



642-541

**Cisco SAFE Implementations
(CSI)**

**Study Guide
DEMO Version**

Copyright (c) 2003 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

TABLE OF CONTENTS

List of Tables

List of Acronyms

Introduction

1. Networking Fundamentals

- 1.1 SAFE Blueprint defined
- 1.2 Assets
- 1.3 Matters concerning Location
- 1.4 Threats
 - 1.4.1 Motivation of network intruders
 - 1.4.2 Different attacks
- 1.5 Security Policies
 - 1.5.1 The Objectives of a Security Policy
 - 1.5.2 The Checklist for a Security Policy
 - 1.5.3 Network Security as a Procedure

2. Management Procedures and Functions

- 2.1 Network Time Protocol (NTP)
 - 2.1.1 Using NTP
 - 2.1.2 Configuring NTP
 - 2.1.2.1 Configuring NTP on a Router
 - 2.1.2.2 Configuring NTP on a Switch
 - 2.1.3 Securing NTP
 - 2.1.3.1 Using Access Lists to Secure NTP
 - 2.1.3.2 Authentication
 - 2.1.4 NTP Versions
- 2.2 Simple Network Management Protocol
 - 2.2.1 Configuring SNMP
 - 2.2.1.1 Configuring SNMP on a Router
 - 2.2.1.2 Configuring SNMP on a Switch
 - 2.2.2 SNMP Versions
- 2.3 Cisco Discovery Protocol
 - 2.3.1 Configuring CDP
 - 2.3.2 CDP Versions

2.4. Authentication, Authorization, Accounting (AAA)

2.4.1 Authentication

2.4.1.1 Authentication Methods

2.4.1.2 Configuring Line Password Authentication

2.4.1.3 Configuring Username Authentication

2.4.1.4 Remote Security Servers

2.4.1.5 PAP and CHAP Authentication

2.4.1.5.1 Challenge Handshake Authentication Protocol (CHAP)

2.4.1.5.2 Microsoft Challenge Handshake Authentication Protocol

2.4.1.5.3 Password Authentication Protocol (PAP)

2.4.1.5.4 Configuring AAA Authentication

2.4.1.5.5 Configuring Login Authentication

2.4.1.5.6 Facilitating Password Protection at the Privileged Level

2.4.1.5.7 Setting up PPP Authentication

2.4.2 Configuring AAA Authorization

2.4.3 Configuring AAA Accounting

2.4.4 Troubleshooting AAA

2.5 Trivial File Transport Protocol

3. SAFE Security Blueprint

3.1 Outlook

3.2 Approach

3.3 Enterprise SAFE Assumptions

3.4 Objectives of the Enterprise SAFE Design

3.5 General truths accepted by Enterprise SAFE Blueprint

3.5.1 Routers as Targets

3.5.2 Switches as Targets

3.5.3 Hosts as Targets

3.5.4 Networks as Targets

3.5.5 Applications as Targets

3.6 Intrusion-Detection Systems

3.7 Secure Management and Reporting

3.8 Modular Approach

3.8.1 Edge module relationships

3.8.1.1 Edge Modules

3.8.1.2 E-Commerce Modules

3.8.1.2.1 Design Alternatives

3.8.1.3 Corporate Internet Module

- 3.8.1.3.1 Design Alternatives
- 3.8.1.4 VPN/Remote Access Module
- 3.8.1.5 WAN Module
 - 3.8.1.5.1 Design Alternatives
- 3.8.2 Campus Module Relationships
 - 3.8.2.1 Campus Modules
 - 3.8.2.2 Server Module
 - 3.8.2.2.1 Design Alternatives
 - 3.8.2.3 Management Module
 - 3.8.2.3.1 Design Alternatives

