features.

10.1.4. *An overview of ASA 5505*

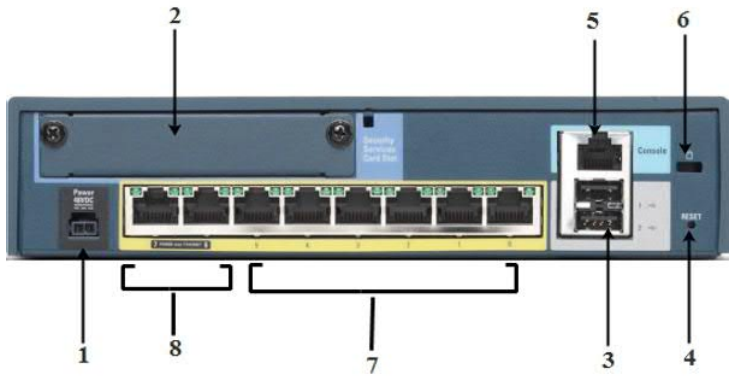
Front view of ASA 5505



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

1	**USB interface**: used notably for backup or updates.
2	**Speed indicator**: – a steady green light indicates a bandwidth of 100 Mo/s; – if the light is off, this indicates a bandwidth of 10 Mo/s.
3	**Link indicator:** – a steady green light indicates that a network link has been established; – a flashing green light indicates network activity.
4	**Electricity indicator**: a green light indicates that the device is receiving power.
5	**Status indicator**: – power indicator: a green light indicates that the device is starting up; – a steady green light indicates that the system is operational; – a steady orange light shows that the system start-up failed.
6	**Active indicator**: A green light indicates that this ASA device is active when configured for switching.
7	**VPN indicator**: a green light indicates that one or more VPN tunnels are active.
8	**SSC indicator:** a green light indicates that an SSC card is in the SSC slot (see the following figure).

Rear view of the ASA 5505



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

1	**Power supply**
2	**SSC slot:** this slot makes it possible to insert an SSC card that provides Cisco's advanced security inspection and prevention services (IPS)
3	**USB interfaces**
4	**The reset button**
5	**The console port**
6	**The anti-theft cable slot**
7	**10/100 Mo/s ethernet ports (port 0 to 5)**
8	**PoE 10/100 Mo/s Ports (port 6 to 7)**

10.1.5. *ASA levels of security*

ASA assigns security levels to classify different network segments based on reliability. The security levels have the following characteristics:

– the security level numbers range from 0 (unreliable) to 100 (very reliable);

– the higher the security level, the more reliable the interface;

– each activated ASA interface must have a name and security level;

– by default, an interface named "inside" takes the value 100 and an interface named "outside" takes the value 0.

10.1.6. *Configuring an ASA with CLI*

10.1.6.1. *The types of ASA 5505 licenses*

ASA 5505 comes with an operating system, under two types of license: a "Basic license" and a "Security Plus license". The Security Plus license supports more features.

Characteristics	Basic license	Security Plus license
The maximum number of connections to the firewall	10,000	25,000
The maximum number of VPN sessions	10	25
The maximum number of VLANs to be created	3, with the restriction that only two zones may communicate with each other.	20, with no restrictions on communication between zones.

10.1.6.2. *Overview of CLI on ASA*

The operating system on ASA devices offers a Command Line Interface (CLI) that looks similar to the one used by the IOS of Cisco routers. However, several commands are different in both operating systems.

Command on the IOS system	The equivalent command on the ASA
enable secret *password*	**enable password** *password*
line con 0 **password** *password* **login**	**passwd** *password*
ip route	**route outside**
show ip interfaces brief	**show interfaces ip brief**
show ip route	**show route**
show vlan	**show switch vlan**
show ip nat translations	**show xlate**
copy running-config startup-config	**write** [**memory**]

10.1.6.3. *Configuring interfaces*

– ASA 5510 has two types of interfaces:

- **routed interfaces**: these are directly configured with IP addresses. The configuration is carried out via an SVI (Switch Virtual Interface).

- **Layer 2 Ethernet interfaces**: These are assigned to VLAN interfaces.

– To configure an SVI on an ASA, proceed as follows:

Command	Description
ciscoasa(config)# **interface vlan** *vlan-id*	Creates an SVI
ciscoasa(config-if)# **nameif** { **inside** | **outside** | *name* }	Gives the SVI a name
ciscoasa(config-if)# **security-level** *level*	Defines or modifies the security level of the SVI
ciscoasa(config-if)# **ip address** *ip-address netmask*	Assigns an IP address and mask to the SVI
ciscoasa(config-if)# **no forward interface vlan** *vlan-id2*	Prevents routing of traffic between the two VLANs

– To configure a Layer 2 interface on the ASA, proceed as follows:

Command	Description
ciscoasa(config)# **interface** *interface/number*	Accesses the interface
ciscoasa(config-if)# **switchport access vlan** *vlan-id*	Assigns it to a VLAN
ciscoasa(config-if)# **no shutdown**	Activates the interface

10.1.6.4. *Configuration of the DHCP service*

You can configure the DHCP service on the ASA using the following steps:

Command	Description
ciscoasa(config)# **dhcpd address** [*start-of-pool*]-[*end-of-pool*] **inside**	Defines the pool of IP addresses to assign to internal users
ciscoasa(config)# **dhcpd domain** *domain-name*	Configures the domain name
ciscoasa(config)# **dhcpd dns** *dns-ip-address*	Configures the DNS IP Address
ciscoasa(config)# **dhcpd lease** *seconds*	Configures the lease duration
ciscoasa(config)# **dhcpd enable** *interface-name*	Enables the DHCP Server Service on the specified ASA interface

NOTE.– You can now attempt Exercise 14.

10.1.6.5. *ACL configuration*

– There are many similarities between ASA ACLs and IOS ACLs. The chief differences can be summarized as follows:

- ASA ACLs use a netmask rather than a generic mask;

- ASA ACLs are named rather than numbered;

- by default, the security levels of an interface apply access control without an ACL being configured.

– ACLs can be configured on an ASA by following the below steps:

Command	Description
ciscoasa(config)# **access-list** *id* **extended** { **deny** |**permit** } *protocol* { *source_addr source_mask* } | **any** | **host** *src_host* | **interface** *src_if_name* [*operator port* [*port*]{ *dest_addr dest_mask* } | **any** | **host** *dst_host* | **interface** *dst_if_name* [*operator port* [*port*]]}	Creates an extended ACL
ciscoasa(config)# **access-group** *acl-id* { **in** | **out** } **interface** *interface-name*	Activates an ACL on an interface

10.1.6.6. *NAT service configuration*

– ASA supports the following NAT types:

- **Dynamic NAT**: consists of translating several private IP addresses into several public IP addresses;

- **Dynamic PAT**: consists of translating several private IP addresses into a single public IP address;

- **Static NAT**: consists of translating a single private IP address to a single public IP address.

– To configure a **dynamic NAT** on an ASA, proceed as follows:

Command	Description
ciscoasa(config)# **object network** *public-pool-obj*	Creates a network object for the pool of public IP addresses

ciscoasa(config-network-object)# {**host** *ip_addr* | **subnet** *net_addr net_mask* | **range** *ip_addr_1 ip_addr_2* }	Defines the pool of public IP addresses using a host address, a subnet or a range of IP addresses
ciscoasa(config)# **object network** *private-pool-obj*	Creates another network object for the pool of private IP addresses
ciscoasa(config-network-object)# { **subnet** *net_addr net_mask* | **range** *ip_addr_1 ip_addr_2* }	Defines the pool of internal IP addresses using a subnet or a range of addresses
ciscoasa(config-network-object)# **nat (** *real-ifc* **,** *mapped-ifc* **) dynamic** *public-pool-object*	Activates dynamic NAT between the two interfaces

– To configure **dynamic PAT** on the ASA, proceed as follows:

Command	Description
ciscoasa(config)# **object network** *pat-obj-name*	Creates a network object for the pool of internal IP addresses
ciscoasa(config-network-object)# { **subnet** *net_addr net_mask* | **range** *ip_addr_1 ip_addr_2* }	Defines the pool of internal IP addresses using a subnet or a range of addresses
ciscoasa(config-network-object)# **nat (** *real-ifc* **,** *mapped-ifc* **) dynamic** [**interface** | *ip-address*]	Activates dynamic PAT between this interface and the public interface

– To configure **static NAT** on ASA, proceed as follows:

Command	Description
ciscoasa(config)# **object network** *static-nat-obj-name*	Creates a network object for the internal IP address
ciscoasa(config-network-object)# **host** *ip_addr*	Defines the internal IP address of the host
ciscoasa(config-network-object)# **nat (** *real-ifc* **,** *mapped-ifc* **) static** *mapped-ip-addr*	Activates the static NAT between the internal IP address and the public interface

ciscoasa(config)# **access-list** *acl-id* **extended permit ip any host** *inside_host*	Creates an extended ACL to allow external users to access the internal IP address
ciscoasa(config-if)# **access-group** acl-id **interface outside**	Applies the ACL to the appropriate interface

10.1.6.7. *AAA configuration*

– An ASA may be configured to authenticate itself using a local user database or an external server, or by using both methods.

– In order to activate AAA authentication for access to **exec**, **http**, **SSH** or **telnet** mode, proceed as follows:

Command	Description
ciscoasa(config)# **aaa authentication enable console LOCAL**	Activates AAA authentication for access to the EXEC mode using the local database
ciscoasa(config)# **aaa authentication http console LOCAL**	Activates AAA authentication for http access using the local database
ciscoasa(config)# **aaa authentication ssh console LOCAL**	Activates AAA authentication for ssh access using the local database
ciscoasa(config)# **aaa authentication telnet console LOCAL**	Activates AAA authentication for telnet access using the local database

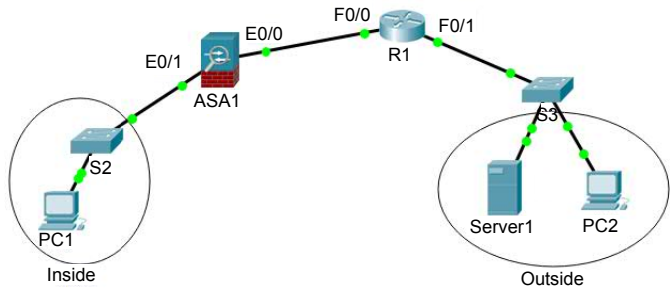
– To activate AAA authentication using an external server, proceed as follows:

Command	Description
ciscoasa(config)# **aaa-server** *server-tag* **protocol** [**tacacs+** | **radius** }	Creates a group of TACACS + or RADIUS servers
ciscoasa(config-aaa-server-group)# **aaa-server** *server-tag* [**(***interfacename***)**] **host** { *server-ip* | *name* } [*key*]	Defines the settings of the AAA server
ciscoasa(config)# **aaa authentication** { **enable** | **http** | **ssh** | **telnet** } **console** *server-tag* [**LOCAL**]	Activates AAA authentication based on the external server

10.2. Exercises for application

EXERCISE 14.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
ASA1	E0/0 (VLAN2)	212.212.1.1	/30	–
	E0/1 (VLAN1)	192.168.1.1	/24	–
R1	F0/0	212.212.1.2	/30	–
	F0/1	192.168.2.1	/24	–
PC1	NIC	192.168.1.2	/24	192.168.1.1
PC2	NIC	192.168.2.2	/24	192.168.2.1
Server1	NIC	192.168.2.3	/24	192.168.2.1

Objectives

– Secure passwords;

– Configure an ASA 5505 firewall with CLI.

Software to be used

– Packet Tracer.

