brainbuzz.com™
Cramsession

Cramsession™ for Cisco Secure VPN

This study guide will help you to prepare you for the Cisco Secure VPN exam, 9E0-570, which is one in a series of four exams required to achieve the Cisco Security Specialty. Exam topics include building and maintaining Cisco security solutions, which encompass standalone firewall products and IOS software features, IPSEC, and Configuring VPNs on the Cisco Concentrator platform.

Check for the newest version of this Cramsession
http://cramsession.brainbuzz.com/checkversion.asp?V=2452006&FN=cisco/csvpn.pdf

Rate this Cramsession
http://cramsession.brainbuzz.com/cramreviews/reviewCram.asp?cert=Cisco+Secure+VPN

Feedback Forum for this Cramsession/Exam
http://boards.brainbuzz.com/boards/vbt.asp?b=1391

More Cramsession Resources:

Search for Related Jobs
http://jobs.brainbuzz.com/JobSearch.asp?R=&CSRE

CramChallenge - practice questions
http://www.cramsession.com/signup/default.asp#day

IT Resources & Tech Library
http://itresources.brainbuzz.com

Certification & IT Newsletters
http://www.cramsession.com/signup/

SkillDrill - skills assessment
http://skilldrill.brainbuzz.com

Discounts, Freebies & Product Info
http://www.cramsession.com/signup/prodinfo.asp

Contents:

Overview of VPN and IPSec Technologies

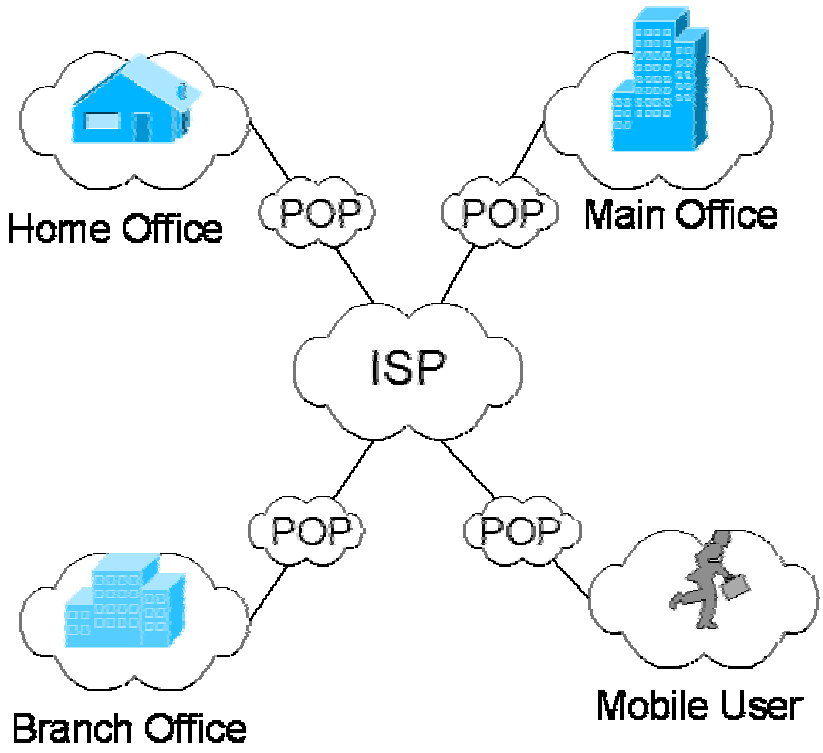
What is a VPN?

Cisco Documentation on VPN

- A VPN is a Virtual Private Network
- Now, as more and more companies need access for remote users, mobile users or remote offices, your current architecture can be augmented with a VPN
- A Virtual Private Network is a network that's created by encryption (Tunneling) across another unsecured medium, like the Internet
- What is great about Cisco and VPN's is that all Cisco devices can be configured as a VPN enabled device solely by the IOS feature set itself. There is a concentrator series, but you can take a PIX or a basic router and "VPN enable it" by configuring the IOS

General VPN Diagram

Here is a general idea of what a VPN solution may look like:



- In any VPN solution, you generally have a Main office or WHQ (World Head Quarters) that everyone comes back to use or get resources
- Here we see that a Mobile user, a branch office, and a home office are all accessing resources in the Main Office via the service provider's network and VPN, Virtual Private Network

Why Use a VPN?

- Well, it is cost effective for one thing. The service provider supplies the brunt of the hardware and support for your new WAN connections
- It can be used as an augmentation to your existing infrastructure. If you have many mobile users, remote offices and remote branches, this may be a technology you can implement

What are some of the other components of a VPN?