4. Extended SAFE Blueprints

- 4.1 The SAFE VPN Blueprint
 - 4.1.1 Design Fundamentals
 - 4.1.1.1 Split Tunneling
 - 4.1.2 Axioms
 - 4.1.2.1 Authentication
 - 4.1.2.2 IPSec
 - 4.1.2.3 IP Addressing
 - 4.1.2.4 Operating Limitations
 - 4.1.2.5 Single-Purpose and Multipurpose Devices
 - 4.1.2.6 Split Tunneling
 - 4.1.2.7 Network Architecture
 - 4.1.2.8 Interoperability and Mixed vs. Homogeneous Deployments
 - 4.1.2.9 Fragmentations and Path Maximum Transmission Unit Discovery
 - 4.1.2.10 Network Operations
 - 4.1.2.11 Remote Access User Requirements
 - 4.1.2.12 High Availability
 - 4.1.3 SAFE VPN Network Designs
- 4.2 The SAFE IP Telephony Blueprint
 - 4.2.1 IP Telephony Design Fundamentals
- 4.3 The SAFE Wireless Blueprint
 - 4.3.1 Wireless Design Fundamentals
 - 4.3.2 Axioms
- 4.4 The SAFE SMR Blueprint
 - 4.4.1 SMR Design Fundamentals
 - 4.4.2 Axioms
 - 4.4.3 Headend vs. Branch
 - 4.4.4 SAFE SMR Medium Network Model
 - 4.4.5 SAFE SMR Small Network Model
 - 4.4.6 SAFE SMR Remote-User Model

5. Products in the Campus

5.1 Routers

- 5.1.1 Securing Access
- 5.1.2 Passwords and AAA
- 5.1.3 Securing Services and Management

5.2 Switches

- 5.2.1 Securing Access
- 5.2.2 Securing Services and Management
- 5.2.3 Securing Ports

5.3 IDS

- 5.3.1 NIDS Configuration
- 5.3.2 HIDS Configuration

5.4. CiscoSecure Access Control Server

6. Products in the Edge

6.1 Routers Redux

- 6.1.1 Unicast RPF
- 6.1.2 Nonperimeter Routers in the Edge
- 6.1.3 NAT on the Router
- 6.1.4 IPSec on the Router

6.2 The PIX Firewall

- 6.2.1 Traffic Segregation
 - 6.2.1.1 NAT on a PIX
 - 6.2.1.2 IPSec on a PIX
- 6.2.2 The VPN Concentrator

6.3 The VPN Client

- 6.3.1 Hardware Client
- 6.3.2 The VPN Software Client

7. The Small Network Implementation

7.1 The Small Network Edge

- 7.1.1 Assets
- 7.1.2 Threats
- 7.1.3 Devices and Implementation
- 7.1.4 Design Alternatives

7.2 The Small Network Campus

- 7.2.1 Assets
- 7.2.2 Threats
- 7.2.3 Devices and Implementation

7.2.4 Design Alternatives

7.3 Branch Versus Standalone

8. The Medium Network Implementation

8.1 The Medium Network Edge

8.1.1 Assets

8.1.2 Threats

8.1.3 Devices and Implementation

8.1.4 Design Alternatives

8.2 The Medium Network WAN

8.3 The Medium Network Campus

8.3.1 Assets

8.3.2 Threats

8.3.3 Devices and Implementation

8.3.4 Design Alternatives

8.4 Branch Versus Headend

9. The Remote-User Design

9.1 The Remote-User Problem

9.1.1 Assets

9.1.2 Threats

9.1.3 Devices and Implementation

9.2 Options

9.2.1 Software Access Option

9.2.2 The Remote Site Firewall Option

9.2.3 The Hardware VPN Client Option

9.2.4 The Remote Site Broadband Router Option

10. User Authentication and Centralized Management

10.1 User Authentication

10.2 Centralized Management

LIST OF TABLES

TABLE 7.1:	Small Network Edge Threats and Their Mitigation
TABLE 7.2:	Small Network Campus Threats and Their Mitigation
TABLE 8.1:	Medium Network Edge Threats and Their Mitigation
TABLE 8.2:	Medium Network Campus Threats and Their Mitigation
TABLE 9.1:	Remote-User Network Threats and Their Mitigation

LIST OF ACRONYMS

AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
ACF	Advanced Communications Function
ACK	Acknowledgment bit (in a TCP segment)
ACL	Access Control List
ACS	Access Control Server
AD	Advertised Distance
ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Standards Institute
API	Application Programming Interface
APPC	Advanced Program-to-Program Communications
ARAP	AppleTalk Remote Access Protocol
ARE	All Routes Explorer
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
AS	Autonomous System
ASA	Adaptive Security Algorithm
ASBR	Autonomous System Boundary Router
ASCII	American Standard Code for Information Interchange
ASIC	Application Specific Integrated Circuits
ATM	Asynchronous Transfer Mode
AUI	Attachment Unit Interface