Part A: establishing the basic device configuration

1. Configure the basic device settings.

1.1. Configure the name of the host as given in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

Part B: securing passwords

On R1

1. Set a minimum password length of 8 characters.

2. Set the password "Ci$c0ena" for the privileged mode.

3. Configure the console, auxiliary ports and virtual access lines.

3.1. Set "**Ci$c0con**" as the console port password and set the inactivity interval to 5 minutes.

3.2. Set "**Ci$c0vty**" as the password on the VTY lines and set the inactivity interval to 2 minutes.

3.3. Disable the auxiliary port.

4. Encrypt all passwords.

5. Create static routes towards the company's internal network.

R1(config)#**ip route 192.168.1.0 255.255.255.0 212.212.1.1**

Part C: configuring an ASA 5505 firewall with CLI

1. Determine the basic characteristics of the ASA device.

1.1. Review the role played by the ASA device.

.....

.....

1.2. Display the characteristics of the ASA device.

```
ciscoasa>
ciscoasa>enable
Password:        (empty)
ciscoasa#
ciscoasa#show version
```

Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)
Compiled on Wed 15-Jun-11 18:17 by mnguyen
System image file is "disk0:/asa842-k8.bin
Config file at boot was "startup-config"
ciscoasa up 19 minutes 18 seconds
Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xfff00000, 2048KB
…

1.3. Based on the output of the previous command, fill in the following table:

The characteristics of the ASA device	
The version of the ASA software being run	
The name of the image file	
The size of the RAM	
The size of the Flash memory	
The number of Ethernet ports	
The type of system license	
The number of VLANs that can be created	

2. Configure the basic settings of the ASA device.

2.1. Configure the name of the host.

ciscoasa(config)#**hostname ASA1**
ASA1(config)#

2.2. Set the system date.

ASA1(config)**#clock set 14:25:00 May 12 2018**

2.3. Configure the password for privileged mode.

ASA1(config)**#enable password 1234**

2.4. Configure the password for telnet connections.

ASA1(config)#**passwd Cisco123**

3. Configure Telnet and SSH access to the ASA from the internal network.

3.1. Configure telnet access from the internal network.

ASA1(config)#**telnet 192.168.1.0 255.255.255.0 inside**

3.2. Set the telnet timeout to 10 minutes.

ASA1(config)#**telnet timeout 10**

3.3. Configure remote ssh access to the ASA.

ASA1(config)#**crypto key generate rsa modulus 1024**
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.
Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait..

ASA1(config)# **ssh 192.168.1.0 255.255.255.0 inside**
ASA1(config)# **ssh timeout 10**

4. Configure the interfaces of the ASA device.

4.1. Configure a VLAN 1 logical interface for the internal network and set the security level to the highest setting.

ASA1 (config)# **interface vlan 1**
ASA1 (config-if)# **nameif inside**
ASA1 (config-if)# **ip address 192.168.1.1 255.255.255.0**
ASA1 (config-if)# **security-level 100**

4.2. Configure a VLAN 2 logical interface for the external network and set the security level to the lowest setting.

ASA1 (config)# **interface vlan 2**
ASA1 (config-if)# **nameif outside**
ASA1 (config-if)# **ip address 212.212.1.1 255.255.255.252**
ASA1 (config-if)# **security-level 0**

4.3. Assign ASA ports to the connected VLANs.

ASA1 (config)# **interface e0/1**
ASA1 (config-if)# **switchport access vlan 1**
ASA1 (config-if)# **no shutdown**

ASA1 (config-if)# **interface e0/0**
ASA1 (config-if)# **switchport access vlan 2**
ASA1 (config-if)# **no shutdown**

4.4. Check the configuration and allocation of ports.

ASA1#**sh interface ip brief**

Interface	IP-Address	OK? Method	Status	Protocol
Ethernet0/0	unassigned	YES unset	up	up
Ethernet0/1	unassigned	YES unset	up	up
Ethernet0/2	unassigned	YES unset	up	up
…				
Vlan1	192.168.1.1	YES manual	up	up
Vlan2	212.212.1.1	YES manual	up	up

ASA1#**sh ip address**

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
Vlan1	inside	192.168.1.1	255.255.255.0	manual
Vlan2	outside	212.212.1.1	255.255.255.252	manual

ASA1#**sh switch vlan**

VLAN	Name	Status	Ports
1	inside	up	Et0/1, Et0/2, Et0/3, Et0/4 Et0/5, Et0/6, Et0/7
2	outside	up	Et0/0

4.5. Ensure that the **ping** command was successful between ASA1 and R1 and between ASA1 and PC1.

5. Configure a default static route for the ASA.

5.1. Configure a default route towards the external networks.

ASA1(config)#**route outside 0.0.0.0 0.0.0.0 212.212.1.2**

5.2. Display the routing table.

```
ASA1#sh route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
          Gateway of last resort is 212.212.1.2 to network 0.0.0.0
          C    192.168.1.0 255.255.255.0 is directly connected, inside
             212.212.1.0/30 is subnetted, 1 subnets
          C       212.212.1.0 255.255.255.252 is directly connected, outside
          S*   0.0.0.0/0 [1/0] via 212.212.1.2
```

6. Modify the default security policy applied to the ASA.

6.1. Create a Class-Map to identify authorized traffic.

```
ASA1(config)#class-map CMAP-IN-TO-OUT
```

6.2. Display the options available for the "***match***" command.

```
ASA1(config-cmap)#match?
```

6.3. Select the default traffic.

```
ASA1(config-cmap)#match default-inspection-traffic
ASA1(config-cmap)#exit
```

6.4. Create Policy-Maps to apply access rules to Class-Maps.

```
ASA1(config)#policy-map PMAP-IN-TO-OUT
ASA1(config-pmap)#class CMAP-IN-TO-OUT
ASA1(config-pmap-c)#inspect icmp
ASA1(config-pmap-c)#inspect http
ASA1(config-pmap-c)#exit
```

6.5. Enable this security policy on all ASA interfaces.

ASA1(config)#**service-policy PMAP-IN-TO-OUT global**

7. Test the configuration of your firewall.

– Ensure that it is possible to send a **ping** request from **PC1** to **PC2**.

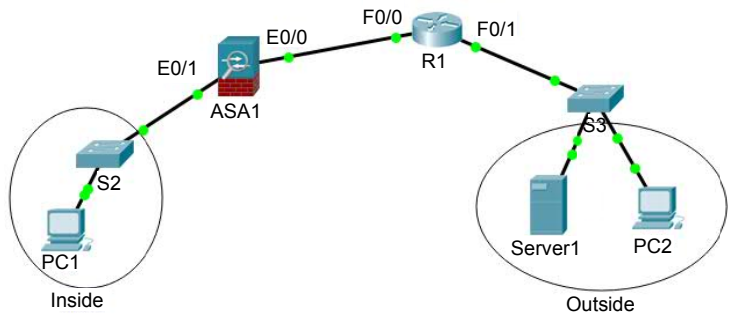
– Ensure that it is not possible to send a **ping** request from **Server1** to **PC1**.

– Ensure that it is possible to access the **Server1** http service from **PC1**.

– Ensure that it is not possible to access the **Server1** ftp service from **PC1**.

EXERCISE 15.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
ASA1	E0/0 (VLAN2)	212.212.1.1	/30	–
	E0/1 (VLAN1)	192.168.1.1	/24	–
	E0/2 (DMZ)	192.168.10.1	/24	–
R1	F0/0	212.212.1.2	/30	–
	F0/1	192.168.2.1	/24	–

PC1	NIC	Automatic		
PC2	NIC	192.168.2.2	/24	192.168.2.1
Server0	NIC	192.168.2.3	/24	192.168.2.1
Serveur_http	NIC	192.168.10.2	/24	192.168.10.1
Server_ftp	NIC	192.168.10.3	/24	192.168.10.1

Objectives

– Configure the ASA 5505 firewall with CLI.

Software to be used

– Packet Tracer.

Part A: establishing the basic device configuration

1. Configure the basic device settings.

1.1. Configure the name of the host as given in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

2. Create static routes towards the company's internal networks.

R1(config)#**ip route 192.168.1.0 255.255.255.0 212.212.1.1**
R1(config)#**ip route 192.168.10.0 255.255.255.0 212.212.1.1**

Part B: configuring the ASA 5505 firewall with CLI

1. Configure the basic settings of the ASA device.

1.1. Configure the name of the host.

ciscoasa(config)#**hostname ASA1**
ASA1(config)#

1.2. Set the system date.

ASA1(config)**#clock set 14:25:00 May 12 2018**

1.3. Configure the password for privileged mode.

ASA1(config)**#enable password 1234**

1.4. Configure the password for telnet connections.

ASA1(config)#**passwd Cisco123**

2. Configure Telnet and SSH access to the ASA from the internal network.

2.1. Configure Telnet access from the internal network.

ASA1(config)#**telnet 192.168.1.0 255.255.255.0 inside**
ASA1(config)#**telnet timeout 10**

2.2. Configure remote ssh access to the ASA.

ASA1(config)#**crypto key generate rsa modulus 1024**

WARNING: You have an RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: y

Keypair generation process begin. Please wait..

ASA1(config)# **ssh 192.168.1.0 255.255.255.0 inside**

ASA1(config)# **ssh timeout 10**

3. Configure the interfaces of the ASA device.

3.1. Configure a VLAN 1 logical interface for the internal network and set the security level to 100.

ASA1 (config)# **interface vlan 1**
ASA1 (config-if)# **nameif inside**
ASA1 (config-if)# **ip address 192.168.1.1 255.255.255.0**
ASA1 (config-if)# **security-level 100**

3.2. Configure a VLAN 2 logical interface for the external network and set the security level to 0.

ASA1 (config)# **interface vlan 2**
ASA1 (config-if)# **nameif outside**
ASA1 (config-if)# **ip address 212.212.1.1 255.255.255.252**
ASA1 (config-if)# **security-level 0**

3.3. Configure a VLAN 3 logical interface for the DMZ network.

ASA1 (config)# **interface vlan 3**

ASA1 (config-if)# **nameif DMZ**

ERROR: This license does not allow configuring more than 2 interfaces with nameif and without a "no forward" command on this interface or on 1 interface(s) with nameif already configured.

3.4. Explain why this error message is displayed.

……

……

3.5. Block any traffic between the internal network (vlan1) and the DMZ (vlan3).

ASA1(config-if)#**no forward interface vlan 1**
ASA1(config-if)#**nameif DMZ**
ASA1(config-if)# **ip address 192.168.10.1 255.255.255.0**
ASA1(config-if)# **security-level 50**

3.6. Assign ASA ports to the connected VLANs.

ASA1 (config)# **interface e0/1**
ASA1 (config-if)# **switchport access vlan 1**
ASA1 (config-if)# **no shutdown**
ASA1 (config-if)# **interface e0/0**
ASA1 (config-if)# **switchport access vlan 2**
ASA1 (config-if)# **no shutdown**
ASA1 (config-if)# **interface e0/2**
ASA1 (config-if)# **switchport access vlan 3**
ASA1 (config-if)# **no shutdown**

3.7. Check the configuration and port allocation using the **sh interface ip brief**, **sh ip address** and **sh switch vlan** commands.

4. Configure the DHCP service on ASA.

4.1. Configure the DHCP service for the company's internal network.

ASA1(config)#**dhcpd address 192.168.1.5-192.168.1.100 inside**
Warning, DHCP pool range is limited to 32 addresses, set address range as: 192.168.1.5-192.168.1.36
ASA1(config)# **dhcpd dns 192.168.1.1**

4.2. Enable the DHCP service on the internal network.

ASA1(config)# **dhcpd enable inside**

4.3. Check that PC1 has received a valid IP address.

NOTE.– On the internal network, the DHCP service is enabled on the ASA services by default.

