



642-511

Cisco Secure VPN

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 Figures

List of Acronyms

Introduction

1. Virtual Private Networks (VPN's) and IPSec: An Overview

1.1 Virtual Private Network Applications

- 1.1.1 Remote Access VPN's
- 1.1.2 Intranet Access VPN's
- 1.1.3 Extranet Access VPN's

1.2 Cisco VPN Technologies

- 1.2.1 Cisco VPN Routers
- 1.2.2 Cisco Pix Firewalls
- 1.2.3 Cisco VPN 3000 Concentrators
- 1.2.4 Cisco VPN Clients
- 1.2.5 Cisco Management Software

1.3 Cisco IOS IPSec Technologies

- 1.3.1 IPSec Overview
- 1.3.2 IPSec Security Protocols
 - 1.3.2.1. Authentication Header (AH)
 - 1.3.2.2 Encapsulating Security Payload (ESP)
 - 1.3.2.3 Transport Mode
 - 1.3.2.4 Tunnel Mode

1.4 Security Associations (SA)

1.5 Protocols used by IPSec

- 1.5.1 Message Encryption
- 1.5.2 Message Integrity
- 1.5.3 Peer Authentication
- 1.5.4 Key Management
 - 1.5.4.1 Diffie-Hellman Key Agreement (DH)
 - 1.5.4.2 Certificate Authorities (CAs)

1.6 IPSec Peer Authentication and the Formation of Security Associations

1.7 Creating VPN's with IPSec



2. Cisco VNP 3000 Concentrator Hardware Overview

2.1 The Benefits of Cisco VPN 3000 Series Concentrators

- 2.1.1 Easy deployment, utilization and improvement
- 2.1.2 Security
- 2.1.3 Scalability and Performance
- 2.1.4 Vigorous Management
- 2.1.5 High Availability and Fault Tolerance

2.2 Cisco VPN 3000 Concentrator Series Models

- 2.2.1 Cisco VPN 3005 Concentrator
- 2.2.2 Cisco VPN 3015 Concentrator
- 2.2.3 Cisco VPN 3030 Concentrator
- 2.2.4 Cisco VPN 3060 Concentrator
- 2.2.5 Cisco VPN 3080 Concentrator

2.3 Cisco VPN 3000 Concentrators LED Indicators

2.4 Cisco VPN 3000 Concentrator Series Client Support

- 2.4.1 Cisco VPN Client
- 2.4.2 Cisco VPN 3002 Hardware Client
- 2.4.3 Cisco Internet Mobile Office
- 2.4.4. Wireless Client Support

3. Configuring Cisco VPN 3000 Remote Access Networks Using Preshared Keys

3.1 Remote Access VPN's with Preshared Keys

- 3.1.1 Unique Preshared Keys
- 3.1.2 Group Preshared Keys
- 3.1.3 Wildcard Preshared Keys

3.2 VPN Concentrator Configuration

- 3.2.1 Initial Configuration
- 3.2.2 Using the VPN 3000 Concentrator Series Manager
- 3.2.3 Advanced Configuration options of the VPN Concentrator
 - 3.2.3.1 Configuration | System | Servers
 - 3.2.3.2 Configuration | System | Address Management
 - 3.2.3.3 Configuration | System | Tunneling Protocols
 - 3.2.3.4 Configuration | System | IP Routing
 - 3.2.3.5 Configuration | System | Management Protocols
 - 3.2.3.6 Configuration | System | General
 - 3.2.3.7 Configuration | System | Events
 - 3.2.3.8 Configuration | System | Load Balancing Cisco VPN Clients
 - 3.2.3.9 Configuration | System | Client Update
 - 3.2.3.10 Configuration | User Management
 - 3.2.2.11 Configuration | Policy Management

- 3.3 Installing and Configuring the VPN Client
 - 3.3.1 VPN Client Overview
 - 3.3.2 VPN Client Features
 - 3.3.3 VPN Client Installation and Configuration
 - 3.3.3.1 Installing the VPN Client
 - 3.3.3.2 Configuring the VNP Client

4. Configuring Cisco VPN 3000 for Remote Access with Digital Certificates

- 4.1 CA Support Overview
 - 4.1.1 Certificate Authorities (CA) Architecture
 - 4.1.1.1 Certificate Requests
 - 4.1.1.2. Enrollment and Authentication
 - 4.1.1.3 CA Hierarchies
 - 4.1.1.4 Certificate Revocation
 - 4.1.2 Simple Certificate Enrollment Protocol (SCEP)
 - 4.1.2.1 Manual SCEP Authentication Mode
 - 4.1.2.2 Preshared Key SCEP Authentication Mode
 - 4.1.3 CA Vendors and Products who Support Cisco VPN Products
- 4.2 Digital Certificate Support using the VPN 3000 Concentrator Series Manager
 - 4.2.1 Generating, Enrolling and Installing Certificates
 - 4.2.1.1 Enrolling Identity Certificates through PKCS #10
 - 4.2.1.2 Generating and Installing Certificates Automatically through SCEP
 - 4.2.1.3 Enrolling Identity Certificates through SCEP
 - 4.2.2 Validating Certificates
 - 4.2.3 Certificate Revocation Lists
 - 4.2.4 IKE Configuration
- 4.3 Configuring Cisco VPN Client for CA Support

5. Configuring Cisco VPN Client Firewall Features

- 5.1 VPN Client Firewall Features Overview
- 5.2 VPN Client Firewall Configuration Overview
 - 5.2.1 The Stateful Firewall (Always On) Feature
 - 5.2.1.1 The Cisco Integrated Client Feature
 - 5.2.1.2 The Centralized Protection Policy Feature
 - 5.2.1.3 The Are You There Feature
- 5.3 Firewall Rules
 - 5.3.1 Default Firewall Rules
 - 5.3.2 Configuring Firewall Rules
- 5.4 Configuring the Stateful Firewall Feature

5.5 Configuring the VPN Concentrator for Firewall Usage

- 5.5.1 Firewall Setting
- 5.5.2 Firewall
- 5.5.3 Custom Firewall
- 5.5.4 Firewall Policy

5.6 VPN Client Firewall Statistics

5.7 Providing Automatic Client Updates

6. Administering and Monitoring the VPN 3000 Series Concentrator

6.1 Administering the VPN 3000 Series Concentrator

6.2 Monitoring the VPN 3000 Series Concentrator

7. Configuring the Cisco 3002 Hardware Client for Remote Access

7.1 Configuring VPN 3002 Hardware Client remote access with Preshared Keys

- 7.1.1 Confirming IKE and IPSec Configurations
- 7.1.2 Setting Debug Levels
 - 7.1.2.1. Ping Failure through an Established Tunnel
 - 7.1.2.2. IKE Phase 1 Failures
- 7.1.3 Configuring the VPN 3002 Hardware Client and LAN Extension Modes
- 7.1.4 Split Tunneling