Bc	Committed burst (Frame Relay)
B channel	Bearer channel (ISDN)
BDR	Backup Designated Router
Be	Excess burst (Frame Relay)
BECN	Backward Explicit Congestion Notification (Frame Relay)
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol version 4
BIA	Burned-in Address (another name for a MAC address)
BOD	Bandwidth on Demand.
BPDU	Bridge Protocol Data Unit
BRF	Bridge Relay Function
BRI	Basic Rate Interface (ISDN)
BSD	Berkeley Standard Distribution (UNIX)
CBT	Core Based Trees
CBWFQ	Class-Based Weighted Fair Queuing
CCITT	Consultative Committee for International Telegraph and Telephone
CCO	Cisco Connection Online
CDDI	Copper Distribution Data Interface
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Interdomain Routing
CIR	Committed Information Rate. (Frame Relay)
CGMP	Cisco Group Management Protocol
CLI	Command-Line Interface
CLSC	Cisco LAN Switching Configuration
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CR	Carriage Return.
CRC	Cyclic Redundancy Check (error)
CRF	Concentrator Relay Function
CST	Common Spanning Tree
CSU	Channel Service Unit
DB	Data Bus (connector)
DCE	Data Circuit-Terminating Equipment
dCEF	Distributed Cisco Express Forwarding
DDR	Dial-on-Demand Routing
DE	Discard Eligible Indicator
DECnet	Digital Equipment Corporation Protocols
DES	Data Encryption Standard
DHCP	Dynamic Host Control Protocol

CCSP 642-541

DLCI	Data-Link Connection Identifier
DNIC	Data Network Identification Code. (X.121 addressing)
DNS	Domain Name System
DoD	Department of Defense (US)
DR	Designated Router
DRiP	Duplicate Ring Protocol
DS	Digital Signal
DS0	Digital Signal level 0
DS1	Digital Signal level 1
DS3	Digital Signal level 3
DSL	Digital Subscriber Line
DSU	Data Service Unit
DTE	Data Terminal Equipment
DTP	Dynamic Trunking Protocol
DUAL	Diffusing Update Algorithm
DVMRP	Distance Vector Multicast Routing Protocol
EBC	Ethernet Bundling Controller
EGP	Exterior Gateway Protocol
EIA/TIA	Electronic Industries Association/Telecommunications Industry Association
EIGRP	Enhanced Interior Gateway Routing Protocol
ESI	End-System Identifier
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FC	Feasible Condition (Routing)
FD	Feasible Distance (Routing)
FDDI	Fiber Distributed Data Interface
FEC	Fast EtherChannel
FECN	Forward Explicit Congestion Notification
FIB	Forwarding Information Base
FIFO	First-In, First-Out (Queuing)
FR	Frame Relay
FS	Feasible Successor (Routing)
FSSRP	Fast Simple Server Redundancy Protocol
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converters
GEC	Gigabit EtherChannel
GSR	Gigabit Switch Router
HDLC	High-Level Data Link Control
HDSL	High data-rate digital subscriber line
HSRP	Hot Standby Router Protocol

HSSI	High-Speed Serial Interface
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDN	International Data Number
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface
IOS	Internetwork Operating System
IP	Internet Protocol
IPSec	IP Security
IPv6	IP version 6
IPX	Internetwork Packet Exchange (Novell)
IRDP	ICMP Router Discovery Protocol
IS	Information Systems
IS-IS	Intermediate System-to-Intermediate System
ISDN	Integrated Services Digital Network
ISL	Inter-Switch Link
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Provider
ITU-T	International Telecommunication Union–Telecommunication Standardization Sector
kbps	kilobits per second (bandwidth)
LAN	Local Area Network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LAPD	Link Access Procedure on the D channel
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LED	Light Emitting Diode
LES	LAN Emulation Server
LLC	Logic Link Control (OSI Layer 2 sublayer)
LLQ	Low-Latency Queuing
LMI	Local Management Interface
LSA	Link-State Advertisement
MAC	Media Access Control (OSI Layer 2 sublayer)
MAN	Metropolitan-Area Network