5. Configure a default static route for the ASA.

ASA1(config)#**route outside 0.0.0.0 0.0.0.0 212.212.1.2**

6. Modify the default security policy applied to the ASA.

6.1. Create a Class-Map to identify authorized traffic.

ASA1(config)#**class-map CMAP-IN-TO-OUT**

6.2. Display the options available for the ***"match"*** command.

ASA1(config-cmap)#**match ?**

6.3. Select the default traffic.

ASA1(config-cmap)#**match default-inspection-traffic**
ASA1(config-cmap)#**exit**

6.4. Create a Policy-Map to apply the access rules.

ASA1(config)#**policy-map PMAP-IN-TO-OUT**
ASA1(config-pmap)#**class CMAP-IN-TO-OUT**
ASA1(config-pmap-c)#inspect icmp
ASA1(config-pmap-c)#inspect ftp
ASA1(config-pmap-c)#inspect http
ASA1(config-pmap-c)#exit

6.5. Enable this security policy on all ASA interfaces.

ASA1(config)#**service-policy PMAP-IN-TO-OUT global**

7. Configure the NAT service on ASA.

7.1. Configure the PAT service to allow the internal network to access the Internet.

```
ASA1(config)# object network inside-internet
ASA1(config-network-object)# subnet 192.168.1.0 255.255.255.0
ASA1(config-network-object)# nat (inside,outside) dynamic interface
ASA1(config-network-object)# end
```

7.2. Configure the static NAT service to allow access to servers in the DMZ zone from the Internet.

```
ASA1(config)# object network dmz-server-http
ASA1(config)# host 192.168.10.2
ASA1(config)# nat (dmzoutside) static 212.212.1.10
ASA1(config)# object network dmz-server-ftp
ASA1(config)# host 192.168.10.3
ASA1(config)# nat (dmz,outside) static 212.212.1.11
```

8. Configure the ACLs to define authorized access.

8.1. Create an ACL to authorize access to DMZ servers.

```
ASA1(config)# access-list outside-dmz extended permit ip any host
192.168.10.2
ASA1(config)# access-list outside-dmz extended permit tcp any host
192.168.10.2 eq www
ASA1(config)# access-list outside-dmz extended permit ip any host
192.168.10.3
ASA1(config)# access-list outside-dmz extended permit tcp any host
192.168.10.3 eq ftp
```

8.2. Activate the ACL on the outside interface

```
ASA1(config)# access-group outside-dmz in interface outside
```

9. Test the configuration of your firewall.

9.1. Check the configuration of your ASA firewall using the command **show running-config**.

9.2. Test the following elements:

– ensure that it is possible to access the **Server0** http service from **PC1**;

– ensure that it is possible to access the http service of Server_http from **PC2** using the IP address **212.212.1.10**;

– ensure that it is possible to access the FTP service of Server_ftp from **PC2** using the IP address **212.212.1.11**.

9.3. Display the NAT translations that were carried out.

ASA1#**sh xlate**

10.3. Configuring Cisco elements with graphical tools

10.3.1. *An overview of the CCP*

Cisco Configuration Professional (CCP) is a graphical tool that facilitates the configuration, monitoring, and troubleshooting of Cisco routers without using Cisco IOS CLI commands.

There are two versions of CCP:

– **CCP:** this is a full version used to organize and manage multiple routers using an application installed on a host;

– **CCP Express:** this is a light version of CCP, available on the router's flash memory. It allows a basic configuration of the equipment.

10.3.2. *An overview of the ASDM*

The Cisco Adaptive Security Device Manager (ASDM) is a Java graphical tool that allows the configuration, monitoring and troubleshooting of Cisco ASA systems.

10.3.3. *Using CCP and ASDM*

Complete Exercise 16.

10.4. The TMG 2010 firewall

10.4.1. *Introduction*

Forefront Threat Management Gateway (TMG) is a Microsoft product that can protect companies against threats arising chiefly from the Web.

This solution includes a firewall, a VPN, URL filtering and an IPS.

Forefront TMG is available in two versions: Enterprise and Standard. Which version is chosen depends on the size of the network infrastructure to be protected.

NOTE.– At present, Forefront TMG 2010 is no longer commercially available but still receives updates and patches from Microsoft.

10.4.2. *Installation and configuration*

Complete Exercise 17.

EXERCISE 16.–

Topology

Addressing table

Device	Interface	IP address / subnet mask	Operating system	Gateway
R1	F0/0	192.168.10.1/24	c2600-adventerprisek9-mz.124-1	–
PC	NIC	192.168.10.2/24	Windows 7 or later	192.168.10.1

Objectives

– Configure a router using Cisco Configuration Professional (CCP).

Software to be used

– GNS3.

Part A: establishing the basic device configuration

1. Install the Cisco Configuration Professional (CCP) tool on PC1.

There is usually no problem installing CCP on a PC running Windows 7 or a later version of Windows. In case of any problem, first ensure that the following minimum parameters are in place:

– Internet Explorer 6.0 or later;

– Java Runtime Environment version 1.6.0 _11 or later;

– Adobe Flash Player version 10 or later.

NOTE.– Other configuration parameters, notably the memory used by the Java applications, may also be required in some cases for the proper functioning of the application.

2. Set the IP address of PC1 to 192.168.10.2/24.

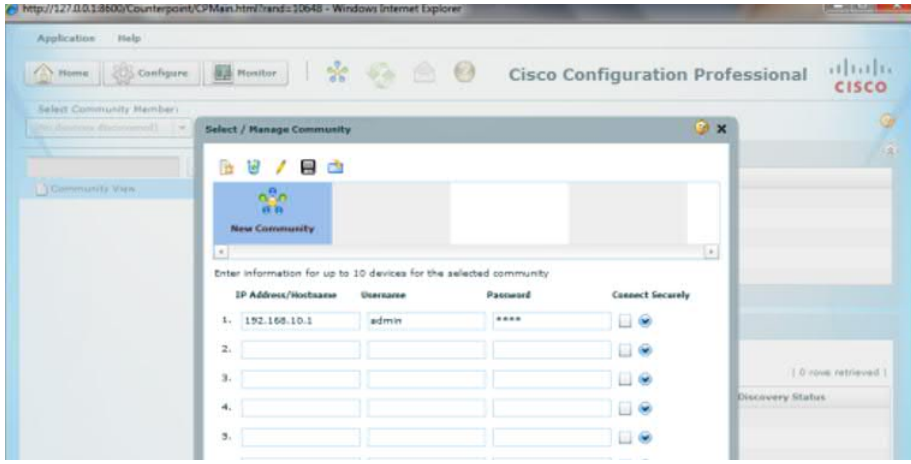
3. Configure the basic R1 settings to support a CCP connection.

```
Router(config)# username admin privilege 15 secret 1234
R1(config)# hostname R1
R1(config)# ip http server
R1(config)# ip http authentication local
R1 (config)# interface E0/0
R1(config -if)# ip address 192.168.10.1 255.255.255.0
R1(config -if)# no shutdown
```

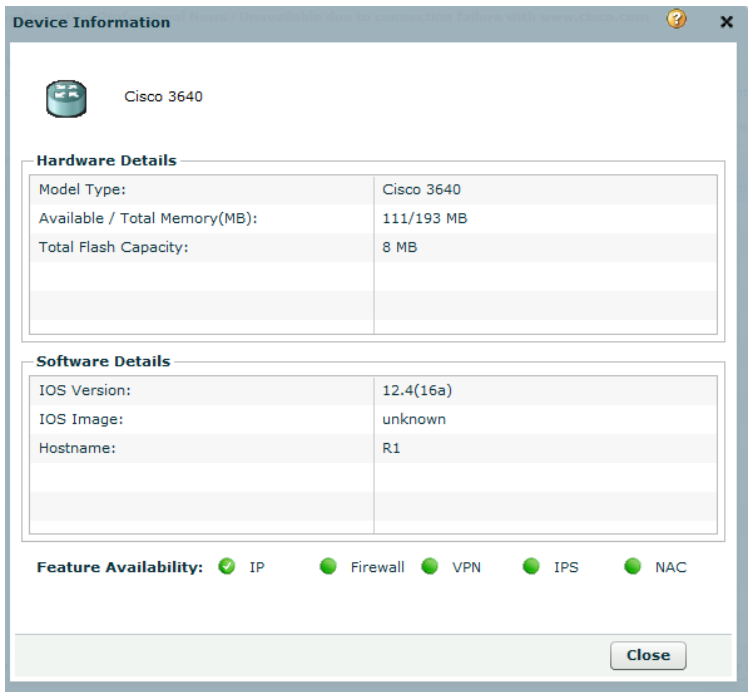
Part B: configuring a router using Cisco Configuration Professional (CCP)

1. On PC1 start up the CCP tool and connect to R1.

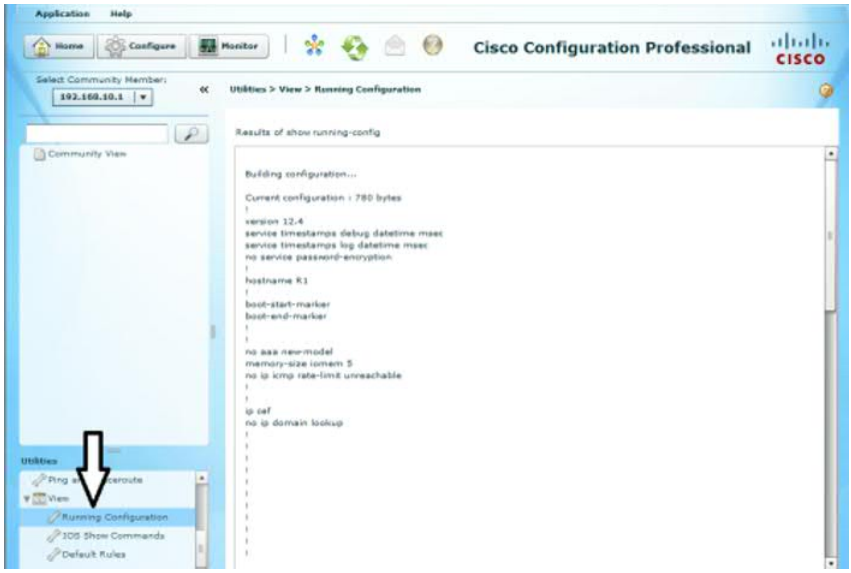
1.1. As an administrator, launch the CCP tool on PC1 and in the appropriate field, enter the IP address of R1 as well as the login **admin** with its password and then click on **OK**.



1.2. Click on the "**Discover**" button to connect to R1 and on the "**Router status**" button to display the characteristics of your router.

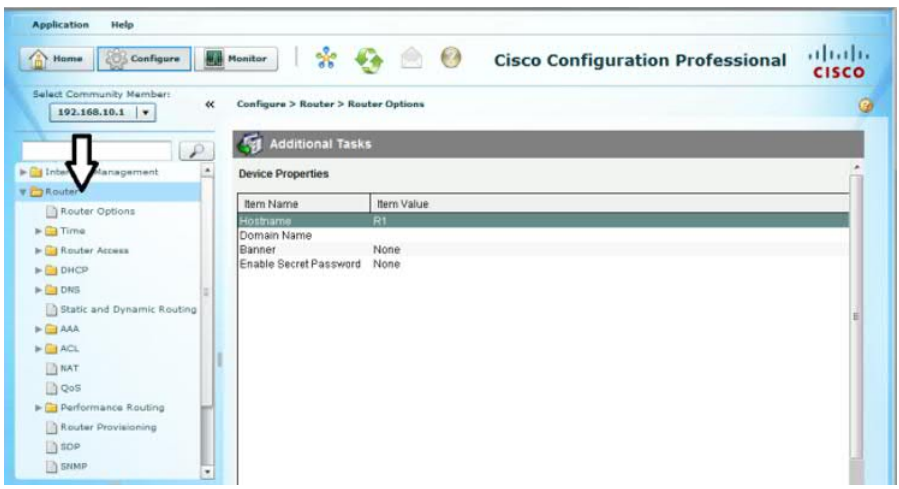


1.3. Using the menu "**Utilities > View > Running Configuration**" (see arrow), display the running configuration of R1.



2. Configure R1 using CCP.

NOTE.– All the configurations specified in the following questions can be implemented using an option from the menu "**Configure > Router >…**"



2.1. Rename the router to "Rt1".

2.2. Configure the following warning (***a banner***) "*Access strictly forbidden for unauthorized persons"*.

2.3. Set "Cisco12" as the encrypted password for the privileged mode.

2.4. Set the system date and time.

2.5. Create a user "User1" with password "123456" and privilege level 3.

2.6. Create a DHCP scope with the following parameters:

- scope name: scope1;
- network address: 192.168.10.0/24;
- range: 192.168.10.50-192.168.10.100;
- lease: 8 days;
- DNS address: 192.168.50.10.