7.2 VPN 3002 Hardware Client Interactive Unit and User Authentication Feature

- 7.2.1 Configuring the Head-End VPN Concentrator
- 7.2.2 Configuring Unit and User Authentication
- 7.2.3 Testing Interactive Hardware Client and User Authentication Configuration

8. Configuring the Cisco 3002 Hardware Client for Scalability

8.1. VPN 3002 Hardware Client Reverse Route Injection (RRI)

- 8.1.1 Configuring the VPN Concentrator for RIP version 2
- 8.1.2 Configuring the VPN Concentrator for OSPF
- 8.1.3 Configuring Reverse Route Injection
 - 8.1.3.1 Setting up LAN to LAN Network RRI
 - 8.1.3.2 Setting up LAN to LAN with Autodiscovery
 - 8.1.3.3 Setting up Network Extension Mode RRI
 - 8.1.3.4 Setting up Client RRI
 - 8.1.3.5 Setting up Hold-Down Routes

8.2 Configuring the VPN 3002 Hardware Client Backup Servers

8.3 VPN 3002 Hardware Client Load Balancing



8.4 Port Address Translation (PAT)

8.5 Configuring IPsec on the VPN 3002 Hardware Client

8.5.1 Configuring IPsec Over TCP/IP

8.5.2 Configuring IPsec over UDP (UDP NAT Transparent IPsec)

8.5.3 Troubleshooting the VPN 3002 Hardware Client IPsec Connection

8.5.4 Configuring Debug Levels

8.5.4.1 Ping Failure Across an Established Tunnel

8.5.4.2 IKE Phase 1 Failures

8.5.4.3 Incorrect Password on the VPN 3002 Hardware Client

8.6 Configuring the VPN 3002 Hardware Client Auto-Update feature

8.7 Monitoring the VPN 3002 Hardware Client Auto-Update Events

9. Cisco VPN 3000 LAN-to-LAN Networks with Preshared Keys

9.1 VPN Concentrator in LAN-to-LAN VPN's

9.2. LAN-to-LAN Configuration

9.2.1 Configuring Network Lists

9.2.2 Using the LAN-to-LAN Wizard to Create the Tunnel

9.3 Simple Certificate Enrollment Protocol (SCEP) Support

9.3.1 Certificate Management

9.3.2 Installing Root Certificate through SCEP

9.3.2.1 Enrolling the Concentrator

9.3.2.2 Installing Identity Certificates through SCEP

9.4 Configuring Digital Certificates ON the LAN-to-LAN Connections

LIST OF TABLES

TABLE 2.1:	Cisco VPN 3000 Concentrator Series Model Comparison
TABLE 2.2:	Front Panel LED Indicators
TABLE 2.3:	Rear Panel LED Indicators
TABLE 2.4:	SEP Module LED Indicators
TABLE 5.1:	The Default Rules for the VNP 3000 Concentrator
TABLE 5.2:	Protocols and their IANA Protocol Numbers

LIST OF FIGURES

FIGURE 3.1:	The Manager Login Screen
FIGURE 3.2:	The IP Interface Screen
FIGURE 3.3:	The VPN Concentrator Series Manager
FIGURE 3.4:	The Configuration User Management Groups Screen
FIGURE 3.5:	The Modify Groups – General Tab
FIGURE 3.6:	The VPN Client Main Screen
FIGURE 4.1:	The Certificate Management Enrollment Screen
FIGURE 4.2:	The Administration Certificate Management Enrollment Identity Screen
FIGURE 4.3:	The Administration Certificate Management Enrollment Request Generated Screen
FIGURE 4.4:	The Certificate Management Screen
FIGURE 4.5:	The Configuration System Tunneling Protocols IPSec IKE Proposals Modify Screen
FIGURE 5.1:	The Statistics of the VPN Client Connection Screen
FIGURE 8.1:	Configuring RIP
FIGURE 9.1:	Administration Certificate Management Install CA Certificate

LIST OF ACRONYMS

AAA	Authentication / Authorization / Accounting
ACL	Access Control List
ACS	Access Control Server
AH	Authentication Header
AYT	Are You There
CA	Certificate Authority
CBC	Cipher Block Chaining
CET	Cisco Encryption Technology
CRL	Certificate Revocation Lists
DES	Data Encryption Standard
DH	Diffie-Hellman Key Agreement
DHCP	Dynamic Host Configuration Protocol
DLSw	Data-link Switching
DSL	Digital Subscriber Line
DSP	Digital Signal Processor
3DES	Triple DES
ECC	Elliptic Curve Cryptography
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
GRE	Generic Routing Encapsulation
HDLC	High-Level Data-Link Control
HMAC	Hash-based Message Authentication Code
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol

ICV	Integrity Check Value
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPSec	IP Security Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
IV	Initialization Vector
Kbps	kilobits per second (bandwidth)
LAN	Local Area Network
LMS	LAN Management Solution
L2FP	Layer 2 Forwarding Protocol
L2TP	Layer 2 Tunneling Protocol
MAC	Message Authentication Code
MD	Message Digest
MD5	Message Digest 5
MPPC	Microsoft Point-to-Point Compression
MPPE	Microsoft Point-to-Point Encryption
MTBF	Mean Time Between Failure
NAT	Network Address Translation
NEM	Network Extension mode
NTP	Network Time Protocol
OS	Operating System
OSPF	Open Shortest Path First
PAT	Port Address Translation
PFS	Perfect Forward Secrecy
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure

PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
QPM	QoS Policy Manager
RADIUS	Remote Authentication Dial-In User Service
ROBO	Remote office/branch office
RRI	Reverse Route Injection
RSA	Rivest, Shamir, and Adelman
RWAN	Routed WAN Management Solution
SA	Security Association
SDI	Security Dynamics International authentication
SEP	Scalable Encryption Processing
SHA-1	Secure Hash Algorithm-1
SNMS	Small Network Management Solution
SOHO	Small Office/Home Office
SPI	Security Parameters Index
SRB	Source-route bridging
SSH	Secure Shell
SSL	Secure Sockets Layer
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
URT	User Registration Tool
VDM	VPN Device Manager
VMS	VPN/Security Management Solution
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

WEP	Wired Equivalent Privacy
WLSE	Wireless LAN Solution Engine
XML	Extensible Markup Language
XAUTH	eXtended Authentication

642-511 CCSP Cisco Secure VPN

Exam Code: 642-511

Certifications:

Cisco Certified Security Professional (CCSP)

Core

Prerequisites:

Some experience and knowledge on VPN's

About This Study Guide

This Study Guide is based on the exam questions for the 9E0-121 or 642-511 Cisco Secure VPN (CSVPN) exam. It presents all the information necessary to pass the 642-511 Cisco Secure VPN (CSVPN) exam, and is detailed on the particular proficiencies examined in the exam. The Cisco Secure VPN exam is designed to test your knowledge on configuring, administering and monitoring the Cisco VPN 3000 Series Concentrators. The information provided in this Study Guide is specific to the 642-511 examination, and does not symbolize a complete reference work on the other four areas covered by the CCSP series of exams.