MD5	Message Digest Algorithm 5
MLS	Multilayer Switching
MLS-RP	Multilayer Switching Route Processor
MLS-SE	Multilayer Switching Switch Engine
MLSP	Multilayer Switching Protocol
MOSPF	Multicast Open Shortest Path First
MSAU	Multistation Access Unit
MSFC	Multilayer Switch Feature Card
MTU	Maximum Transmission Unit
NAK	Negative Acknowledgment
NAS	Network Access Server
NAT	Network Address Translation
NBMA	Nonbroadcast Multiaccess
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card
NMS	Network Management System
NNI	Network-to-Network Interface
NSAP	Network Service Access Point
NVRAM	Nonvolatile Random Access Memory
OC	Optical Carrier
ODBC	Open Database Connectivity
OLE	Object Linking and Embedding
OSI	Open Systems Interconnection (Model)
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
OUI	Organizationally Unique Identifier
PAgP	Port Aggregation Protocol
PAP	Password Authentication Protocol
PAT	Port Address Translation
PDN	Public Data Network
PDU	Protocol Data Unit (i.e., a data packet)
PIM	Protocol Independent Multicast
PIM	SM Protocol Independent Multicast Sparse Mode
PIMDM	Protocol Independent Multicast Mode
PIX	Private Internet Exchange (Cisco Firewall)
PNNI	Private Network-to-Network Interface
POP	Point of Presence
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol

PQ	Priority Queuing
PRI	Primary Rate Interface (ISDN)
PSTN	Public Switched Telephone Network
PTT	Poste, Telephone, Telegramme
PVC	Permanent Virtual Circuit (ATM)
PVST	Per-VLAN Spanning Tree
PVST+	Per-VLAN Spanning Tree Plus
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Service
RIF	Routing Information Field
RIP	Routing Information Protocol
RJ	Registered Jack (connector)
RMON	Embedded Remote Monitoring
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RSFC	Route Switch Feature Card
RSM	Route Switch Module
RSP	Route Switch Processor
RSTP	Rapid Spanning Tree Protocol
RTP	Reliable Transport Protocol
RTO	Retransmission Timeout
SA	Source Address
SAID	Security Association Identifier
SAP	Service Access Point; also Service Advertising Protocol (Novell)
SAPI	Service Access Point Identifier
SAR	Segmentation and Reassembly
SDLC	Synchronous Data Link Control (SNA)
SIA	Stuck in Active (EIGRP)
SIN	Ships-in-the-Night (Routing)
SLIP	Serial Line Internet Protocol
SMDS	Switched Multimegabit Data Service
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture (IBM)
SNAP	SubNetwork Access Protocol
SNMP	Simple Network Management Protocol
SOF	Start of Frame
SOHO	Small Office, Home Office
SONET	Synchronous Optical Network
SONET/SDH	Synchronous Optical Network/Synchronous Digital Hierarchy

SPAN	Switched Port Analyzer
SPF	Shortest Path First
SPID	Service Profile Identifier
SPP	Sequenced Packet Protocol (Vines)
SPX	Sequenced Packet Exchange (Novell)
SQL	Structured Query Language
SRAM	Static Random Access Memeory
SRB	Source-Route Bridge
SRT	Source-Route Transparent (Bridging)
SRTT	Smooth Round-Trip Timer (EIGRP)
SS7	Signaling System 7
SSAP	Source service access point (LLC)
SSE	Silicon Switching Engine.
SSP	Silicon Switch Processor
SSRP	Simple Server Redundancy Protocol
STA	Spanning-Tree Algorithm
STP	Spanning-Tree Protocol; also Shielded Twisted-Pair (cable)
SVC	Switched Virtual Circuit (ATM)
SYN	Synchronize (TCP segment)
TA	Terminal Adapter (ISDN)
TAC	Technical Assistance Center (Cisco)
TACACS	Terminal Access Controller Access Control System
TCI	Tag Control Information
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCN	Topology Change Notification
TDM	Time-Division Multiplexing
TDR	Time Domain Reflectometers
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TLV	Type-Length-Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TrBRF	Token Ring Bridge Relay Function
TrCRF	Token Ring Concentrator Relay Function
TTL	Time-To-Live
UDP	User Datagram Protocol
UNC	Universal Naming Convention or Uniform Naming Convention
UNI	User-Network Interface
URL	Uniform Resource Locator