2.7. Create a default route to the E0/1interface.

2.8. Configure the OSPF protocol with the following parameters:

- process number: 10;
- network1 192.168.10.0/24 area 0;
- network2 192.168.20.0/24 area 0.

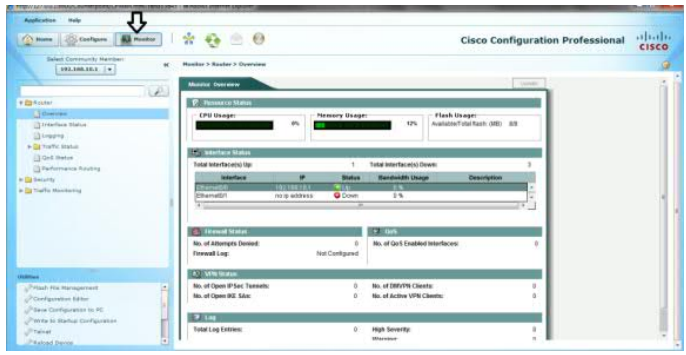
2.9. Create an ACL with the following parameters:

- name of the ACL: ACL1
- objective 1: to allow the 172.16.0.0/16 network to access the http server whose IP address is 192.168.10.13;
- objective 2: to allow the network 192.168.0.0/24 to access the FTP server whose IP address is 192.168.10.14;
- objective 3 Allow station 192.168.10.56/24 to access the telnet server whose IP address is 192.168.10.10.

Apply this LCD to the E0/1 interface.

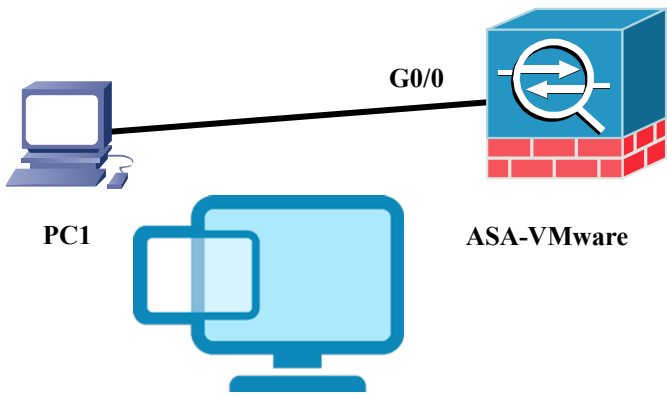
3. Supervise R1 using CCP.

Using the menu "**Monitor > Router > Overview**" (see arrow) display the state of R1.



EXERCISE 17.–

Topology



Addressing table

Device	Operating system	IP address / mask
ASA0	ASAv version: asa921-smp-k8	192.168.10.20/24
PC1	Windows 7 or later	192.168.10.10/24

Objective

Configure an ASA firewall using the Adaptive Security Device Manager (ASDM).

Software to be used

VMware.

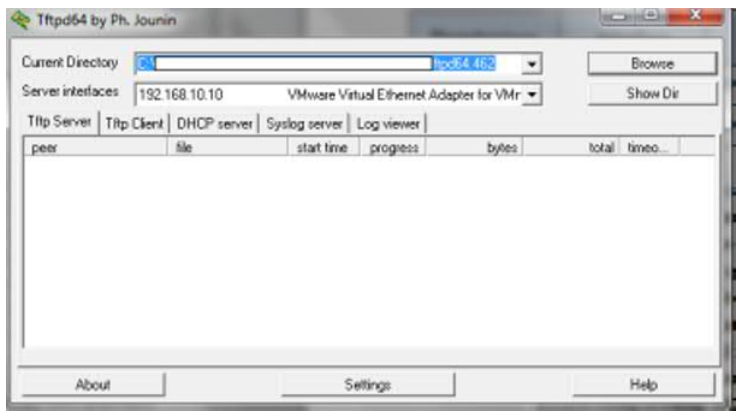
Part A: configuring the basic settings on PC1 and ASA0 to support an ASDM connection

1. Configure the following parameters on ASA0.

ciscoasa(config)#**hostname ASA0**
ASA0(config)#**username admin password 1234**
ASA0 (config)# **ssl encryption aes128-sha1 aes256-sha1**
ASA0(config)#**interface g0/0**
ASA0(config-if)#**ip address 192.168.10.20 255.255.255.0**
ASA0(config-if)# **no shutdown**
ASA0(config-if)#**nameif inside**
ASA0(config-if)# **http server enable**
ASA0(config-if)#**http 192.168.10.0 255.255.255.0 inside**

2. Set the PC1 IP address to 192.168.10.10/24 and ensure that a "ping request" is carried out between PC1 and ASA0.

3. Use the tftpd32 tool to download the library "asdm-x.x.x.bin" from ASA0.

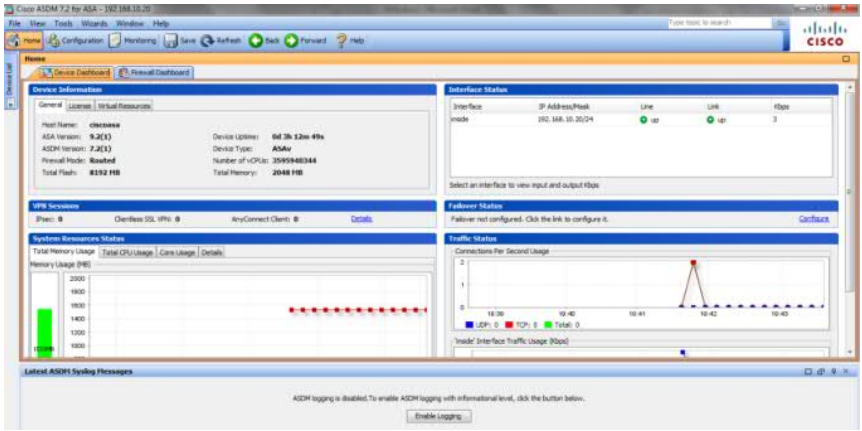


ASA0#**copy tftp: flash:**
Address or name of remote host []? **192.168.10.10**
Source filename []?**asdm-752-153**
Destination filename [asdm-752-153]?
Accessing tftp://192.168.10.10/

4. Launch your browser on PC1 and access ASA0 using the following link: "https://192.168.10.20".

5. After validating the exception, click on the "Install ASDM Launcher" button to download the "Cisco ASDM-IDM Launcher" tool using the login "admin" and its password.

6. Install and launch the "Cisco ASDM-IDM Launcher" tool.



NOTE.– In version 7.2, the Cisco ASDM-IDM Launcher tool is a ".jar" file, which must be launched from its installation location.

Part B: configuring the ASA 5505 firewall with ASDM

1. Use the menu "wizards/startup wizard" to configure the following basic settings on the ASA device:

– host name: ASA1;

– domain name: Cisco.com;

– the privilege mode password: 1234;

– interface g0/1:

- IP address: 212.212.1.10/24;

- zone name: outside;

- security level: 0;

- state: active;

– a default static route from the "outside" zone to the IP address 212.212.1.11/24;

– the DHCP SERVICE for the company's internal network:

- the range of IP addresses: 192.168.10.50 – 192.168.10.100;

- the DNS server: 192.168.10.2;

-enable PAT on g0/1.

Save Configuration.

2. Set the system date.

3. Create a user "User3" with password "1234" and privilege level 5.

4. Set a minimum password length of 8 characters.

5. Use the menu "Configuration > Firewall > Service Policy Rules" to create a Class-Map and a Policy-Map to inspect the "icmp" traffic between the "inside" and "outside" zones.

6. Use the menu "Configuration > Firewall > Access Rules" to create an ACL that authorizes all http and FTP traffic from the "inside zone" to the Internet.

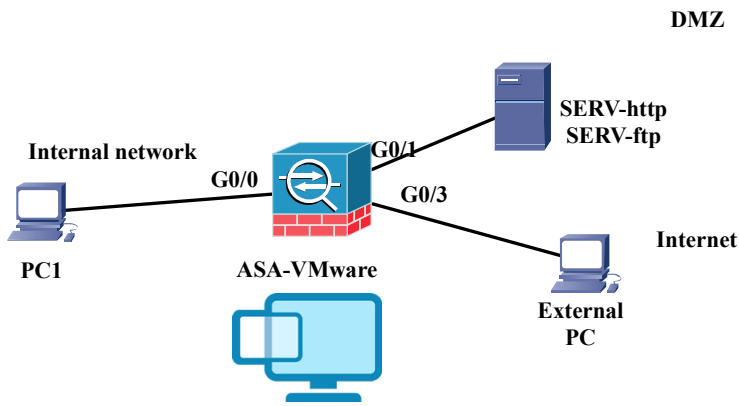
7. Configure the static NAT service to allow access to the following internal servers from the Internet:

– Server-http: internal IP address: **192.168.10.2/24**; external IP address: **212.212.1.20/30**;

– Server-ftp: internal IP address: **192.168.10.3/24**; external IP address: **212.212.1.21/30**.

Part C: testing the firewall (optional)

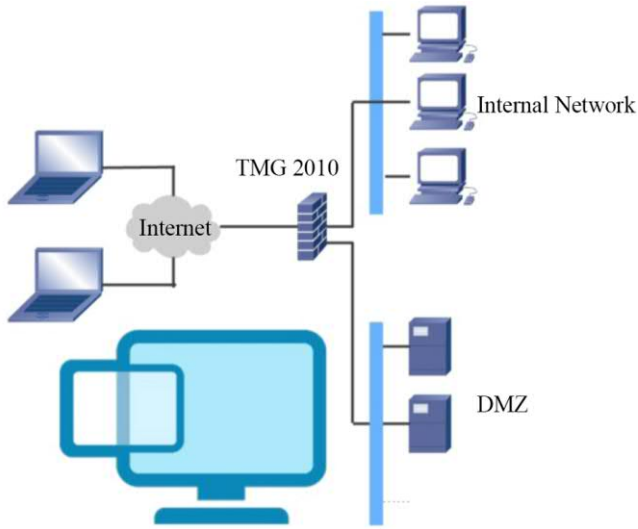
Topology



Implement the topology and test the working of the ASA 5505 firewall.

EXERCISE 18.–

Topology



Software used

– VMware Workstation.

Addressing table

Device	Interface	IP address / mask
TMG server 2010	Internal network	192.168.0.1/24
	DMZ	192.168.10.1/24
	External network	212.212.212.4/32

Objectives

– Install and configure the basic elements of a Forefront TMG 2010 server.

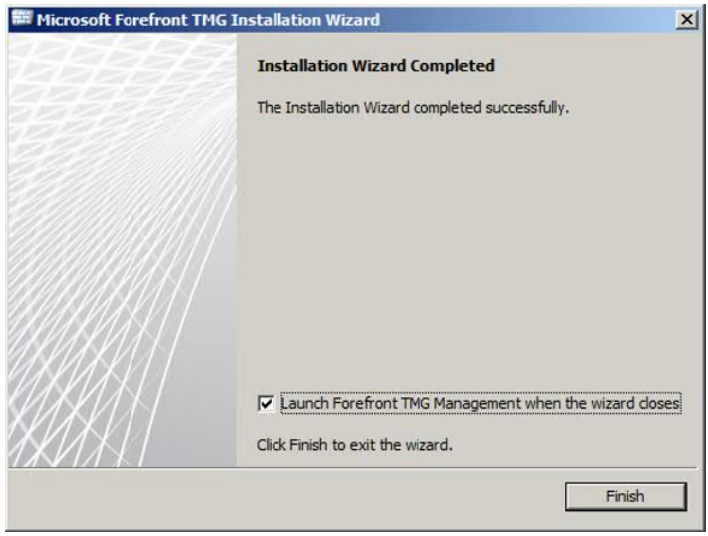
Software to be used

– VMware.