The following topics are covered in this Study Guide: Cisco products enable a secure VPN, Overview of IPSec Protocols, IPSec Protocol framework, How IPSec works, Cisco VPN 3000 Concentrator Series overview, Cisco VPN 3000 Concentrator Series features, Cisco VPN 3000 Concentrator Series device models, Cisco VPN 3000 Concentrator Series client support, Remote access utilizing preshared keys, Initial Cisco VPN 3000 Concentrator Series configuration for remote access, Cisco VPN 3000 Concentrator Series browser configuration, Configuring users and group, Advanced configuration of the Cisco VPN 3000 Concentrators, Configuring IPSec Windows Client, CA support, Certificate generation and installation, Authenticating certificates, Configuring the Cisco VPN 3000 Concentrators for CA support, Software client's firewall feature overview, the Stateful Firewall feature, Software client's Are You There (AYT) feature, Central Policy Protection feature, Customizing firewall policy, Client firewall statistics, Administering the Cisco VPN 3000 Series Concentrator, Monitoring the Cisco VPN 3000 Series Concentrators, Cisco VPN 3002 Hardware Client remote access using preshared keys, VPN 3002 Hardware Client interactive unit and user authentication feature, Configuring VPN 3002 Hardware Client's integrated unit authentication feature, Configuring the VPN 3002 Hardware Client's user authentication, Monitoring the VPN 3002 Hardware Client's user statistics, the VPN 3002 Hardware Client's Reverse Route Injection feature, Configuring the VPN 3002 Hardware Client backup server feature, Overview on the VPN 3002 Hardware Client's Auto-Update feature, Configuring the Auto-Update feature, Monitoring VPN 3002 Hardware Client's Auto-Update events, Configuring the VPN 3002 Hardware Client's load balancing feature, Port Address Translation Overview, Configuring IPSec over TCP, Configuring IPSec over UDP, Overview of Cisco VPN 3000 IPSec LAN-to-LAN connections, LAN-to-LAN configuration, SCEP overview, Root and Identity Certificate installation.

Intended Audience



This Study Guide is targeted specifically for people that have efficiently finished the Cisco Secure Virtual Private Networks (CSVPN) class or those that have gained knowledge on VPN's who now desire to complete the 642 -511 CCSP Cisco Secure VPN exam. The information in this Study Guide is specific to that exam. It is not a complete reference work on the other four exam topics. 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 VPN's would be advantageous.

Note: Because VPN technology is a vital component in network security, certain information contained in this Study Guide overlaps with content of the other four topics covered by the CCSP series of exams. This Study Guide does not combine all five exam topics.

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

Good luck!

1. Virtual Private Networks (VPN's) and IP Security Protocol (IPSec)

Virtual Private Networks (VPN's) provide secure and advanced connections (communication) to private institutions through a non-secure network by enabling **reliability** of data, the **privacy** of the data, and allows a user the opportunity to **validate** the data source. Private data is secure in a public environment. By eliminating WAN circuits and pricy modems, a VPN is **cost efficient**. The service provider network provides most of the hardware. Internet service providers (ISP's) provide continuous internet connectivity. **Scalability** exists when network availability can be extended with minimal costs and users can be added or deleted with ease.

1.1 Virtual Private Network Applications

A variety of VPN technologies exists. When deciding on what VPN application to implement, factors that should be considered would be the infrastructure that exists, and the business applications that are going to be deployed.

VPN's fall into three basic categories:

- Remote Access
- Intranet Access (site to site)
- Extranet Access (site to site or remote access)

Intranet VPN's enables a user to access an institutions internal network. Extranet or Remote Access VPN's enables a common environment where many different sources such as intermediaries, clients and off-site employees can access information via web browsers or email. VPN's can be established anywhere via the Internet.

1.1.1 Remote Access VPN's

Many institutions supply their own VPN connections via the Internet. Through their ISPs, remote users running VPN client software are assured private access in a publicly shared environment. By using analog, ISDN, DSL, cable technology, dial and mobile IP, VPN's are implemented over extensive shared infrastructures. Email, database and office applications use these secure remote VPN connections.

Remote Access VPN Advantages:

- Third parties oversee the dial up to the network.
- New users can be added with hardly any costs and with no extra expense to the infrastructure.
- Wan circuit and Modem costs are eliminated.
- Remote-access VPN's call to local ISP numbers. VPN's can be established from anywhere via the internet
- Cable modems enable fast connectivity and are relatively cost efficient.
- Information is easily and speedily accessible to off-site users in public places via Internet availability and connectivity.

Remote Access VPN Disadvantages:

- IPsec can be slow in interpreting data as it has to be encrypted as the data leaves and decrypted as it enters. This can be pricy for smaller business and can have a performance hit on some applications.
- Connections can be lost as data travels via the Internet because it is Public Infrastructure. There is no certainty on the time that a delay can take.

VPN's can use one of the following 2 points to commence encryption:

- **@ dial up (client- initiated)** - The encryption channel is initiated by using Layer 2 Tunnel Protocol (L2TP), Point-to-Point Tunneling Protocol or IPsec. Many ISP's can be used. End to end data security exists. This can be enhanced by using Cisco's VPN Client. However, a disadvantage is that each remote user has to install a VPN Client.
- **network access server (NAS initiated)** - The encryption channel is initiated by using Layer 2 Tunnel Protocol (L2TP) or Layer 2 Forwarding (L2F) with a ISPs presence. Only one ISP can be used. The need for each client to install a VPN Client is eliminated. End to end data security is questionable because the data circuits between the ISP and the client is not secure.