CCSP 642-541

UTC	Coordinated Universal Time (same as Greenwich Mean Time)
UTL	Utilization
UTP	Unshielded Twisted-Pair (cable)
VBR	Variable Bit Rate
VC	Virtual Circuit (ATM)
VID	VLAN Identifier
VIP	Versatile Interface Processor
VLAN	Virtual Local Area Network
VLSM	Variable-Length Subnet Mask
VMPS	VLAN Membership Policy Server
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
vtty	Virtual terminal line
WAIS	Wide Area Information Server
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WLAN	Wireless Local Area Network
WWW	World Wide Web
XNS	Xerox Network Systems
XOR	Exclusive-OR
XOT	X.25 over TCP
ZIP	Zone Information Protocol (AppleTalk)

Exam Code: 642-541

Certifications:

Cisco Certified Security Professional (CCSP)

Core

Prerequisites:

Cisco Certified Network Associate (CCNA) Certification

About This Study Guide

This Study Guide is based on the current pool of exam questions for the Cisco CCSP 642-541 composite exam. As such it provides all the information required to pass the 642-541 exam and is organized around the specific skills that are tested in that exam. Thus, the information contained in this Study Guide is specific to the 642-541 exam and does not represent a complete reference work on the subject of Interconnecting Cisco Networking Devices. Topics covered in this Study Guide includes: Security Fundamentals; Introduction to Network Security; Network Attack Taxonomy; Network Security Policy; Management Protocols and Functions; Architectural Overview; Design Fundamentals; SAFE axioms; Security Wheel; the Cisco Security Portfolio; Secure connectivity, including Virtual Private Network Solutions, the 3000 Concentrator Series, and Cisco VPN Optimized Routers; Perimeter security firewalls, including Cisco PIX and Cisco IOS Firewall; Intrusion Protection, including IDS and Cisco Secure Scanner; Access Control Solutions; Security Management with VMS and CSPM; Cisco AVVID; SAFE Small Network Design, including the Small Network Corporate Internet Module, the Small Network Campus Module, Implementing ISP Routers, Implementing IOS Firewall Features and Configuration, Implementing PIX Firewalls; SAFE Medium Network Design, including the Medium Network Corporate Internet Module, the Medium Network Corporate Internet Module Design Guidelines, the Medium Network Campus Module, the Medium Network Campus Module Design Guidelines, the Medium Network WAN Module, Implementing ISP Routers, Implementing Edge Routers, Implementing PIX Firewalls, Implementing IOS Firewalls, Implementing NIDS and HIDS, Implementing VPN Concentrators, and Implementing Layer 3 Switches; and SAFE Remote-User Network Implementation, including Key Devices, Threat Mitigation, Software Access Options, Remote Site Firewall Options, Hardware VPN Client Options, and Remote Site Router Options.

Intended Audience

This Study Guide is targeted specifically at people who wish to take the Cisco CCSP 642-541 Composite exam. This information in this Study Guide is specific to the exam. It is not a complete reference work. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in this Study Guide are complex. Knowledge of CompTIA's A+ and Network+ courses would be advantageous.

How To Use This Study Guide

To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work. Where possible, attempt to implement the information in a lab setup.

CCSP 642-541

- Be sure that you have studied and understand the entire Study Guide before you take the exam.

Note: Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

Good luck!

1. Networking Fundamentals

1.1 SAFE Blueprint defined

Cisco's SAFE architecture is proposed to be a security implementation blueprint geared towards networks that contain threats outside as well as valuable components inside. SAFE is able to protect a network while still maintaining its ability to be used.

1.2 Assets

The entire IT system is an information asset. Each physical device within it is an information asset, and all the **data** that exist in or is transported over the system is an information asset. Information assets may be grouped as follows:

- **Hardware Assets** can be end-user devices, devices proposed to support a multitude of users (user-support devices), and networking devices.
- **User-Support Devices** are devices that are not operated directly but accessed periodically. Examples of user-support devices are file and print servers, as well as the printers controlled by the print servers.
- **Networking Devices**. These are devices such as routers and switches, Software Assets as well as CSPFA (PIX firewalls), CSIDS (intrusion detection), CSVPN (VPN concentrators and clients), and the Network Access Server (NAS).
- **End-User Devices** are the devices that users operate. Desktops and laptops are but two examples of such devices.
- **User-Support Devices** are devices that are not operated directly but accessed periodically. Examples of user-support devices are file and print servers, as well as the printers controlled by the print servers.
- **Software Assets**. Database software is regularly used to access information.