NOTE.– Following the objectives stated above for this document, this exercise will be restricted to the installation and configuration of certain basic elements of the TMG2010. The reader may consult other specialized documents on this product for more information.

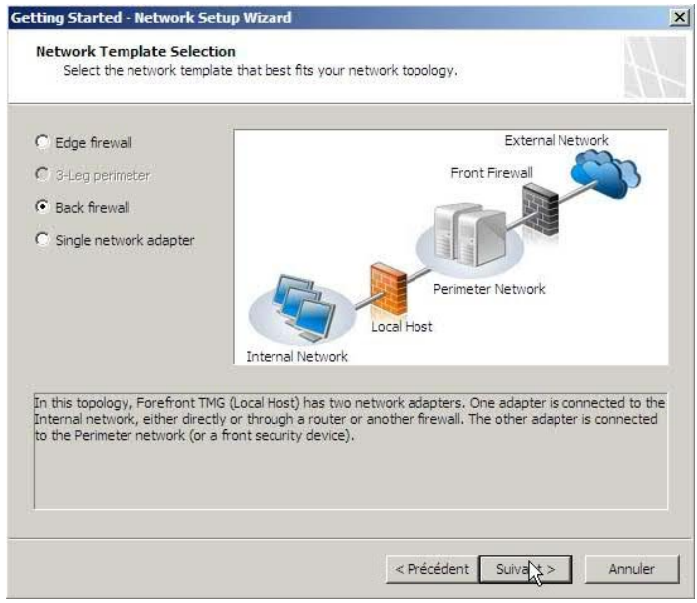
Part A: installing Forefront TMG 2010

The Forefront TMG 2010 server can only be installed on Windows Server 2008 or Windows Server 2008 R2. Begin by installing updates before installing the server. Both these tasks can usually be carried out easily.

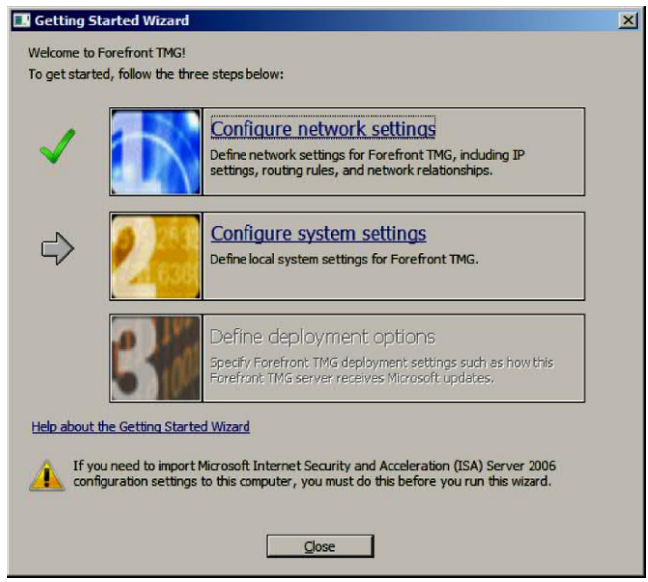


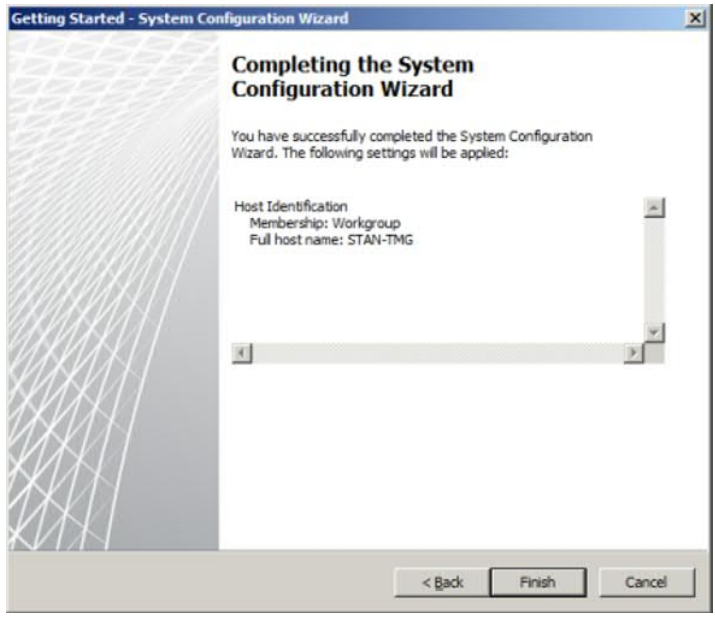
Part B: Initial configuration of Forefront TMG 2010

1. Configure the Forefront TMG 2010 server interfaces based on the addressing table.

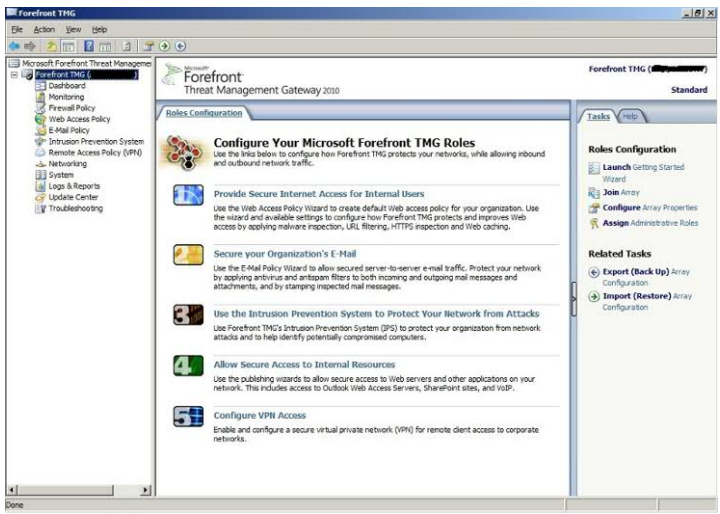


2. Configure the system parameters by filling in the hostname, domain or workgroup and the DNS suffix. Retain the default values of all these parameters since we will not be using them in this exercise.



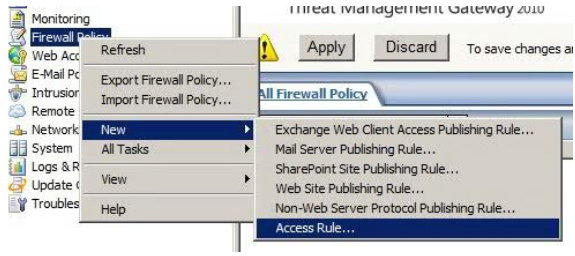


3. Exit the wizard and launch the TMG2010 management console.



Part C: configuring some basic elements of Forefront TMG 2010

1. Create an access rule, called "Rule1", which will authorize all https and FTP flows between the internal network and the Internet.

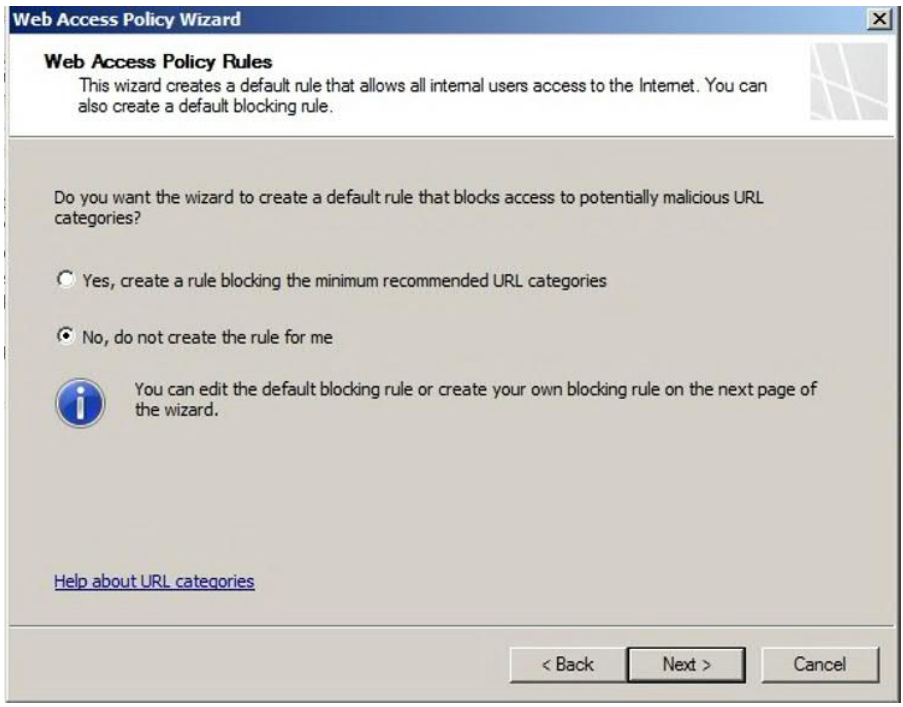


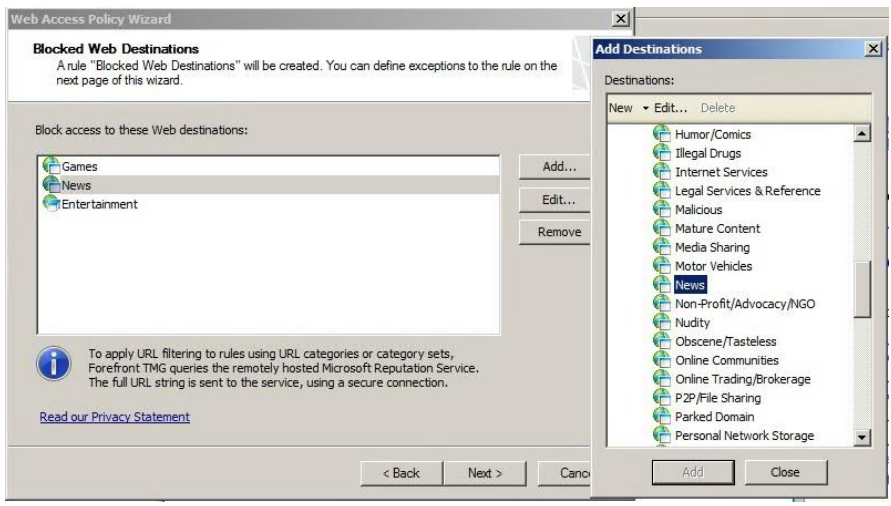
2. Create an access rule, named "Rule2" which will authorize all https and ssh flows between the internal network and the DMZ.

