



642-501

Securing Cisco IOS Networks

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 Acronyms

List of Tables

Introduction

1. Network Security

- 1.1 Security Policies
 - 1.1.1 The Objectives of a Security Policy
 - 1.1.2 The Checklist for a Security Policy
- 1.2 Network Security Procedure
- 1.3 The legal Issue Relating to Network Security
- 1.4. Network Attack Threats
 - 1.4.1 Security Vulnerabilities
 - 1.4.1.1 Self Inflicted Vulnerabilities
 - 1.4.2 Threats
 - 1.4.3 The Motivation of Network Intruders
- 1.5 Different Network Attacks
 - 1.5.1 Renaissance Attacks
 - 1.5.2 Access attacks
 - 1.5.3 Denial of Service (DoS) Attacks
- 1.6 Defense
 - 1.6.1 Elements of Defense
 - 1.6.2 Physical Security

2. Basic Router Management

- 2.1 Router Configuration Modes
- 2.2 Configuration Modes and Submodes
- 2.3 Accessing the Cisco Router CLI
- 2.4 Cisco IOS Firewall Features
- 2.5 Securing Router Administration
 - 2.5.1 Privilege Access Levels
 - 2.5.2 Securing Access to the Console
 - 2.5.3 Configuring the Enable Password
 - 2.5.3.1 The Enable Secret Command

- 2.5.3.2 The Service Password Encryption Command
- 2.5.4 Configuring Multiple Privilege Levels
- 2.5.5 Warning Banners
- 2.5.6 Interactive Access
- 2.5.7 Securing VTY Access
- 2.5.8 Secure Shell (SSH) Protocol
- 2.5.9 Port Security for Ethernet Switches

3. Authentication, Authorization, Accounting (AAA)

3.1 Authentication

- 3.1.1 Authentication Methods
 - 3.1.1.1 Configuring Line Password Authentication
 - 3.1.1.2 Configuring Username Authentication
 - 3.1.1.3 Remote Security Servers
- 3.1.2 PAP and CHAP Authentication
 - 3.1.2.1 Challenge Handshake Authentication Protocol (CHAP)
 - 3.1.2.2 Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
 - 3.1.2.3 Password Authentication Protocol (PAP)

3.2. Configuring AAA Authentication

- 3.2.1 Configuring Login Authentication
- 3.2.2 Facilitating Password Protection at the Privileged Level
- 3.2.3 Setting up PPP Authentication