1.1.2 Intranet Access VPN's

Site to site VPN's enable a company to extend its internal network to branch offices or off-site employees. Remote users would therefore have access to the shared network e.g. via email. VPN's enable a secure point of contact between two end devices e.g. firewalls, routers. The user on each LAN connected to the router can communicate to the other LAN. What information is available would depend on what information is sharable and is determined by a company's security policies. Company data is kept safe by the use of dedicated circuits. Frame Relay, Asynchronous Transfer Mode (ATM), or point-to-point circuits are examples of infrastructures used by VPN's.

1.1.3 Extranet Access VPN's

Extranet Access could be a remote access or site to site access connection for a broker, agent, business partner or any other applicable non employee. Extranet VPN's enable these connections to a company's network. A combination of remote access and intranet access infrastructures are used. The distinction would be the rights that are assigned to these users. Some level of security or authentication would be necessary to access the network, protect network resources, and prevent others from accessing the information.

1.2 Cisco VPN Technologies

Cisco provides various technologies like VPN Routers, Pix Firewalls, VPN 3000 Concentrators and various VPN Clients.

1.2.1 Cisco VPN Routers

Cisco VPN-Optimized routers are used when building intranet or extranet site-to-site VPN's. Cisco VPN Routers running on IOS Software provide routing, quality of service (QoS), security, multi-protocol capabilities and scalability. Digital Subscriber Lines (DSL) and cable modems provide VPN access for

businesses from small office/home office (SOHO). Specific components can be provided for VPN routers that will deal with encryption processing. This in turn will free memory.

The following Cisco VPN Routers exists:

- The **Cisco 827H ADSL Router** and **Cisco uBR905 Cable** is used at the following locations: Remote Access VPN's, Extranet VPN's and SOHO's. Features include integrated DSL modem, 4-port 10BaseT hub, fixed configuration and support for EzVPN Remote. The Cisco 827H ADSL performs at 384 kbps, having a max of 50 tunnels and the Cisco uBR905 Cable performs at 6 Mbps and a max of 50 tunnels.
- The **Cisco 806 Broadband Router** is used at the following locations: Remote Access VPN's, Extranet VPN's and SOHO's. Aspects include fixed configuration, installed behind broadband modem, 10BaseT Ethernet WAN interface, 4-port 10BaseT LAN hub and support for EzVPN Remote, performing at 384 kbps with a max of 50 tunnels.
- The **Cisco 1700 Router Series** is used at the following locations: Remote Access VPN's, Extranet VPN's, Intranet VPN's and small branches. Features comprise of modular configuration, support for VPN Module, and EzVPN Remote and Server, performing at 4 Mbps and a max of 100 tunnels with VPN Module.
- The **Cisco 1710 Router Series** is used at the following locations: Remote Access VPN's, Extranet VPN's and SOHO's. Aspects include fixed configuration, 10/100 Fast Ethernet port, 10BaseT Ethernet port and support for EzVPN (Easy VNP) Remote and Server, performing at 3 Mbps with a max of 100 tunnels
- The **Cisco 2600 Router Series** is used at the following locations: Extranet VPN's, Intranet VPN's and branches. Features include modular configuration, support for VPN Module and EzVPN Server, performing at 14 Mbps with a max of 800 tunnels with VPN Module.
- The **Cisco 3600 Router Series** is used at the following locations: Extranet VPN's, Intranet VPN's and large branches. Aspects include modular configuration, support for VPN Module and EzVPN Server, performing at 40 Mbps, and a max of 1800 tunnels with VPN Module.
- The **Cisco 7100 Router Series** is used at the following locations: Extranet VPN's, Intranet VPN's and central hub sites. Aspects include modular configuration, support for EzVPN Server and VAM, performing at 145 Mbps and a max of 5000 tunnels with VPN and Acceleration Modules.
- The **Cisco 7200 Router Series** is used at the following locations: Extranet VPN's, Intranet VPN's and central hub sites. Aspects include modular configuration, support for EzVPN Server and VAM, performing at 145 Mbps and a max of 5000 tunnels with Acceleration Module.

1.2.2 Cisco Pix Firewalls

Cisco Pix Firewalls offers a VPN gateway alternative to a router or concentrator, and supplies a variety of security and networking services. Cisco PIX Firewalls supports VPN Clients, Cisco VPN 3002 Hardware Client, IPsec VPN, PPTP and Layer 2 Tunneling Protocol (L2TP) VPN's from Microsoft Windows clients, Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) AAA support and Dynamic Host Configuration Protocol (DHCP).

The following Cisco Pix Firewalls exists:



- The **Cisco PIX 501 Firewall** is used at the following locations: Extranet VPN's, Intranet VPN's, SOHO and Remote Access VPN's. Features include fixed configuration, 10 Mbps of firewall throughput, perfect for securing always-on broadband connections, 10BaseT outside interface, integrated 4-port 10/100 switch, supports EzVPN Client, performs at 3 Mbps with 5 simultaneous VPN peers.
- The **Cisco PIX 506E Firewall** is used at the following locations: Extranet VPN's, Intranet VPN's, Remote office/branch office (ROBO) and Remote Access VPN's. Aspects include fixed configuration, 20 Mbps of firewall throughput, 10BaseT inside and outside interfaces, and performs at 16 Mbps with 25 simultaneous VPN peers.
- The **Cisco PIX 515E Firewall** is used at the following locations: Extranet VPN's, Intranet VPN's and small and medium business. Features comprise of modular configuration, capacity for up to 6 10/100 Fast Ethernet (FE) interfaces, support for up to 125,000 concurrent connections and for 2 single-port FE modules or one 4-port FE module, a failover port for high availability, support for VPN Accelerator Card, performs at 63 Mbps with a max of 2000 tunnels.
- The **Cisco PIX 525 Firewall** is used at the following locations: Extranet VPN's, Intranet VPN's and enterprise and service provider. Features include modular configuration, a failover port for high availability, support for VPN Accelerator Card, 280,000 concurrent connections, Gigabit Ethernet interface and single-port or fourport 10/100 Fast Ethernet interfaces, performs at 70 Mbps with a max of 2000 tunnels with VAC
- The **Cisco PIX 535 Firewall** is used at the following locations: Extranet VPN's, Intranet VPN's and enterprise and service provider. Aspects include modular configuration, a failover port for high availability, support for VPN Accelerator Card, 500,000 concurrent connections, 66-MHz Gigabit Ethernet interface and single-port or fourport 10/100 Fast Ethernet interfaces, performs at 95 Mbps with a max of 2000 tunnels with VAC

1.2.3 Cisco VPN 3000 Concentrators

Cisco VPN 3000 Series Concentrators offers excellent encryption and authentication procedures and supports wireless clients. They are available in several models that handle many VPN connections while supplying site to site and remote access VPN abilities for a network.