3. Create an access rule, named "Rule3" which allows IPsec ESP clients to access the DMZ.

4. Start the configuration of the web access policy.

4.1. Create a web access policy that blocks access to entertainment, games and news sites.

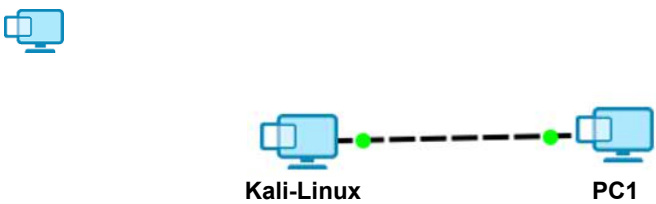

Web Access Policy Wizard
Web Access Policy Rules
This wizard creates a default rule that allows all internal users access to the Internet. You can also create a default blocking rule.
Do you want the wizard to create a default rule that blocks access to potentially malicious URL categories?
Yes, create a rule blocking the minimum recommended URL categories
No, do not create the rule for me
You can edit the default blocking rule or create your own blocking rule on the next page of the wizard.
Help about URL categories
< Back
Next >
Cancel


Web Access Policy Wizard
Blocked Web Destinations
A rule "Blocked Web Destinations" will be created. You can define exceptions to the rule on the next page of this wizard.
Block access to these Web destinations:
Games
News
Entertainment
Add...
Edit...
Remove
To apply URL filtering to rules using URL categories or category sets, Forefront TMG queries the remotely hosted Microsoft Reputation Service. The full URL string is sent to the service, using a secure connection.
Read our Privacy Statement
< Back
Next >
Add Destinations
Destinations:
New
Edit...
Delete
Humor/Comics
Illegal Drugs
Internet Services
Legal Services & Reference
Malicious
Mature Content
Media Sharing
Motor Vehicles
News
Non-Profit/Advocacy/NGO
Nudity
Obscene/Tasteless
Online Communities
Online Trading/Brokerage
P2P/File Sharing
Parked Domain
Personal Network Storage
Add
Close

4.2. Create an access rule, named "Rule-Web1" which authorizes authenticated users to only access professional sites.

EXERCISE 19.–

Topology



Software used

– **VMware Workstation.**

– **GNS3.**

Addressing table

Device	Operating system	IP address / mask
Kali-Linux	Kali Linux version 2018.2	192.168.21.163/24
PC1	Windows XP SP3	192.168.21.164/24

Objectives

– Understanding the working of different types of attacks;

– knowing the countermeasures to implement to secure a computer network;

– using the Kali-linux system to test network vulnerabilities in order to protect the network.

Software to be used

– VMware.

Overview of the Kali-Linux system

Kali-Linux is a Debian-based Linux distribution that allows you to perform security audits. This system contains several tools that facilitate a variety of information security tasks, such as intrusion tests and search for vulnerabilities, among others. Kali-Linux is nowadays classified as an essential tool for anyone wishing to learn about or specialize in the field of computer security.

Configure the basic settings on the PC

1. Configure the IP addresses at the interfaces of the two PCs based on the address table.

2. Test the connectivity between the two PCs.

Part A: exploiting a vulnerability in an operating system

Overview of the attack

This attack involves exploiting a vulnerability, known as “MS08-67”, in the Windows samba service. This affects all Windows XP operating systems: Windows XP SP1, SP2 and SP3. Having been classified as an obsolete system, Windows XP no longer receives updates or patches from Microsoft.

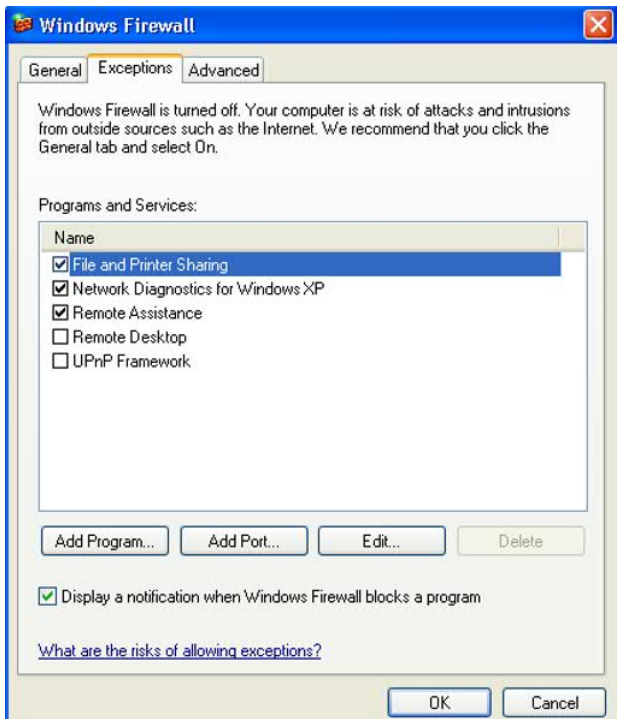
Tools used to test the attack

– **Metasploit** is a project integrated into Kali-Linux, which aims to provide information on vulnerabilities in a computer system and to help in performing penetration tests.

– **Armitage** is a graphical interface that facilitates the use of Metasploit.

1. Activate the vulnerability in the operating system.

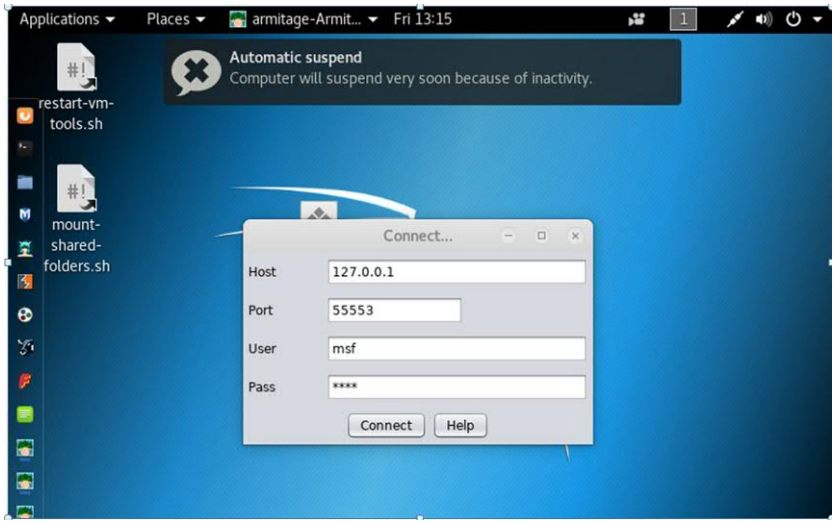
On PC1, launch Control Panel and in the Firewall settings, select "File and Printer Sharing".



NOTE. – The attack is also possible if the firewall is completely disabled on the victim's station.

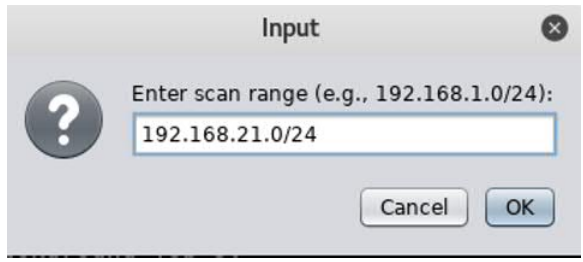
2. Exploiting the vulnerability.

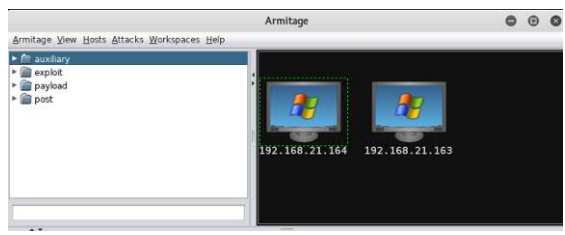
2.1. Launch the "armitage" tool on Kali-Linux by clicking on the icon: 



2.2. Launch a reconnaissance attack.

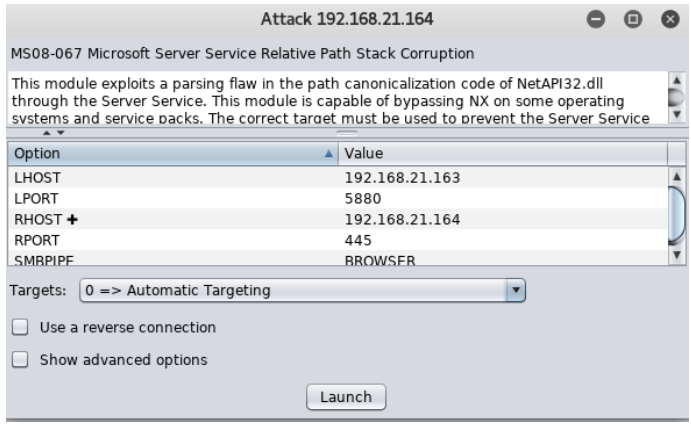
In the menu "Hosts/Nmap Scan/Ping Scan" launch a "**ping scan**" on the network 192.168.21.0/24.





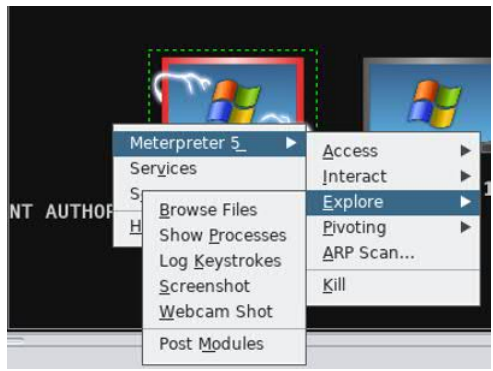
2.3. Launch the attack.

From the list of attacks, choose the following path: "exploit/windows/smb/ms08_067_netapi" and double-click.



Click on the "Launch" button and ensure that the attack is carried out successfully.

2.4. Exploit the victim's machine.



Countermeasure

Always update operating systems and migrate to recent systems.

Part B: exploiting the vulnerability of an application

Overview of the attack

This attack involves exploiting a vulnerability, known as "ms10_046_shortcut_icon_dllloader", in the "Windows Shell" software. It runs on multiple Windows operating systems (see Microsoft Security Bulletin MS10-046-Critical).

Tools used to test the attack

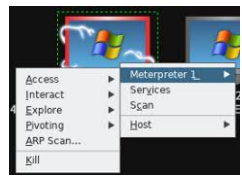
– **Metasploit.**

– **Armitage.**

1. Exploiting the vulnerability.

1.1. Release station PC1.

In the "armitage" tool, click on the PC1 address and then choose the submenu "Kill" to release it from the previous attack.



1.2. Launch the attack.

From the list of attacks, choose the following path: "exploit/windows/browser/ ms10_046_shortcut_icon_dllloader" and double-click.

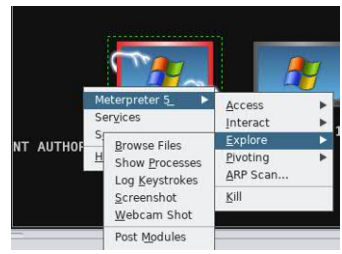
Click on the “Launch” button.

1.3. Activate the vulnerability.

Launch Internet Explorer and type in the link http://192.168.21.163. Ensure that the attack is carried out successfully.

NOTE.– In practice, the attacker uses a public IP address linked to a domain name. The link is sent through email to the victim.

1.4. Exploit the victim’s machine.



Countermeasure

Apply all patches for the applications and operating systems.

Part C: exploiting the execution of a “Trojan Horse”

Overview of the attack

A Trojan horse (or Trojan) is malicious code that contains two functionalities: the first carries out a useful task and the second can lead to data espionage or even deletion of data.

Tools used to test the attack

– **Metasploit.**

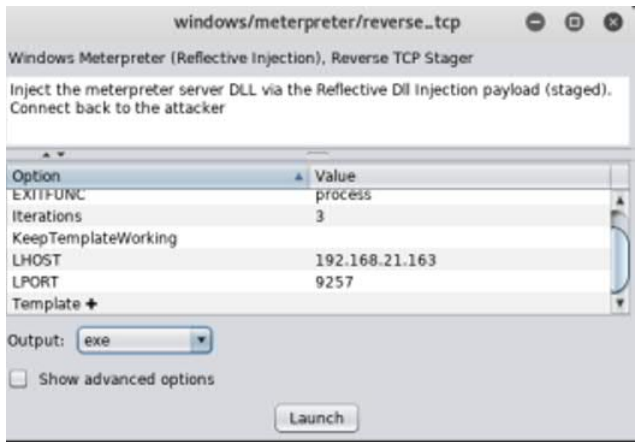
– **Armitage.**

1. Preparing for the attack.

1.1. Release station PC1.

1.2. Create the Trojan.

From the list of attacks, choose the following path: "windows/meterpreter/reverse_tcp" and double-click. Then, from the drop-down option "Output", choose the ".exe" option and click on the "Launch" button.



Note down the value of the LPORT parameter (9,257). This value could be any value of your choice between 1024 and 65,536.

Save the resulting file as "Trojan" on your desktop.