3.3 Configuring AAA Authorization

3.4 Configuring AAA Accounting

3.5 Configuring TACACS+ and RADIUS

3.6 Troubleshooting AAA

4. Cisco Secure Access Control Server

4.1 Cisco Secure ACS for Windows

- 4.1.1 Authentication
- 4.1.2 Authorization
- 4.1.3 Accounting

4.2 Administration

4.3 Cisco Secure ACS for Windows Architecture

- 4.3.1 CSAdmin
- 4.3.2 CSAuth
- 4.3.3 CSDBSync
- 4.3.4 CSLog
- 4.3.5 CSMon



4.3.6 CSTacacs and CSRADIUS

4.3.7 Cisco ACS for UNIX

4.4 Basic Deployment Factors for Cisco Secure ACS

4.4.1 Minimum Hardware and Operating System Requirements

4.4.2 Browser Compatibility

4.4.3 Port Requirements

4.5 Installing Cisco Secure ACS

4.5.1 Recommended Cisco Secure ACS Deployment Sequence

4.6 Troubleshooting Cisco Secure ACS for Windows

4.6.1 Authentication Problems

4.6.2 Troubleshooting Authorization Problems

4.6.3 Administration Issues

5. Securing the Network with a Cisco Router

5.1 Simple Network Management Protocol (SNMP)

5.1.1 Controlling Interactive Access Through a Browser

5.2 Inactivating Directed Broadcasts

5.2.1 Routing Protocol Authentication

5.2.2 Small Server Services

5.2.3 Disabling Finger Services

5.2.4 Disabling Network Time Protocol (NTP)

5.2.5 Disabling Cisco Discovery Protocol (CDP)

5.3 Access Lists

5.3.1 Types of IP ACLs

5.3.1.1 Standard IP ACLs

5.3.1.2 Extended IP ACLs

5.3.1.3 Reflexive ACLs

5.3.1.4 Time-Based ACLs

5.3.2 Configuring ACLs

5.4 The Cisco IOS Firewall

5.4.1 The Cisco IOS Firewall Feature Set

5.4.1.1 Authentication Proxy

5.4.1.2 DoS Protection

5.4.1.3 Logging and Audit Trail

5.4.1.4 Intrusion Detection

5.4.2 Port-To-Application Mapping (PAM)

5.4.2.1 System-Defined Port Mapping

5.4.2.2 User-Defined Port Mapping

5.4.2.3 Host-Specific Port Mapping

5.5 Context Based Access Control

- 5.5.1 DoS Detection and Protection
- 5.5.2 Alerts and Audit Trails
- 5.5.3 CBAC Operation
- 5.5.4 CBAC Restrictions
- 5.5.5 Supported Protocols
- 5.5.6 Configuring CBAC
- 5.5.7 Specifying the Inspection Rule
 - 5.5.7.1 Configuring Generic TCP and UDP Inspection
 - 5.5.7.2 Configuring Java Inspection
- 5.5.8 Applying the Inspection Rule to an Interface
- 5.5.9 Verifying and Debugging CBAC

5.6 Authentication Proxy and the Cisco IOS Firewall

- 5.6.1 Authentication Proxy and the Cisco IOS Firewall
- 5.6.2 Configuring Authentication Proxy
 - 5.6.2.1 Configuring AAA
 - 5.6.2.2 Configuring the HTTP Server
 - 5.6.2.3 Setting up the Authentication Proxy
- 5.6.3 Verifying Configuration of Authentication Proxy
- 5.6.4 Using Authentication Proxy with TACACS+
- 5.6.5 Using Authentication Proxy with RADIUS
- 5.6.6 Limitations of Authentication Proxy

5.7 Intrusion Detection (IDS)

- 5.7.1 Compatibility with the CSIDS
- 5.7.2 Cisco IOS Firewall IDS Configuration
 - 5.7.2.1 Initializing the Cisco IOS firewall IDS
 - 5.7.2.2 Configuring Information and Attack Signatures
 - 5.7.2.3 Creating and Applying Audit Rules
 - 5.7.2.4 Adding the Cisco IOS Firewall IDS to the Centralized Management
- 5.7.3 Verifying the Cisco IOS Firewall IDS Configuration

6. Creating a VPN Using IPSec

6.1 The Five Steps of IPSec

6.2 Configuring a Cisco Router for IPSec Using Preshared Keys

- 6.2.1 Selecting the IKE and IPSec Parameters
 - 6.2.1.1 Defining the IKE (Phase 1) Policy
 - 6.2.1.2 Defining the IPSec Policies
 - 6.2.1.3 Verifying the Current Router Configuration
 - 6.2.1.4 Verifying Connectivity
- 6.2.2 Configuring IKE
- 6.2.3 Configuring IPSec
- 6.2.4 Testing and Verifying IPSec Configurations