1.3 Matters Concerning Location

Two categories exist:

- **Internal-Only Assets**, which are the assets totally inside your network space. Access to these assets is solely under the users' control.
- **External-Facing Assets**, which are those that you control but that connect directly to devices that are outside of your control. These are devices such as edge or perimeter routers, NASs, and firewalls. Cisco refers to this part of the network as **the edge** in the SAFE architecture.

1.4 Threats

Threats can originate from within a network (**internal**) or from outside (**external**). There are two types of threats that exist:

- **Prearranged threats**-Performed by individuals seeking a particular target. Often the more dangerous because it is organized.
- **Unplanned threats**-Far more regular and mostly as a result of users searching the Internet for targets. It is possible to download a variety of scanning files from the Internet and put them to use in scanning a network for weaknesses.

1.4.1 Motivation of Network Intruders

A hacker or cracker or script kiddie, is someone who enters a network or system without permission.

- **Cracker** is an individual possessing a broad knowledge of networking and Internet. Most often thought to have spiteful intentions.
- **Hacker** often uses highly developed programming techniques to source for weaknesses in the network or operating system. Intentions are not always unethical and they are often used by businesses to test their security.
- **Script kiddie** is a novice hacker who uses publicly available scripts to test the integrity of networks and scan for weakness.
- **Insufficient knowledge of computers and networks.** It is possible for a user to initiate a violation due to a lack of understanding. On a system like Windows NT it is possible for a novice user to unintentionally change or remove important settings rendering the system unusable. As regards firewalls, an administrator might open connectivity to the extent where the firewall becomes obsolete. Temporary openings could become permanent due to a lack of measures to ensure temporary openings are closed after need for them is met.
- **Fun and pride**-The challenge is the primary motivation here. Often done purely for the sport of it.
- **Revenge**-Usually unhappy former employees armed with a secure knowledge of the network. They normally target specific data. Passwords as well as other security measures need to be changed as soon as vital staff leave to protect company assets.
- **Profit**-Access to credit card information, bank transfers and billing information can prove to be very profitable. Access to a company's data may give its competitor an unfair advantage.
- **Political reasons**-Cyber-warfare as it is known, poses a real threat to any economy. It is possible to launch an attack from any base. Add to this the low cost of equipment and connectivity buffed by the lack of adequate protection, and it is easy to see why. Electronic transactions are the norm for many an economy, and therefore place itself at huge risk. This is also known as hactivism, the act of defacing an organisation's web site for political objectives.

1.4.2 Different Types of Attacks

The three major types are:

- **Investigation Attacks** are performed to ascertain the structure of the network or computer in question and discover any weaknesses. An attack of this nature could indicate the potential for more intrusive attacks. Many of these attacks have been written into programmes enabling rookie attackers to launch attacks on networks. Here are a few examples of reconnaissance attacks.
 - **DNS whois queries** will grant the user access to information such as the address of a specific domain and its owner.
 - **Ping sweep** will provide details like the number of hosts on a network.
 - **Vertical scans**, scan service ports of a single host, requesting different services at every port. This gives the user the ability to figure out the type of operating system as well as the services operating on the system.
 - **Horizontal scans**, scan an address range for a specific port or service. The FTP sweep is a common example.
 - **Block scans** combine both vertical and horizontal scans. It scans a segment of the network and attempts connections at a number of ports of individual hosts on the specific segment.

- **Admission attacks.** The goal here would be to gain access to a computer or network. After access a user can perform various functions, which could fall into one of three categories.
 - **Interception**-If the user captures traffic between its source and destination, they can store it for future use. This data is anything that crosses the network segment that the user is connected to.
 - The user may also gain access to passwords if the network management data is crossing the network, thereby taking control of that equipment. It requires physical connectivity in order to intercept traffic. Going from hub to switching technology reduces the amount of traffic that can be intercepted. Most effective is having sensitive data encrypted and sent via an encrypted connection. This prohibits the intruder from reading the data.
 - **Alteration** occurs subsequent to having gained access; the illegal user is now able to alter the resource. Among others they will also be able to alter the content of the files, system arrangements, system access and privileged access. The user is able to achieve this because of a weakness in the operating system or using other software running on the system. Unauthorised privilege escalation refers to a legal user with low access status trying to gain privileged information to obtain higher access status. This provides the invader with more control of the system or network.
 - **Manufacture**-The user will be able to fabricate untrue items and place them in the network or system. This may include the insertion of viruses and worms or a Trojan horse that will continue to attack the network from within.
 - **Virus** can be annoying while others may be destructive in nature. They are made up of computer code that fixes itself to other software operating on the computer. In this manner the virus is able to proliferate each time the software is opened.
 - **Worm**-A worm takes advantage of weaknesses on the network to copy itself. A worm would scan the network searching for a computer with a specific weakness. Once it has located a host, it replicates itself to that system and scans from there as well.
 - **Trojan horse** is a program that professes to perform a certain function but does another like tainting data on the harddrive. They are used at times to misuse systems by fabricating user accounts on systems that will allow illegal users access to or enable them to increase their privilege level. Some capture information and transfers it to a location where it can be retrieved and scrutinised by the attacker. More commonly, it will be used to control the system and incorporate it in a DDoS attack.
- **DoS attacks** are designed to reject access to a computer or system. Normally targets precise services and tries to overpower them by inundating them with countless requests. Launching the attack from multiple systems has the ability to increase the size of the DoS attack. This is referred to as distributed denial of service (DDoS) attack.