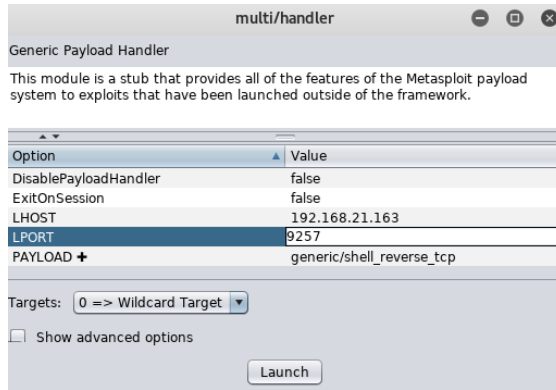
1.3. Activate the vulnerability.

Copy the file "Trojan.exe" onto PC1 and run it.

NOTE.– In practice, the file already created will either be integrated into another program that appears legitimate (a game, a screensaver etc.) or will be linked to an office file (pdf, Word etc.) or even an image and will then be triggered when executed by the user.

2. Launch the attack.

From the directory of attacks, choose the following path: "exploit/multi/handler" and double-click.



Set the LPORT parameter to the value that is already configured on the reception ports and click on the “Launch” button.

3. Exploit the victim’s machine.

Countermeasure

– Install and update the anti-virus software.

– Do not run programs from unreliable sources.

Part D: exploiting the vulnerability of an unsecured connection

Overview of the attack

The “Man-in-the-middle” attack consists of placing oneself between two network elements to try to take advantage of unencrypted data exchanged. Among other things, the attacker can steal the login and password details from an unsecured connection between the client and the server.

Tool used to test the attack

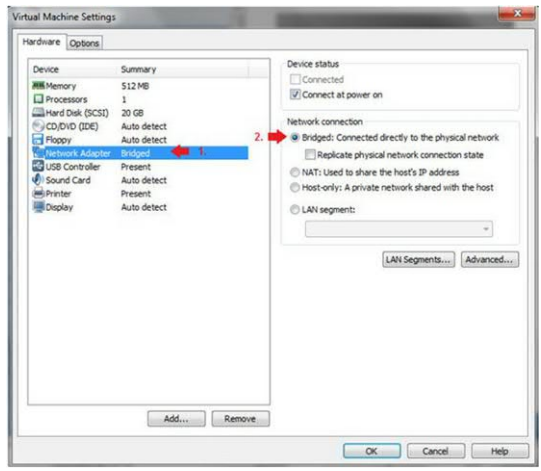
Setoolkit is suite of custom tools that focuses solely on attacks on network elements for personal use (PC, tablet, phone, etc.). These allow the creation of “Man-in-the-middle” attacks, among others.

NOTE.– For this part, you will need to modify your network settings to connect to the Internet.

1. Configuring the basic settings on the PCs.

1.1. Release station PC1.

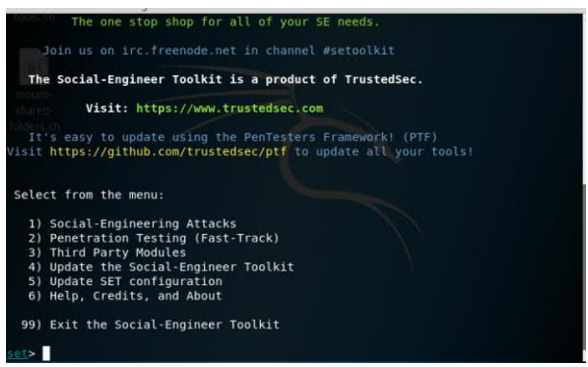
1.2. Modify the VMware network settings on both PCs.



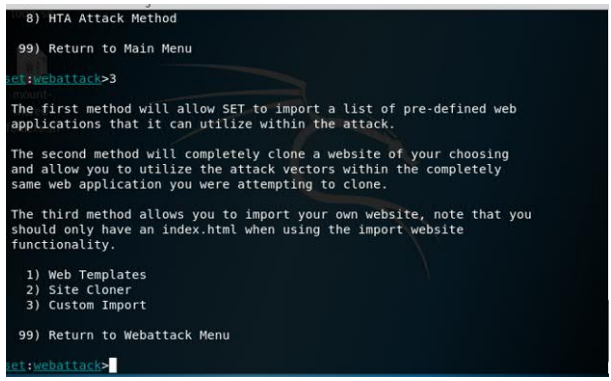
Make sure both stations have an Internet connection.

2. Launch the attack.

2.1. Start a terminal and enter the "setoolkit" command.



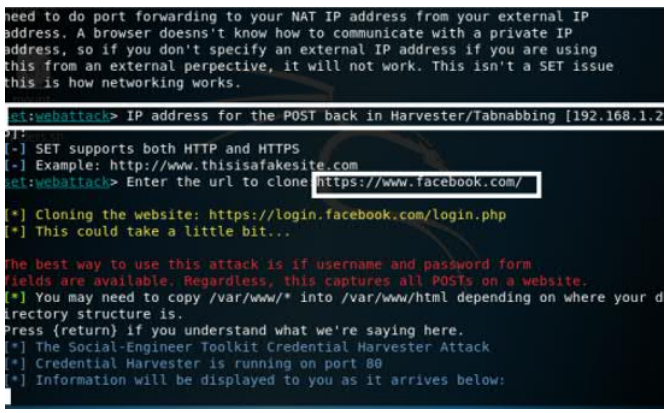
2.2. Type in the following choices consecutively: 1; 2; 3.



2.3. Type in the following choice: 2 and type in the following parameters:

– retain the default IP address;

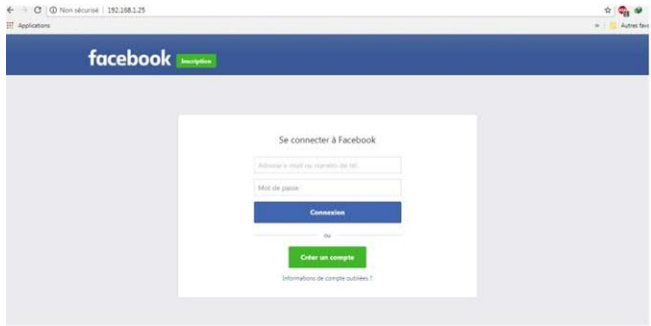
– type in the link: https://www.facebook.com/.



3. Activate the vulnerability.

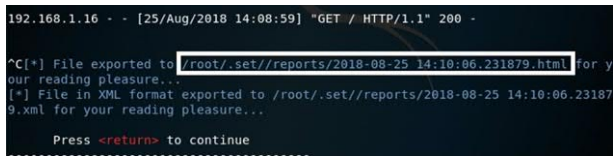
– Launch the browser on the client station and type in the following link: http://192.168.1.25 (the IP address of the Kali-Linux station). Ensure that your browser indicates that your connection is not secure.

NOTE.– In practice, the attacker uses a public IP address linked to a domain name that is very close to the name of the targeted site, for instance: facebok.com, facebooke.com.

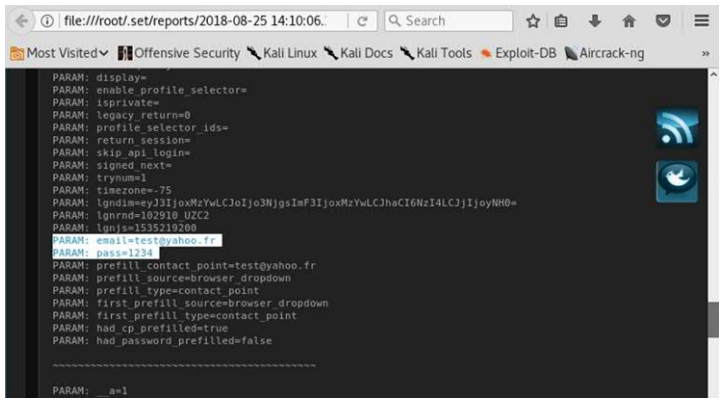


– Type in the login: test@yahoo.fr and the password: 1234 in the indicated fields, then validate. Note that you will be redirected to the site www.facebook.com.

– On the Kali-Linux station, type in Ctrl+C to stop the attack.



– Open the report generated by the tool and check that the login and password have been captured and saved (open the ".html" file saved with the path /root/.set/report/).



Countermeasure

Ensure that connection to a sensitive site is secured by the https protocol.

Part E: exploiting the vulnerability of simple passwords

Overview of the attack

The purpose of a password attack is to discover usernames and passwords to access various resources. There are two commonly used methods for this type of an attack: a dictionary attack and brute force attacks.

Tools used to test the attack

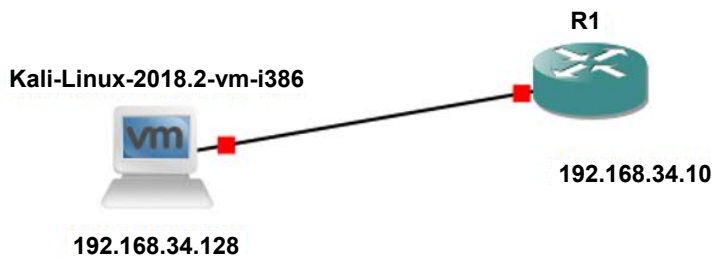
– **Crunch**: this is a tool that can generate all possible combinations of a given set of characters. It is used in the brute force password attacks.

– **Hydra**: this is a tool that can carry out password attacks and supports many network protocols. It is very fast and flexible, and new modules can be easily added.

NOTE.– For this section, you will need to use GNS3 to complete the exercise.

1. Configure the basic settings on the PCs and on R1.

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

1.1. Configure the IP addresses at the interfaces of both PCs based on the topology.

1.2. Test the connectivity between the two elements.

1.3. Type in the following commands on R1:

R1(config)#**username admin password 1234**

R1(config)#**line vty 0**
R1(config-line)#**login local**

2. Prepare for the attack.

2.1. Generate a list of passwords.

Start a terminal on Kali-Linux and type in the following command:

root@kali:~#**crunch 4 4 1234 -o /root/*PassList.txt***

NOTE.– For simplicity's sake, we will restrict ourselves to creating passwords with 4 characters, composed of combinations of the digits: 1, 2, 3 and 4.

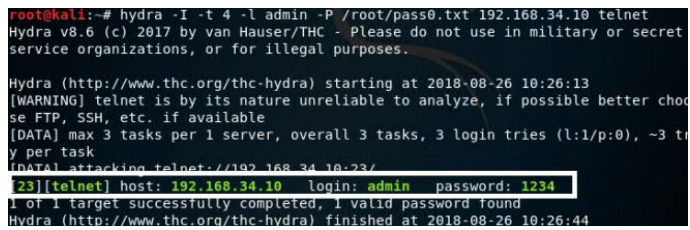
2.2. Generate a list of users.

root@kali:~#**echo admin >> /root/*listeUser.txt***
root@kali:~#**echo cisco >> /root/*listeUser.txt***
root@kali:~#**echo admintrateur >> /root/*UserList.txt***

3. Launch the attack.

Launch the attack by using only the "admin" account combined with all the possible passwords generated earlier.

root@kali:~#**hydra -I -t 4 -l admin -P /root/*PassList*.txt 192.168.34.10 telnet**



NOTES.–

– To use the "UserList" file, simply type in the command:

root@kali:~#**hydra -I -t 4 -L /root/*UserList.txt* -P /root/pass0.txt 192.168.34.10 telnet**

– The “Xhydra” tool is the graphical interface of the hydra utility. It simplifies the execution of attacks of this type. However, it offers fewer options than command line.

Countermeasure

– Ensure that passwords are hard to guess, that they contain a high level of complexity, and that they have a minimum length of 8 characters.

– Install IPS to detect this type of attack.

References

Anandh, V., Vinod, M., Singh, G.D. (2018). *CCNA Security 210-260 Certification Guide*. Packt Publishing, Birmingham.