6.3 Configuring IPSec Manually

- 6.4 Configuring IPSec Using RSA Encrypted Nonces
- 6.5 Scaling a VPN Using IPSec with a Certificate Authority
 - 6.5.1 Cisco Router CA Support
 - 6.5.2 Configuring the Cisco Router for IPSec VPNs Using CA Support
 - 6.5.3 Test and Verify the Configuration
- 6.6 Configuring Remote Access by Utilizing the Easy VPN
 - 6.6.1 The Functionality and Features of Easy VPN Server
 - 6.6.2 Easy VPN Server Configuration
 - 6.6.3 Easy VPN Modes of Operation
- 6.7 Scaling Management of the VPN and Router
 - 6.7.1 CiscoWorks 2000
 - 6.7.2 VPN/Security Management Solution (VMS)
 - 6.7.3 Management Center for VPN Routers (Router MC)
 - 6.7.4 Components of the Router MC
 - 6.7.5 Supported Tunneling Technologies
 - 6.7.6 Router MC Integration with CiscoWorks Common Services
 - 6.7.7 Installation and Login to Router MC
 - 6.7.8 Connecting to the Router MC
 - 6.7.9 Router MC Workflow

LIST OF TABLES

- TABLE 2.1: Configuration Modes on the Cisco Router
- TABLE 5.1: Protocols and their Related Number Identification for ACLs
- TABLE 5.2: Default setting in the PAM Table
- TABLE 5.3: CBAC Commands

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
DLCI	Data-Link Connection Identifier

645-501 Secur

DNIC	Data Network Identification Code. (X.121addressing)
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

645-501 Secur

URL	Uniform Resource Locator
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
vt	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)

Securing Cisco IOS Networks

Exam Code: 642-501

Certifications:

Cisco Certified Security Professional (CCSP)

Core

Prerequisites:

None

About This Study Guide

This Study Guide is based on the current pool of exam questions for the Cisco CCSP 642-501 - Securing Cisco IOS Networks exam. As such it provides all the information required to pass the 642-501 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 642-501 exam and does not represent a complete reference work on Securing Cisco IOS Networks. Topics covered in this Study Guide includes: Network Security, Security Policies, Network Procedures, Network Attack Threats, Elements of Defence in Depth, Router Configuration Modes, Accessing the Cisco Router CLI, Privilege Access Levels, Configuring the Enable Password, Securing Access to the Console, Authentication Methods, PAP and CHAP Authentication, Configuring AAA Authentication, Configuring AAA Authorization, Configuring AAA Accounting, Troubleshooting AAA, Configuring TACACS+, Configuring RADIUS, Cisco Secure Access Control Server, Securing the Network with a Cisco Router, Access Lists, The Cisco IOS Firewall Feature Set, DoS Detection and Protection, CBAC Operation, Configuring CBAC, Authentication Proxy and the Cisco IOS Firewall, Configuring Authentication Proxy, Using Authentication Proxy with TACACS+, Using Authentication Proxy with RADIUS, Intrusion Detection and the Cisco IOS Firewall, Creating and Applying Audit Rules, Configuring a Cisco Router for IPSec Using Preshared Keys, Configuring IKE, Configuring IPSec, Testing and Verifying IPSec Configurations, Configuring IPSec Manually, Configuring IPSec Using RSA Encrypted Nonces, Configuring the Cisco Router for IPSec VPNs Using CA Support, The Functionality and Features of Easy VPN Server, Easy VPN Server Configuration, Scaling Management of the VPN and Router.

Intended Audience

This Study Guide is targeted specifically at people who wish to take the Cisco CCSP 642-501 Securing Cisco IOS Networks 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.

Note: This Study Guide does not combine all five CCSP exams but addresses the 642-501 exam specifically. As such, we would not advise using this Study Guide for the other exams.

How To Use This Study Guide



645-501 Secur

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.
- 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. Network Security

It is the execution of security mechanisms, policies and processes to prohibit unlawful admission to network resources and, or the destruction and alteration of data. Security policies form the basis of securing the network resources. A trade off exist between a completely secure network and the needs of business.

1.1 Security Policies

Security policies are created in accordance with the security philosophy of the organization. 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 standard for naming
- 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.

1.1.1 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.

1.1.2 The Checklist for a Security Policy

A policy requires the full **support of management** or it will not be honored. 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.

Security should be a continuous process, not just a once off effort. Continued efforts are generally referred to as Security Posture Assessment (SPA)

1.2 Network Security Procedure

There are 4 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.
- **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.