The products in the Cisco VPN 3000 Series Concentrator range are:

- The **Cisco VPN 3005 Concentrator** and **Cisco VPN 3015 Concentrator** handle a majority of 100 simultaneous sessions. The Cisco VPN 3015 Concentrator is upgradeable to the Cisco VPN 3030 Concentrator.
- The **Cisco VPN 3030 Concentrator** handles a majority of 1500 simultaneous sessions, support Scalable Encryption Processor (SEP) modules and offer redundant and nonredundant configuration. The Cisco VPN 3030 Concentrator is upgradeable to the Cisco VPN 3060 Concentrator.
- The **Cisco VPN 3060 Concentrator** supports a majority of 5000 simultaneous sessions, support Scalable Encryption Processor (SEP) modules and offers redundant and nonredundant configuration. The Cisco VPN 3060 Concentrator is upgradeable to the Cisco VPN 3080 Concentrator.
- The **Cisco VPN 3080 Concentrator** handles a majority of 10 000 simultaneous sessions, supports Scalable Encryption Processor (SEP) modules and offer redundant and nonredundant configuration.

1.2.4 Cisco VPN Clients

Client VPN software ensures secure remote access to central Cisco routers, PIX Firewalls, and VPN Concentrators and eases the maintenance and administration of VPN connections.

The following Cisco VPN Clients exists:

- The **Cisco VPN Client** (Unity Client) supports Windows 95, 98, Me, NT 4.0, 2000, XP, versions of Linux, Solaris, and MAC OS. It can be preconfigured and is packaged with the Cisco VPN 3000 Series Concentrator at no extra charge to the purchasing party, thus ensuring cost efficiency and the simplification of initial build up. IPSec VPN's can be created to any other Cisco remote access VPN product at a core location.
- The **Cisco VPN 3002 Hardware Client** ensures a VPN tunnel for the whole location and eliminates the need for having many software clients installed at each workstation. The mechanism can connect with an EzVPN Server and the use of an integrated 8-port 10/100 Ethernet switch is not compulsory
- The **Cisco Easy VPN Client** is made up of Cisco Easy VPN Remote and Cisco Easy VPN Server. Because the end points of the VPN connections do not need to be configured alike, Cisco Easy VPN Remote can be configured to create IPSec. Cisco Easy VPN Remote and Cisco Easy VPN Server are constructed on Cisco Unified Client Framework. Cisco Easy VPN Server can cease Cisco VPN Client connections. Cisco VPN 3002 Hardware Clients, Cisco Easy VPN Remote Cisco 800 Series Routers, Cisco 1700 Series Routers, Cisco uBR900 Series Routers and Cisco PIX 501 Firewalls support Cisco Easy VPN Remote. Cisco VPN 3000 Series Concentrators, Cisco PIX Firewalls, Cisco 1700 Series, Cisco 7100 Series, Cisco 7200 Series and other Cisco Routers support Cisco Easy VPN Server.
- **Wireless Client Support** is Elliptic Curve Cryptosystem (ECC)–compliant and is used with IP-enabled wireless mechanisms. Like Cisco VPN Client, they are packaged with Cisco VPN 3000 Series Concentrators. They are best suited for mechanisms with inadequate processing resources and ensure speedy data processing.
- By using remote access devices, Cisco Mobile Office At Work networks, wireless LANs, routers, firewalls, and concentrators, **Cisco Internet Mobile Office** provides secure VNP support for on-site and off-site users.

1.2.5 Cisco Management Software

The Cisco VPN Device Manager (VDM) and Cisco Works 2000 supply many web based management and maintenance tools for VPN system

- The **Cisco VPN Device Manager** (VDM) is installed on the Cisco Series 7100, Cisco Series 7200 and Cisco 7400 Series Routers' flash memory at no charge. VPN tunnel throughput, traffic and system performance can be monitored.
- **CiscoWorks 2000** is a wide-ranging assemblage of modular management and monitoring tools available for a network. Examples include CiscoWorks for Windows, CiscoWorks LAN Management Solution (LMS), CiscoWorks QoS Policy Manager (QPM), CiscoWorks Routed WAN Management Solution (RWAN), CiscoWorks Small Network Management Solution (SNMS), CiscoWorks VPN/Security Management Solution (VMS), CiscoWorks Wireless LAN Solution

Engine (WLSE), Cisco Catalyst 6500 Network Analysis Module (NAM), Cisco Hosting Solution Engine, Cisco Secure Access Control Server (ACS), Cisco User Registration Tool (URT).

Cisco's Authentication, Authorization, and Accounting (AAA) server supports TACACS+ and RADIUS and is Cisco Secure Access Control Server (ACS). Like CiscoWorks VPN/Security Management Solution, they are more associated with VPN controls than other members of the Cisco Works family. Cisco Secure ACS is easy to install. It can be used to create different access application security groups and can be coupled to handle application failover support. Cisco Secure for UNIX runs on the Sun Solaris operating system, versions 2.51, 2.6, 7, 8, while Cisco Secure for NT runs on Microsoft Windows NT 4.0 Server and Microsoft Windows 2000 Server. However, Cisco Secure ACS for NT version 3.1 can only run on the Windows 2000 platform.

Intranet VPN's, extranet VPN's and remote access VPN's are configured and monitored via the capabilities available by CiscoWorks VPN/Security Management Solution (VMS). They comprise of the following products:

- Cisco IDS Host Sensor runs on Microsoft Windows NT or 2000 Server and Sun Solaris Ultrasparc systems running Solaris versions 2.6, 7, and 8. The servers are turned into intrusion detection sensors. The Cisco IDS Host Sensor acquires attack signatures from the console system and reports the attempt to the console.
- The CiscoWorks VPN Monitor aids problem solving by assembling and hoarding knowledge about IPSec VPN connections. They support Cisco VPN Routers and the Cisco VPN 3000 Series Concentrators.
- CiscoView provide administrators with a depiction of each mechanisms performance. Color coded modules, indicators and ports show the updated status of each component.

CiscoWorks Auto Update Server Software, CiscoWorks CD One, CiscoWorks Common Services Software, CiscoWorks Management Center for IDS Sensors, CiscoWorks Management Center for PIX Firewalls, CiscoWorks Management Center for VPN Routers, CiscoWorks Monitoring Center for Security are all part of the Cisco Works.