- You definitely need to look into security for one, and pay attention to QoS for another. Security is in your hands and is your responsibility; therefore, you must use encryption and configure it. Also, if there are mission critical services, remember… a VPN may not offer you the flexibility of having a specific amount of bandwidth. Usually it is comprised of going over dial up connections that are not very fast
- Cisco VPNs employ outstanding encryption and tunneling support: IPSec, L2TP and GRE, to name a few tunneling standards, and DES and 3DES based encryption technologies

A VPN generally consists of a secure, private tunnel between a remote endpoint and a gateway. (A tunnel is explained below.) The sensitive nature of some communications requires the help of **IPSec** to provide: 1) confidentiality, 2) integrity, and 3) authentication services.

Here is what these three services really do:

Confidentiality

- If something is sent, then the intended party can read it, while at the same time other parties may intercept it but are not be able to read it
- Provided by encryption algorithms such as DES

Integrity

- Is making sure that the data is transmitted from the source to the intended destination without undetected alterations or changes
- Provided by hashing algorithms such as MD5

Authentication

- Is knowing that the data you received is in fact the same as the data that was sent and that the person or sender who claims to have sent it is in fact the actual person or sender
- Provided by mechanisms such as the exchange of digital certificates

VPN Types

Internet VPN

- A private communications channel over the public access Internet

This type of VPN can be divided into:

- Connecting remote offices across the Internet
- Connecting remote-dial users to their home gateway via an ISP (sometimes called a VPDN, Virtual Private Dial Network)

Intranet VPN

- A private communication channel in an enterprise or an organization that may or may not involve traffic going across a WAN
- Remember, an Intranet is a network that is only accessible from within your Internetwork. You can have users dial in for access your to Intranet via a VPN

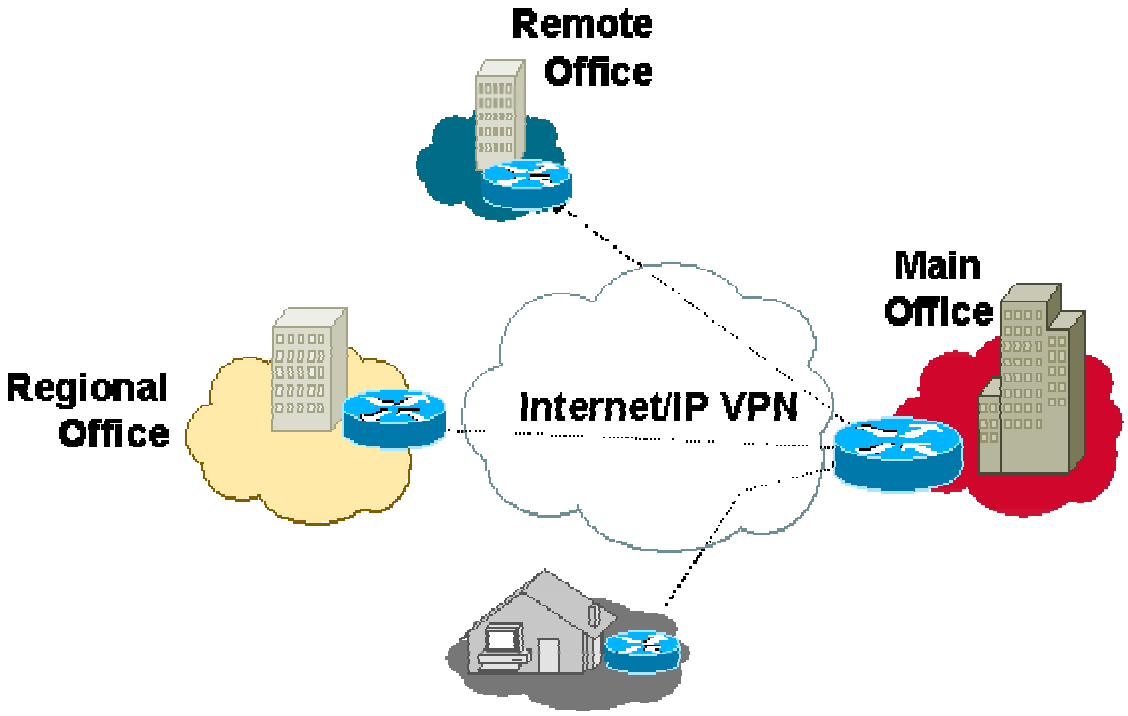
Extranet VPN

- A private communications channel between two or more separate entities that may entail data going across the Internet or some other WAN
- Extranets are used so companies can easily create links with their suppliers and business partners