1.3 The legal Issue Relating to Network Security

Should an employee illegally use the company resources to surf the internet and manage to get into a server belonging to another company, or take control of the server, they then can use it to enter the database of another company. Here they access sensitive information and proceed to post it on the Internet. Regardless of whether the employee is in the wrong, the companies involved are still liable for damages seeing as how they have a responsibility to ensure the privacy of stored data. A clear definition can be found in the Internet Engineering Task Force's Sight (IETF) security handbook, RFC 2196.

1.4. Network Attack Threats

Because many institutions rely on computers to help them manage and store their information, and because of the level of interconnectivity, the computer has become a vital tool in any business. Add to this the fact that many a business maintains a connection to the Internet and exposes their business to the general public it is not difficult to see how susceptible the network can become to threats. Being in possession of an ineffective security policy places the company at greater risk of a network security breach.

1.4.1 Security Vulnerabilities

Computers, however complex, are but machines incapable of differentiating between authorized and unauthorized access. It is only able to respond to previously loaded instructions. Any part of a software package that allows a user to either change or get access to a system that was not coordinated into the package, is referred to as a **vulnerability**. It is through this vulnerability that a user is able to gain access to a system without the necessary authority. With the advancement of technology, new susceptibilities continue to surface. It is therefore necessary for software manufacturers to produce patches for their products.

1.4.1.1 Self Inflicted Vulnerabilities

Generally a network will contain both private as well as public data. It is in a company's best interest to protect both sets of data and make provision for the data to be accessed by outside users without enabling them to alter it. The company's website should be available to the general public, whereas certain internal private information should remain privileged. Network security ensures that any attempt at hacking is averted and prevents the network from being used as a launch pad for attacks against other networks.

Three specific reasons explain why a security program may be ineffective

- Because a security program forms the bases of all efforts related to security, it is vital that it is fundamentally sound. It may be flawed for the following reasons:
 - **An unwritten policy:** Printing and handing out the policy reduces confusion
 - **Politics:** Ensuring that the policy remains consistent ensures that it does not become redundant.
 - **No continuity:** A high staff turnover will result in a reluctance to adhere to the policy
 - **Absence of a recovery plan:** Forensic efforts may be stunted if there is no recovery plan. A good plan includes contingencies for security violations.
 - **No reviewing:** Failure to observe error logs and configuration changes places companies at risk.
 - **No allocation for patch management:** An effective policy makes provision for regular upgrades without compromising security
 - **No access control:** No control over password distribution can lead to a security violation
- With the increase in network complexity the information base needed to be configured as the system broadens. If it is not, it would represent a weak configuration.
 - **Equipment that has been misconfigured:** To simple a configuration will result in serious security issues. Simple Network Management Protocol (SNMP) settings and router protocols are some of the areas that are vulnerable.
 - **Simple passwords:** Passwords should not be easy to guess. Avoid the use of common words. The more complex the password the better. Ideally a minimum of eight characters should be used and should include lower and uppercase numbers. Avoid using the default password. The password should not be too difficult to remember. The **vanity plate** method suggests that a word or phrase be changed using characters found on a vanity license plate. Change the case of the letters and exchange one or two with numbers.

- **Internet services that are misconfigured:** Identifying the exact services needed as well as the ones presently in operation will prevent Internet services from developing security violations. Some protocols like File Transfer Protocol (FTP) security settings, as well as Java scripts and Java applets are all capable of being misconfigured.
- **Default settings** are largely designed to assist in the configuration of devices to enable it to be placed in a production environment.
- The majority of technology has inherent weaknesses or flaws. These may be found in the operating system or inside the protocol or the networking equipment itself:
 - **Weak operating system:** Operating systems are coded instructions written for the computer. If a user is able to manipulate these instructions as a result of a weakness in the operating system, it will affect the functioning of that system. Keeping these systems patched reduces weaknesses.
 - **Weak protocols:** Some protocols like Network File System (NFS), ICMP, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are designed without security components
 - **Weak Application:** When designing an application, it is important to keep it functional. Service packs, upgrades and patches are often made available by the developer as flaws are discovered. With the development of technology it has become increasingly important to make security a serious issue, to the point of having them written into the design of new applications.
 - **Weak Equipment:** Most systems have their strengths and weaknesses. Identifying them would place the administrator in good stead when overcoming pitfalls. Knowledge of the nature of network traffic to be supported will assist in placing the proper device in the proper location on the network. Of equal importance is the regular testing of systems to ensure effectiveness of their functions.