1.3 Cisco IOS IPSec Technologies

1.3.1 IPSec Overview

IPSec protects, secures and authenticates data between IPSec peer devices such as Cisco Routers, VPN software clients, VPN 3002 hardware clients, PIX Firewalls, and the VPN 3000 Series Concentrators. Peers can be teams of hosts, teams of security gateways or can be between a security and a host gateway. Multiple data flows between IPSec peers are confidential and protected.

The primary IPSec traffic security protocols are the Authentication Header (AH) and Encapsulating Security Payload (ESP). IPSec uses existing encryption and authentication standards to complete the protocol suite and to negotiate protocol between peers:

- Other IPSec protocols are Security Association: Internet Key Exchange (IKE), Internet Security Association and Key Management Protocol (ISAKMP);
- Message Encryption: Data Encryption Standard (DES) and Triple DES (3DES);

- Message Integrity (Hash) Functions: Hash-based Message Authentication Code (HMAC), Message Digest 5 (MD5), Secure Hash Algorithm-1 (SHA-1);
- Peer Authentication: Rivest\ Shamir\Adelman (RSA) Digital Signatures, RSA Encrypted Nonces; and
- Key Management: Diffie-Hellman (D-H), Certificate Authority (CA).

IPSec packets can be disintegrated and assembled again. IPSec provides perpacket data authentication and is slower than Cisco Encryption Technology (CET). IPSec does not support multipoint tunnels. In order for IPSec to have access to global addresses, it has to occur before NAT. IPSec only supports unicast IP datagrams, High-Level Data-Link Control (HDLC), ATM, Point-to-Point Protocol (PPP), Frame Relay serial encapsulation, Generic Routing Encapsulation (GRE), IP-in-IP (IPinIP) and Encapsulation Layer 3 tunneling protocols.

1.3.2 IPSec Security Protocols

Authentication Header (AH) and Encapsulating Security Payload (ESP) are IPSec's main security protocol and can be used jointly or separately. They perform at the network layer and determine which security components to use for an IP packet. Security Associations (SA's) are created between security pairs after Internet Key Exchange (IKE) and IPSec determine encryption and authentication services amongst pairs. SA information is stored in a Security Association Database. Authentication Header or Encapsulating Security Payload identifies a Security Association by its unique Security Parameters Index (SPI) number and IP destination address. The exact same SA must be to be created on each peer.

1.3.2.1. Authentication Header (AH)

AH authentication protocol is used when data integrity and authentication are relevant factors and confidentiality is not. ESP encryption costs are eliminated. AH does not provide for encryption. Both ends of the tunnel do a one-way hash calculation on the IP packet by using a shared secret key that is inserted between the IP header and the Layer 4 header of the IP datagrams. The packet is sent to the IPSec receiver, who in turn performs a one-way hash calculation on the IP header and data using the known shared secret key. In this manner data authenticity is guaranteed. The receiving host will dispose of a modified packet. Optional antireplay protection services that necessitate a receiving host to indicate that an IP packet has been perceived can be used.

- The 8 bit Next Header field holds the Layer 4 header protocol number (6 or 17) following the IPSec header. The value would be 51 where the IP header is before the IPSec header.
- The 8 bit Payload Length field holds the length of the IPSec header. The Authentication Data portion and fixed data portion are each 3 32-bit words minus 2 in length, thereby making the value in the Payload Length field 4 (6 minus 2).
- The 16 bit Reserved field is not used and is merely packed with zeros.
- The 32 bit Security Parameters Index holds the receiving IP address and the IPSec protocol
- The 32 bit Sequence Number field is a designated increasing sequence counter that facilitates antireplay services for Security Associations. The value starts at zero and cannot be repeated when the receiving hosts has antireplay services. The source has to send this data although the IPSec receiver does not have to use it.

- The Authentication Data field is variable, contains the Integrity Check Value (ICV) that comprises of an integral multiple of 32-bits. Authentication algorithms like keyed Message Authentication Codes (MAC) that contains the shared secret key are used.

1.3.2.2 Encapsulating Security Payload (ESP)

ESP ensures data confidentiality through encryption, data integrity, data authentication, features that support optional antireplay services and limited traffic flow confidentiality. With ESP, encryption is done at the IP packet layer and the IP datagram is encapsulated with a header and footer. To ensure confidentiality, various symmetric encryption algorithms are used e.g. 56-bit DES. MAC addresses can be used to ensure data integrity and authentication.

- The 8 bit Next Header field holds the Layer 4 header protocol number (6 or 17) following the IPSec header. The value would be 50 where the IP header is before the IPSec header.
- The variable Payload field contains the original IP datagram. In tunnel mode it contains the entire original datagram, and in transport mode only the upper-layer portions are included.
- Padding (0–255 bytes) must be used to ensure that the Next Header and Pad Length fields are right aligned, surrounded by a 4-byte (32-bit) boundary.
- The 8-bit Pad field indicates the Padding bytes used.
- The 32 bit Security Parameters Index holds the receiving IP address and the IPSec protocol
- The 32 bit Sequence Number field is a designated increasing sequence counter that facilitates antireplay services for Security Associations. The value starts at zero and cannot be repeated when the receiving hosts has antireplay services. The source has to send this data although the IPSec receiver does not have to use it.
- The Authentication Data field is variable and contains the Integrity Check Value (ICV) that comprises of an integral multiple of 32-bits. When the SA identifies authentication the field is not obligatory.

1.3.2.3 Transport Mode

Transport mode is used for connections between 2 end-hosts mechanisms, or between a gateway e.g. Cisco Pix Firewall or Router, and a remote host device. In this instance the gateway would be the destination device. A one on one host to host connection exists.

In AH transport mode, the AH is added between the Layer3 and Layer 4 headers and all uncommon fields are authenticated. With AH transport mode the IP header is included in the authentication processes, NAT has to occur before the IPSec protocols.

With ESP transport mode, the ESP trailer and Integrity Check Value are added at the end of the datagram. Authentication exists from the ESP header to the ICV. The IP header is not included in the data encryption and authentication processes. ESP supports NAT in both modes of transportation.

1.3.2.4 Tunnel Mode

Tunnel mode is a VPN connection between gateways. Tunnel mode is used when a host wants to connect or gain access to a network controlled by that gateway. The source and destination addresses are encrypted. With transport mode the original IP header is shifted to the left. However, with tunnel mode, the original IP datagram is left in tact. The original IP header is merely copied and moved to the left and becomes a new IP header. The IPSec header is inserted between these two headers. The original IP datagram can be authenticated and encrypted. When utilizing ESP encryption and authentication, encryption occurs before authentication.