1.5 Security Policies

Security policies are created in accordance with the security philosophy of the organisation. It is then used by the technical team to design and employ the corporate security structure. The organization security policy is an official business document containing a set of rules to which users of the network should adhere to when accessing the network. It would include a list of acceptable and unacceptable activities as well as responsibilities in respect of security. It does not however dictate how the business should be operated. The security policy is therefore a guide for administrators to use when planning security efforts and subsequent reactions. The business needs would determine the nature and size of the security policy. The security policy would quite often be split into numerous documents with each one addressing a specific topic. These policies, known as **usage policy statements**, explain the tolerable use and responsibilities with respect to the

use of the network the size of the organization would determine the magnitude of the security policy, but should include the following:

- **Permissible use of resources** addresses suitable use of items such as email and Internet access.
- **Configuration policy** spells out which applications are to be arranged on the network and should assign a particular build for each system. This is important in making sure that all the network systems follow a set arrangement, thus cutting down on troubleshooting time.
- The **Patch management** system explains the upgrade and testing of new patches before being implemented. After approval, it is added to the standard build. This guarantees that all new systems are in accordance with the approved patch.
- **Infrastructure policy** spells out how the system is to be managed and maintained, and by whom. It also addresses the following:
 - Service Quality
 - Checking and Controlling the systems
 - Processing and Consolidating of Logs
 - Managing change
 - The scheme for addressing network
- The **User Account Policy** spells out which users should be designated what permissions. It is important to ensure adherence to the PC configuration policy. This can be achieved by limiting user permissions.
- **Other policies:** The amount of policies varies according to each organization. Factors such as encryption, backup, the handling of data and password requirements, like time span and size, as well as remote access, could be included in other policies.

With the institution of a security policy, three steps are recommended by Cisco:

- **Preparation** should be completed on a rough draft of the previously listed policy documents, or created as general usage statements. Risks analysis should be performed to determine the risks to be guarded against and to achieve a level of tolerable risks. Risks are defined by a company and can be split into the following three levels:
 - High
 - Medium
 - Low

Preparation also involves arranging security personnel and outlining their respective duties.

- **Prevention** lays out how changes to security situations are measured and applied. It also spells out how security should be regulated and checked, inclusive of the handling of data.
- **Response** sets out the course of action to be taken in the event of a problem as well as duties of security team members. The following topics should be addressed:
 - Response to an attempted security breach
 - Isolation and handling of a contaminated system
 - Gathering of evidence and the handling of log data
 - Correspondence with law enforcers
 - Restoration of network systems
 - A revision of the security policy ensures that any new susceptibilities are balanced out.

Members of management, the legal, as well as technical departments, make up the security policy team. In order for the security policy to be effective, it would firstly have to be fully supported by management and be enforceable in accordance with the relevant laws and regulations. It should also be technically viable.

The overriding reason for having a written security policy is cost savings, which are made in numerous ways:

- **Not having the data tainted:** Illegal users will be unable to access the data, thereby minimizing the ability to distort data. Having to restore tainted data can be costly.
- **Denial of service (DoS) attacks:** DoS attacks can be devastating. Although it is virtually impossible to prevent, it is possible to alleviate the attack by prohibiting access at several points on the network. Measures against fending off DoS attacks cannot be put into operation at the last minute.
- **Not having data manipulated:** Data manipulation is largely done to taint the public image of the organization. By restricting access to authorized users only, the risk of data manipulation is significantly reduced.
- **Increased effectiveness:** With a clearly explained practice as well as regular operation, the corporation will be more efficient.
- **Unidentified problems** could possibly arise from the introduction of unproven systems, designs, or applications into the network. Through testing and endorsing all practices, measures, applications and designs before applying them in a production environment minimizes the chances of creating these types of problems.