1.4.2 Threats

Structured threats are performed by individuals seeking a particular target. They are regarded as the more dangerous threats because of its organization. **Unstructured threats** are far more regular and are 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.

1.4.3 The Motivation of Network Intruders

An intruder can be:

- A **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.
- A **script kiddie** is a novice hacker who uses publicly available scripts to test the integrity of networks and scan for weakness.
- A **cracker** is an individual possessing a broad knowledge of networking and the Internet and often thought to have spiteful intentions.

Reasons for intrusions:

- **Curiosity:** As it suggests, these intruders are motivated by pure curiosity and are often not malicious in intent.
- **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 normally target specific data. Passwords as well as other security measures need to be changed as soon as vital staff leaves 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 companies, and therefore places itself at huge risk. This is also known as **hactivism**, the act of defacing an organizations' web site for political objectives.
- **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 the need for them is met.

1.5 Different Network Attacks

1.5.1 Renaissance Attacks

The goal of these attacks would be 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 programs enabling rookie attackers to launch attacks on networks.

- **DNS whois queries:** A whois query of the DNS will grant the user access to information such as the address of a specific domain and its owner.
- **Ping sweep** provides 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 the 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 of this scan
- **Block scans** combines 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.

1.5.2 Access attacks

The goal of an access attack is to gain access to a computer or network. After access is gained, an intruder 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:** After 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. **Unauthorized 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.
- **Fabrication:** The intruder 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:
 - Some **viruses** 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.
 - 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 hard drive. 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 scrutinized by the attacker. More commonly, it will be used to control the system and incorporate it in a DDoS attack.

1.5.3 Denial of Service (DoS) Attacks

They are designed to reject access to a computer or system. DoS attacks normally target precise services and try 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.

1.6 Defense

Internetworking refers to the job of connecting diverse networks so they can communicate and exchange resources. For the majority of businesses, their border would extend as far as the Internet. However with the existence of intranet, extranet and remote user connections, the real border becomes unclear. This translated effectively means that it is difficult to secure your network by only placing a firewall at the Internet gateway. Multiple layers of diverse defense mechanisms are needed to curb an attack. This grants you the ability to stave off a more diverse number of attacks. Because of the complexity of network attacks it has become possible to attack numerous areas of the network. Here are some of the targets:

- **Routers:** The attack on a router may take various forms and depends chiefly on the attackers' objective. Access attacks are used if the intent is to obtain entry to the network or router. To sabotage the router and deny access, a DoS or DDoS attack is used.

- **Firewalls:** This is essentially the same as the attacks on routers although the method may differ according to the size and type of firewall.
- **Switches:** Any attack on a component of the network will have an effect on the way traffic flows across that segment. It is important to secure switches because traffic flow tends to converge there.
- **Networks:** They are usually affected when there is a successful attack on the routers, firewalls and switches.
- **Hosts:** A host can be used to initiate attacks against other network resources. They are often attacked only because the user has found a weakness and wants to take advantage.
- **Applications:** Vulnerabilities within an application can be used to violate a host. With the increase in technology, the number of attacks increase.
- **Data:** The actual data has no weaknesses, but it is possible for it to be copied, altered or destroyed if access is gained.
- **Management components:** Because they are used to manage various network components, it is vital that they are secured to prevent control of the whole network.