1.4 Security Associations (SA)

Security associations are reports between VPN devices that depict the manner in which these end points will use security services. IPSec protocols provide data integrity, data authentication and encryption facilities. Once you decide on which security services you need, the two IPSec peers need to determine which hashing, authentication and encryption algorithms to use for each service. A comparison needs to be done to ensure that the source services are sustained by the receiving peer. Algorithm session key requirements would be exchanged between the peers. IPSec uses SA's to manage this negotiation process that establishes secure communication processes between VPN end points. There are two sorts of SA's namely an IKE SA and an IPSec SA. When traffic flow is two way and IPSec needs to establish a connection between peers, an IKE SA is established that illustrates and handles security parameters between both devices. For the same two way traffic, IPSec would create 2 more SA's, one for each communication direction. IPSec SA's relate to the IPSec tunnel and IP packet. They define which security parameter values to use during an IP session. Every IPSec SA contains security parameter values e.g. a unique security parameters index (SPI), a peer destination address, security keys and IPSec protocol. These parameters are used when identifying SA's amongst peer devices.

1.5 Protocols used by IPSec

1.5.1 Message Encryption

Encryption is the process of converting data into secret code. Mathematical algorithms are used to jumble data with a key known to the sender and receiver. The key decipheres the message as well. Message encryption ensures data security.

- **Data Encryption Standard (DES)** supplies a large number of encryption keys. The longer the key, the higher the security level. A 56-bit key is applied to each 64 bits of data. Cipher Block Chaining (CBC) is a means of applying DES and needs an initialization vector (IV) to commence the encryption process. The IV key is fed into the DES encryption algorithm. The 64-bit blocks of plain/clear text is then supplied and converted into cipher text. The peer device uses the same secret key to decipher the message. 56-bit DES-CBC with Explicit IV is supported by Cisco.
- **Triple DES (3DES)** does three separate encryption processes (encrypt, decipher and encrypt) on the message. The resulting 168-bit key (56-bit X 3) enables stronger security. Triple DES is supported by Cisco products.

1.5.2 Message Integrity

Hashing algorithms provide message integrity. The hashing procedure generates a compressed fixed length value, known as a message digest (MD), of the variable length message file. The MD accompanies the

original data when it is sent to the peer device. The peer device does the same hashing algorithm on the original data and compares the two MDs. With IPSec AH, the fixed data of the whole IP datagram are used to generate the MD that gets placed in the Authentication Data field. The variable fields are filled with 0s. The end device copies the MD, zeroes the Authentication Data field and then creates its own MD. With IPSec ESP, the fixed data between the ESP header and trailer of an IP datagram is used to generate the MD that gets placed in the Authentication Data field at the end of the IP datagram. Hashing is not performed on the Authentication Data field by the end device. Message Digest 5 (MD5) and Secure Hash Algorithm-1 (SHA-1) algorithms are supported by IPSec.

Hashed Message Authentication Codes (HMAC) algorithm produces a fixed length secret key that is added to the message digest

- **Message Digest 5 (MD5)** also known as HMAC-MD5 (RFC 1321) was developed by Ronald Rivest of MIT (Massachusetts Institute of Technology) and RSA Data Security Incorporated. HMAC-MD5 uses a 128-bit secret key to produce 128-bit message digest. The 128-bit is shortened to the first 96 bits and stored in the authentication field of the AH or ESP. The destination peer calculates its own 128-bit message digest and compares the first 96 bits to the value stored in the authentication field of the AH or ESP. HMAC-MD5 is weaker than Secure Hash Algorithm-1 but requires less CPU cycles to perform its calculations.
- **Secure Hash Algorithm-1** also known as HMAC-SHA-1 (RFC 2404), was developed by the National Institute of Standards and Technology (NIST). It uses a 160-bit secret key to produce a 160-bit message digest that is shortened to the left most 96-bits and stored in the authentication field of the AH or ESP. The destination peer calculates its own 160-bit message digest and compares the first 96 bits to the value stored in the authentication field.

1.5.3 Peer Authentication

IKE Phase 1 uses a hashing algorithm key with a key type to authenticate peers. The following key types exist:

- With **Preshared Keys**, the pre-agreed on identical key is manually entered into each peer device and is used to authenticate the peers.
- **RSA Digital Signatures** offer more security than preshared keys and requires no manual intervention by in administrator. It was developed in Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. A RSA digital certificates that create a public and a private key is issued by a Certificate Authority (CA). The source creates a digital signature by using the private key, and sends it along with the RSA digital certificate to the destination peer device. The peer uses the digital certificate's public key to validate the digital signature.
- With **RSA Encrypted Nonces**, RSA digital certificates are obtained from a CA and the keys are manually shared at the initialization phase, i.e., no digital certificates are transmitted. This process enables peers to deny message participation.

1.5.4 Key Management

1.5.4.1 Diffie-Hellman Key Agreement (DH)



Diffie-Hellman Key Agreement (DH) provides the means by which two peers can create a shared private key that authenticates data and encrypts an IP datagram. A public and private key is generated by each IPSec peer. The private key is used to sign messages while the public key is used to validate signatures. The public key is a numerical imitation of the private key. The public keys are shared while the private keys never are. Internet Security Association and Key Management Protocol (ISAKMP) are used by IPSec to supply a key exchange facility. ISAKMP uses the IKE Protocol to provide keying matter for SA's. OAKLEY Protocol that portrays a sequence of key exchanges is used by IKE. OAKLEY makes use of DH to create a shared secret key. A peer combines the other peer's public key with his own private key, and calculates the shared secret number that is converted into a shared secret key. Every IPSec peer therefore has a private key, a public key and a shared private key for each IPSec peer relationship it sustains.

1.5.4.2 Certificate Authorities (CAs)

CAs issue and revoke digital certificates and enable one to authenticate these certificates. In addition, they issue Certificate Revocation Lists (CRLs) that indicate to clients which certificates are expired. When a peer receives a certificate, it consults this list.

A client sets up an unsigned certificate and creates a private and public key. The unsigned certificate containing the public key and other information is sent to the CA who calculates a hash code for the certificate request. The digital signature is created when the CA uses its own private key to encrypt the hash code. The encrypted hash is attached to the signed certificate, now known as an Identity Certificate, and is then sent back to the client. When a peer partner receives a digital certificate and wants to authenticate it, it uses the CAs public key to decrypt the signature. The sending peer party encrypts data by using the other peer's public key of the digital certificate. The receiving peer in turn uses its private key to decrypt the data. Customers use their own private keys to sign (create a hash of) a package. The sender's public key is used by the destination peer to create a comparison hash. Signature authentication occurs when the two hash values match

1.6 IPSec Peer Authentication and the Formation of Security Associations

Internet Key Exchange (IKE) Protocol integrates various protocols.