Cisco (2018). *Cisco Networking Academy* [Online]. Available at: https://www.netacad.com/fr.

Frahim, J., Santos, O., Ossipov, A. (2012). *Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services*, 3rd edition. Cisco Press, Indianapolis.

Keith, B., Scott, M. (2012). *CCNA Security 640-554 Official Cert Guide*. Cisco Press, Indianapolis.

Santos, O., Stuppi, J. (2015). *CCNA Security 210-260 Official Cert Guide*. Cisco Press, Indianapolis.

Vachon, B. (2012). *CCNA Security Portable Command Guide*. Cisco Press, Indianapolis.

Index

Computer Network Security, First Edition. Ali Sadiqui.

I

K, L, M

N, O

P, R

S

T, V

W, X, Z

Other titles from

in

Computer Engineering

2019

BESBES Walid, DHOUIB Diala, WASSAN Niaz, MARREKCHI Emna
Solving Transport Problems: Towards Green Logistics

CLERC Maurice
Iterative Optimizers: Difficulty Measures and Benchmarks

GHLALA Riadh
Analytic SQL in SQL Server 2014/2016

TOUNSI Wiem
Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT

2018

ANDRO Mathieu
Digital Libraries and Crowdsourcing
(Digital Tools and Uses Set – Volume 5)

ARNALDI Bruno, GUITTON Pascal, MOREAU Guillaume
Virtual Reality and Augmented Reality: Myths and Realities

BERTHIER Thierry, TEBOUL Bruno
From Digital Traces to Algorithmic Projections

CARDON Alain
Beyond Artificial Intelligence: From Human Consciousness to Artificial Consciousness

HOMAYOUNI S. Mahdi, FONTES Dalila B.M.M.
Metaheuristics for Maritime Operations
(Optimization Heuristics Set – Volume 1)

JEANSOULIN Robert
JavaScript and Open Data

PIVERT Olivier
NoSQL Data Models: Trends and Challenges
(Databases and Big Data Set – Volume 1)

SEDKAOUI Soraya
Data Analytics and Big Data

SALEH Imad, AMMI Mehdi, SZONIECKY Samuel
Challenges of the Internet of Things: Technology, Use, Ethics
(Digital Tools and Uses Set – Volume 7)

SZONIECKY Samuel
Ecosystems Knowledge: Modeling and Analysis Method for Information and Communication
(Digital Tools and Uses Set – Volume 6)

2017

BENMAMMAR Badr
Concurrent, Real-Time and Distributed Programming in Java

HÉLIODORE Frédéric, NAKIB Amir, ISMAIL Boussaad, OUCHRAA Salma, SCHMITT Laurent
Metaheuristics for Intelligent Electrical Networks
(Metaheuristics Set – Volume 10)

MA Haiping, SIMON Dan
Evolutionary Computation with Biogeography-based Optimization
(Metaheuristics Set – Volume 8)

PÉTROWSKI Alain, BEN-HAMIDA Sana
Evolutionary Algorithms
(Metaheuristics Set – Volume 9)

PAI G A Vijayalakshmi
Metaheuristics for Portfolio Optimization
(Metaheuristics Set – Volume 11)

2016

BLUM Christian, FESTA Paola
Metaheuristics for String Problems in Bio-informatics
(Metaheuristics Set – Volume 6)

DEROUSSI Laurent
Metaheuristics for Logistics
(Metaheuristics Set – Volume 4)

DHAENENS Clarisse and JOURDAN Laetitia
Metaheuristics for Big Data
(Metaheuristics Set – Volume 5)

LABADIE Nacima, PRINS Christian, PRODHON Caroline
Metaheuristics for Vehicle Routing Problems
(Metaheuristics Set – Volume 3)

LEROY Laure
Eyestrain Reduction in Stereoscopy

LUTTON Evelyne, PERROT Nathalie, TONDA Albert
Evolutionary Algorithms for Food Science and Technology
(Metaheuristics Set – Volume 7)

MAGOULÈS Frédéric, ZHAO Hai-Xiang
Data Mining and Machine Learning in Building Energy Analysis

RIGO Michel
Advanced Graph Theory and Combinatorics

2015

BARBIER Franck, RECOUSSINE Jean-Luc
COBOL Software Modernization: From Principles to Implementation with the BLU AGE® Method

CHEN Ken
Performance Evaluation by Simulation and Analysis with Applications to Computer Networks

CLERC Maurice
Guided Randomness in Optimization
(Metaheuristics Set – Volume 1)

DURAND Nicolas, GIANAZZA David, GOTTELAND Jean-Baptiste,
ALLIOT Jean-Marc
Metaheuristics for Air Traffic Management
(Metaheuristics Set – Volume 2)

MAGOULÈS Frédéric, ROUX François-Xavier, HOUZEAUX Guillaume
Parallel Scientific Computing

MUNEESAWANG Paisarn, YAMMEN Suchart
Visual Inspection Technology in the Hard Disk Drive Industry

2014

BOULANGER Jean-Louis
Formal Methods Applied to Industrial Complex Systems

BOULANGER Jean-Louis
Formal Methods Applied to Complex Systems:
Implementation of the B Method

GARDI Frédéric, BENOIST Thierry, DARLAY Julien, ESTELLON Bertrand,
MEGEL Romain
Mathematical Programming Solver based on Local Search

KRICHEN Saoussen, CHAOUACHI Jouhaina
Graph-related Optimization and Decision Support Systems

LARRIEU Nicolas, VARET Antoine
Rapid Prototyping of Software for Avionics Systems: Model-oriented Approaches for Complex Systems Certification

OUSSALAH Mourad Chabane
Software Architecture 1
Software Architecture 2

PASCHOS Vangelis Th
Combinatorial Optimization – 3-volume series, 2nd Edition
Concepts of Combinatorial Optimization – Volume 1, 2nd Edition
Problems and New Approaches – Volume 2, 2nd Edition
Applications of Combinatorial Optimization – Volume 3, 2nd Edition

QUESNEL Flavien
Scheduling of Large-scale Virtualized Infrastructures: Toward Cooperative Management

RIGO Michel
Formal Languages, Automata and Numeration Systems 1: Introduction to Combinatorics on Words
Formal Languages, Automata and Numeration Systems 2: Applications to Recognizability and Decidability

SAINT-DIZIER Patrick
Musical Rhetoric: Foundations and Annotation Schemes

TOUATI Sid, DE DINECHIN Benoit
Advanced Backend Optimization

2013

ANDRÉ Etienne, SOULAT Romain
The Inverse Method: Parametric Verification of Real-time Embedded Systems

BOULANGER Jean-Louis
Safety Management for Software-based Equipment

DELAHAYE Daniel, PUECHMOREL Stéphane
Modeling and Optimization of Air Traffic

FRANCOPOULO Gil
LMF — Lexical Markup Framework

GHÉDIRA Khaled
Constraint Satisfaction Problems

ROCHANGE Christine, UHRIG Sascha, SAINRAT Pascal
Time-Predictable Architectures

WAHBI Mohamed
Algorithms and Ordering Heuristics for Distributed Constraint Satisfaction Problems

ZELM Martin *et al.*
Enterprise Interoperability

2012

ARBOLEDA Hugo, ROYER Jean-Claude
Model-Driven and Software Product Line Engineering

BLANCHET Gérard, DUPOUY Bertrand
Computer Architecture

BOULANGER Jean-Louis
Industrial Use of Formal Methods: Formal Verification

BOULANGER Jean-Louis
Formal Method: Industrial Use from Model to the Code

CALVARY Gaëlle, DELOT Thierry, SÈDES Florence, TIGLI Jean-Yves
Computer Science and Ambient Intelligence

MAHOUT Vincent
Assembly Language Programming: ARM Cortex-M3 2.0: Organization, Innovation and Territory

MARLET Renaud
Program Specialization

SOTO Maria, SEVAUX Marc, ROSSI André, LAURENT Johann
Memory Allocation Problems in Embedded Systems: Optimization Methods

2011

BICHOT Charles-Edmond, SIARRY Patrick
Graph Partitioning

BOULANGER Jean-Louis
Static Analysis of Software: The Abstract Interpretation

CAFERRA Ricardo
Logic for Computer Science and Artificial Intelligence

HOMES Bernard
Fundamentals of Software Testing

KORDON Fabrice, HADDAD Serge, PAUTET Laurent, PETRUCCI Laure
Distributed Systems: Design and Algorithms

KORDON Fabrice, HADDAD Serge, PAUTET Laurent, PETRUCCI Laure
Models and Analysis in Distributed Systems

LORCA Xavier
Tree-based Graph Partitioning Constraint

TRUCHET Charlotte, ASSAYAG Gerard
Constraint Programming in Music

VICAT-BLANC PRIMET Pascale *et al.*
Computing Networks: From Cluster to Cloud Computing

2010

AUDIBERT Pierre
Mathematics for Informatics and Computer Science

BABAU Jean-Philippe *et al.*
Model Driven Engineering for Distributed Real-Time Embedded Systems

BOULANGER Jean-Louis
Safety of Computer Architectures

MONMARCHÉ Nicolas *et al.*
Artificial Ants

PANETTO Hervé, BOUDJLIDA Nacer
Interoperability for Enterprise Software and Applications 2010

SIGAUD Olivier *et al*.
Markov Decision Processes in Artificial Intelligence

SOLNON Christine
Ant Colony Optimization and Constraint Programming

AUBRUN Christophe, SIMON Daniel, SONG Ye-Qiong *et al.*
Co-design Approaches for Dependable Networked Control Systems

2009

FOURNIER Jean-Claude
Graph Theory and Applications

GUÉDON Jeanpierre
The Mojette Transform / Theory and Applications

JARD Claude, ROUX Olivier
Communicating Embedded Systems / Software and Design

LECOUTRE Christophe
Constraint Networks / Targeting Simplicity for Techniques and Algorithms

2008

BANÂTRE Michel, MARRÓN Pedro José, OLLERO Hannibal, WOLITZ Adam
Cooperating Embedded Systems and Wireless Sensor Networks

MERZ Stephan, NAVET Nicolas
Modeling and Verification of Real-time Systems

PASCHOS Vangelis Th
Combinatorial Optimization and Theoretical Computer Science: Interfaces and Perspectives

WALDNER Jean-Baptiste
Nanocomputers and Swarm Intelligence

2007

BENHAMOU Frédéric, JUSSIEN Narendra, O'SULLIVAN Barry
Trends in Constraint Programming

JUSSIEN Narendra
A TO Z OF SUDOKU

2006

BABAU Jean-Philippe *et al.*
From MDD Concepts to Experiments and Illustrations – DRES 2006

HABRIAS Henri, FRAPPIER Marc
Software Specification Methods

MURAT Cecile, PASCHOS Vangelis Th
Probabilistic Combinatorial Optimization on Graphs

PANETTO Hervé, BOUDJLIDA Nacer
Interoperability for Enterprise Software and Applications 2006 / IFAC-IFIP I-ESA'2006

2005

GÉRARD Sébastien *et al.*
Model Driven Engineering for Distributed Real Time Embedded Systems

PANETTO Hervé
Interoperability of Enterprise Software and Applications 2005

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.

Developed in collaboration with a training and certification team from Cisco, *Computer Network Security* is an exploration of the state-of-the-art and good practices in setting up a secure computer system. Concrete examples are offered in each chapter, to help the reader to master the concept and apply the security configuration.

This book is intended for students preparing for the CCNA Security Exam (210-260 IINS) – whether at professional training centers, technical faculties, or training centers associated with the "Cisco Academy" program. It is also relevant to anyone interested in computer security, be they professionals in this field or users who want to identify the threats and vulnerabilities of a network to ensure better security.

Ali Sadiqui is a trainer-researcher at the Office de la Formation Professionnelle et de la Promotion du Travail (OFPPT), Morocco. He is a member of several research laboratories and obtained his doctorate from the Sidi Mohamed Ben Abdellah University, Morocco.

ISTE
www.iste.co.uk
WILEY