1.6.1 Elements of Defense

The following list details the elements used in a defense in depth strategy:

- **Security policy:** It describes the who, what and where of the company's operations.
- **The use of AAA:** When implementing AAA we essentially ensure that only those authorized to do so, access the resources needed to do their jobs. It can also help to see if users are doing tasks that expose the network to security risk.
- **VPN connections:** This technology is usually employed as a cost saving measure because of its ability to interconnect offices across the Internet. This technology is not however limited to the Internet and depends largely on the company's business function, the nature of its data and the risk involved. Because of the sensitive nature of their data, many companies choose VPN technology to secure dedicated circuits between their offices regardless of both end points being known. The saving is made by reason that the company is able to connect across secure public networks and thereby eliminate expensive dedicated connections. An added advantage is the ability to secure connections for remote users. Broadband Internet connections make it possible for many users to work from home employing an encrypted connection to their company's network.
- **Segmentation:** The best manner in which to protect assets is to separate them in order of their value and reserve access to specific users and groups. This segmentation of the network may be completed by means of firewalls, routers and switches, and by effectively implementing access lists, VLANs and address/port translations. Certain assets that require particular access to particular users may be grouped together and placed on the same network segment. Restricting access to confidential data may be done via the use of non standard ports by using Network Address Translation (NAT) and Port Address Translation (PAT). All network resources are separated according to their category and worth. The greater the value to the organization the deeper in the network it will be placed and by so doing protected at a number of levels in the network. RFC 1918 addressing put to use on the internal networks will prevent attacks that come from the Internet unless those systems are NATed at the network border or perimeter. It is strongly advised to place Network Intrusion Detection Systems (IDS) extensively at all critical points on the network.

- The known hostile entities are normally addresses that have done reconnaissance attacks or are verified by either firewall or IDS log correlation and trending. These addresses are usually blocked at the perimeter. Organizations that have amenders that contrast those of another would normally be seen as hostile and either monitored vigilantly or have their access completely blocked.
- **Dynamic perimeter security:** It is unwise to think that a statically arranged firewall or router will guard your network against attacks in an environment that is as ever changing as the Internet. A device set up in this manner can only prevent against known attacks. Because of the advancement of technology it is vital to protect against attacks of an unknown nature. Effective deployment of firewalls, routers and IDS will aid in this respect.
- **Host based defense:** A secure host is needed in order to deploy a host based defense. Service packs and patches are made available by the developers of operating systems and applications as soon as new weaknesses are uncovered. Ensuring that all systems meet with the recommended patch level will reduce the number of weaknesses to be exploited. Should an attacker penetrate numerous levels of defense in order to arrive at the target host, the attack would still be ineffective if they are unable to access their target. In order to detect and prevent illegal actions on the host system, a host based IDS is installed between the operating system and the kernel. They also send out an alarm to indicate that the system is under attack.

Two types of host based IDS exist:

- **Signature based** oversees the system and match instruction sets with the signature of attack profiles that are known.
 - **Anomaly based** establishes a threshold of approved activities. If the instruction does not match or form part of the approved threshold it is identified as an attack. It is possible to configure the anomaly based IDS to execute certain functions when it receives an instruction that is not in the threshold instead of just blocking it. The greatest advantage is that it is able to protect against known and unknown threats.
- **Effective monitoring:** Firewalls, routers, switches and IDS produce vast amounts of log data. It is vital that critical systems are monitored effectively to determine the state of the network.
 - **Correlation and trending** follows monitoring. These step aides in establishing what is normal. Thus having established what is normal it is now possible to determine what is not and needs to be reacted to. Correlation products make it possible to correlate data from various devices to enable you to better understand the situation. This makes it possible to see data from a possible attack from different sources.
 - **Security process:** The process is the effectual execution of the policy. The process is evolving and is the force behind the steady improvement of the security posture.

1.6.2 Physical Security

Physical access to amenities and networks should be restricted to authorized personnel within the company or persons who have a business function within the company.