1.5.1 The Objectives of a Security Policy

- The initial objective would be to **advise the technical team on their choice of equipment**. Because of the policy not being in the nature of a technical document, it neither dictates nor stipulates which equipment or designs are to be used.
- The second objective would be to **guide the team in arranging the equipment**. It might state that the team uses their efforts to block users from viewing unacceptable websites. It does not however stipulate specific sites.
- The third objective spells out the **responsibilities of users and administrators**. This assists management and technicians in evaluating the effectiveness of the security measures.
- The fourth objective would set out to explain the **repercussions of a policy violation**.
- The last objective would be to spell **out the reactions to network threats**. If there is no plan for fending off an attack, the result would be bewilderment. It is also significant to describe escalation steps for items that are not as easily recognized on the network. Each member should know the steps to be taken in the event of a problem.

1.5.2 The Checklist for a Security Policy

- A policy requires the full **support of management** or it will not be honoured. In the event of management not endorsing the policy, it will prove to be ineffective. The policy might obstruct someone from performing a function they deem important, but the policy's objective is to place the organization before the individual.
- The policy should be **consistently effective** and should also be consistent in scope. It should not frustrate users. The job description of users would ascertain their access permission. Indistinct and unpredictable policies are difficult to put into practice and are prone to different interpretations.

- The policy should be **technically practical** to facilitate ease of use, as well as the comprehension of it. The security administrator should suggest solutions that are consistent with the needs of the organization when addressing security requirements.
- The structure of the technical document should be **non technical** as it is easier to comprehend than a technical document. This would also facilitate distribution without having to reveal the technology employed. Server and workstation policy will be more technical in content by reason of its nature. The implementation plan should be restricted to security personnel and anyone involved.
- The policy should be **implemented throughout the organization** because of its interconnectivity with Virtual Private Networks (VPNs) and Frame Relay networks. For this reason it is imperative that all sites share the same security policies. A security loophole at one of the sites could place the entire network at risk.
- The security policy should **outline the roles and responsibilities of users**. This helps make the user aware of security perimeters. In order to achieve set goals, both network administrators and management should be aware of their duties as regards to security.
- The policy should be **flexible** enough to fit in with the changing technology, organizational growth and infrastructure upgrades. However it should be detailed enough so as to meet all the requirements of the corporation. Constant reviewing of the security policy will ensure that the document remains relevant.
- The policy should be **coherent and logical**. It should display clarity and be simple in order not to confuse users. The user should understand their roles with respect to the security policy. Orientation is advised before issuing network logon.
- The security policy should be **broadly publicized** in order to enforce it. Everyone in the organization should receive and acknowledge receipt of the document.
- The security policy should **clearly state the repercussions for contraventions** against it. Because the rights of workers vary according to their location, it is vital that security team members from both the legal and human resources departments are involved in the creation of the policy.
- The security policy should **comprise of a reaction plan for security contraventions**. Complex systems are less easy to monitor, and for this reason, it is important to identify when a network is under threat and the subsequent reaction to it. The plan would help security personnel to react to network security threats. There is a difference between internal threats and external threats. Difficulty exists when trying to pinpoint an offender if the threat originates from the internal network.

1.5.3 Network Security as a Procedure

There are four steps to be taken to ensure the evolution of the security policy:

- **Securing the network** involves the actual application of a method or configuration. AAA servers and firewall devices can be used to secure the network.
- **Monitoring the network** assists administrators in comprehending the security challenges they are faced with. Constant observation should take place after changes to the network. Any discovered issues should be resolved immediately.
- **Testing**: Without testing it would be difficult to determine the efficiency of the applications. It should preferably occur after alterations to the network.

CCSP 642-541

- **Upgrading and improving security:** It is instrumental to adjust to upgrades as it is necessitated. Whether these would involve new equipment or configuration changes, it would be as a result of prior testing and serve as an introduction to future security efforts.