IPSec peers are authenticated in **IKE Phase1**. IKE SAs are agreed on between peers and by using ISAKMP (Security Association and Key Management Protocol), IKE instigates a secure tunnel for IPSec.

Peers use the security tunnel in phase1 to determine security parameters for the IPSec tunnel. This is done in **IKE Phase2**. The IPSec tunnel is created after these security parameters are determined and agreed on.

IKE uses the following five parameters for the VPN 3000 Concentrator Series in IKE Phase1.

- **Encryption algorithm:** 56-bit or 168-bit DES
- **Hash algorithm:** MD5 or SHA-1
- **Authenticated Method:** Preshared Keys, RSA Digital Signatures or RSA Encrypted Nonces
- **Key Exchange:** 768-bit Diffie-Hellman Group 1 or 1024-bit Diffie-Hellman Group 2.
- **IKE SA lifetime:** The default is one day

The following values are needed in IKE Phase2 to establish the IPSec tunnel

- **IPSec protocol:** AH or ESP
- **Hash algorithm:** HMAC-MD5 or HMAC-SHA-1
- **Encryption algorithm** *is only supplied when using ESP:* DES or 3 DES.

When devices need to support an assortment of IPSec VPN's, their IPSec parameters are bundled into predetermined configurations called transforms which distinguishes the hash and encryption algorithm and the IPSec protocol. In this manner, an IPSec transform describe a single IPSec security protocol.

The following are AH Authentication Transforms

- **ah-md5-hmac:** AH coupled with HMAC-MD5 authentication algorithm
- **ah-sha-hmac:** AH coupled with HMAC-SHA-1 authentication algorithm AND
- **ah-rfc1828:** Older version of AH (RFC 1829) with MD-5

The following are ESP Encryption Transforms

- **esp-des:** ESP using 56-bit DES encryption algorithm
- **esp-3des:** ESP using 168-bit DES encryption algorithm
- **esp-rfc1829:** ESP with DES-CBC encryption algorithm. Does not support ESP Authentication Transform
- **Esp-null:** ESP without encryption. Because of its lack of security it should be used in test environments and not a production environment.

The following are ESP Authentication Transforms that can be used with esp-des or esp-3des transform

- **esp-md5-hmac:** ESP with HMAC-MD5 authentication algorithm
- **esp-sha-hmac:** ESP with HMAC-SHA authentication algorithm

A transform set is a grouping of up to 3 individual IPSec transforms that can be supported by an IPSec tunnel.

1.7 Creating VPN's with IPSec

Creating VPN's with IPSec consists of the following 5 steps:

- **STEP 1: Determine interesting traffic:** Interesting traffic initiates the creation of an IPSec tunnel whereby an identical IKE Policy is established at each end of the VNP tunnel.

An IKE policy contains the following fundamentals: A Manual or a certificate authority **Key distribution method** is selected. This determines the **authentication method** to be used. CAs use RSA digital signatures and RSA encrypted nonces while the manual key distribution method makes us of preshared keys. The **IP Address and fully qualified domain name (FQDN)** of the peer hosts is contained in the IKE policy. **IKE policy parameters** contain the key exchange, authentication method, encryption algorithm, hash algorithm and IKE SA lifetime parameters.

VPN security policies determine which traffic is interesting. Security policies are reflected in access lists (ACL). Cisco routers and the PIX Firewall use ACLs to identify the traffic that needs to be secured. ACLs are integrated into a crypto policy. Crypto ACLs must be identical at both ends of the IPsec VPN. When they are un-identical, the packet cannot be processed by the destination peer device. Traffic related with permit statements is encrypted and traffic related with deny statements are not. The two keywords (permit and deny) perform different functions at the source and destination peer devices.

- Permit at source peer: IPsec authenticates data by inserting an AH or ESP header and when applicable, encrypts the packet before it is sent to the destination peer.
 - Deny at source peer: IPsec is not used and the clear text packet is sent to the destination peer
 - Permit at destination peer: The ACL uses the information in the header to determine whether a packet was authenticated by IPsec at the source device, and whether it now needs to be passed through IPsec authentication and decryption processes.
 - Deny at destination peer: Because IPsec authentication was not used on the clear text packet it will not pass through IPsec.
- **STEP 2: IKE Phase 1** authenticates peers and establishes a secure tunnel for IKE SA negotiation. IKE SAs are established in IKE Phase 1. IKE uses **Main Mode** and **Aggressive Mode** to authenticate peers and negotiate an IKE SA policy between these peers.

The following bidirectional exchanges occur during Main Mode

1. Security algorithms and hash methods are negotiated in order to create the IKE SA for each peer.
2. Shared keying material that generates shared secret keys occurs during the DH (Diffie-Hellman) exchange.
3. Peers are verified by their IP addresses

Main Mode protects the identity of the IPsec peers. Cisco VPN products favor Main Mode.

During Aggressive Mode, a single three way message exchange occurs. Aggressive Mode is faster than Main Mode but because most of the information is sent in the initial message it is less secure. At this stage, a secure IPsec tunnel does not exist yet. The initial message contains most of the information namely the IKE SA standards, the sender's DH public key and identity, and a nonce for the peer's signature. The recipient returns the required information together with their public key. The source confirms the exchange.

- **STEP 3: In IKE Phase 2** IPsec SA parameters are determined and the establishment of the secure IPsec tunnel is completed.

IPsec SAs are established in IKE Phase 2. IKE Quick mode happens after the secure tunnel is established in IKE Phase 1 and involves negotiating a shared IPsec policy among peers and establishing IPsec SAs. Quick mode is used to renegotiate IPsec SAs if required. An additional DH key exchange can be done as well.

- **STEP 4: IPsec Data Transfer** enables secure VPN communication. Information can be transmitted via the IPsec session after the IPsec SAs are created. The methods of defining interesting traffic is used and transform sets authenticate and encrypt information.

- **STEP 5: In IPSec Tunnel Termination**, the tunnel is pulled down or an IPSec session is timed out. An IPSec session is terminated when a peer leaves and/or the need for traffic no longer exists. Based on its negotiated SA lifetime, an IKE SA or IPSec SA could timeout. When there is still a need for traffic, IKE Phase 1 must be revisited when an IKE SA timesout. IKE Phase 2 is revisited when an IPSec SA timesout.