Remote users

- The Internet provides a low-cost alternative for enabling remote users to access the corporate network
- Rather than maintaining large modem banks and costly phone bills, the enterprise can enable remote users to access the network over the Internet
- With just a local phone call to an Internet service provider, a user can have access to the corporate network

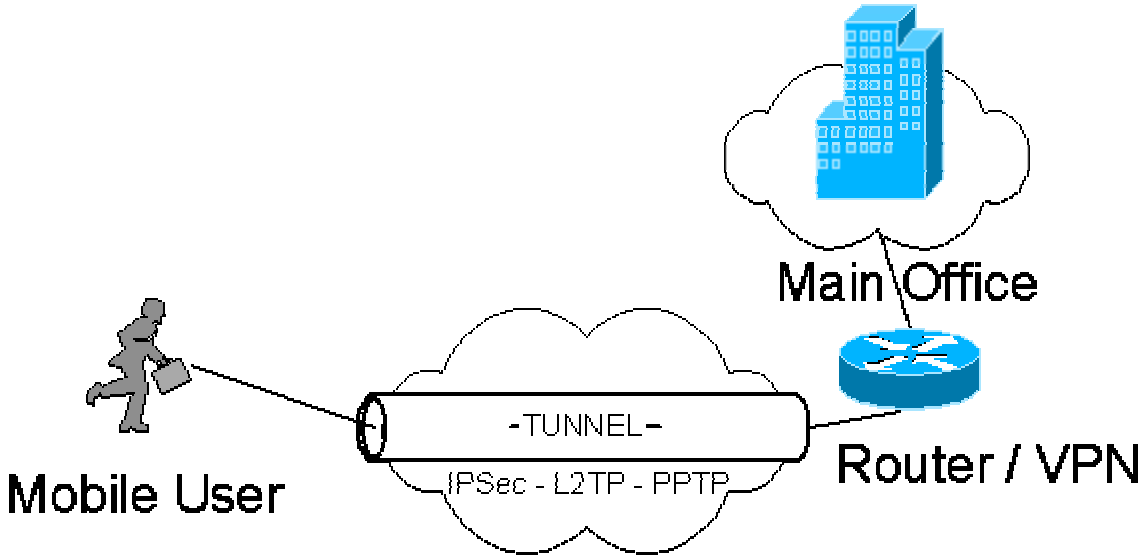
Here is another breakdown of the typical VPN architecture:



What is a Tunnel?

- A Tunnel is type of encryption that makes the connection from one point to the other point secure
- The tunnel is called virtual because it can't be accessed from the rest of the Internet based connection. (Note: It is not technically a tunnel, nor does it resemble a tunnel like depicted below in the diagram, but that is just how it is shown.)

A diagram of a Tunnel may look like this:



What Is IPSec?

All Configuration based commands and details can be found here:

IPSec Network Security Commands

Step by step tutorial from Cisco on how to configure IPSec

Intel White paper on IPSec

Microsoft on IPSec implementation

IPSec or IP (Internet Protocol Security)

- IP Security (IPSec) is a standards based Protocol that provides privacy, integrity, and authenticity to data that is transferred across a network
- A Major problem today is that the Internet has a major lack of security (it wasn't designed to have a lot of security) and more and more people are using it each and every day both for private use and business use – this poses a major problem and a major threat
- The Internet is subject to many attacks that include:
    - Loss of privacy
    - Loss of data integrity
    - Identity spoofing

- Denial-of-service

(Each of these is described below in the “Why Do We Need IPSec?” section.)

- The goal of IPSec is to address all of these threats without the requirement of expensive host or application modifications and changes
- Before IPSec, networks were forced to deploy partial solutions that addressed only a portion of the problem. An example is SSL, which only provides application encryption for Web browsers and other applications. SSL protects the confidentiality of data sent from each application that uses it, but it does not protect data sent from other applications. Every system and application must be protected with SSL in order for it to work efficiently – this does not equal a total solution, only a partial one or one that can be easily fumbled
- IPSec has been mandated in IP Version 6 (IPv6 has IPSec), and if everyone implemented Version 6, then IPSec would be commonplace
- Remember, IPSec is a network and transport level encryption (unlike SSL)
- SSL or Secure Sockets Layer is application level or Web Browser Client based encryption
- IPSec provides IP network-layer encryption. The standards define several new packet formats:
  - The authentication header (AH) to provide data integrity
  - The encapsulating security payload (ESP) to provide confidentiality and data integrity
- IPSec combines several different security technologies into a complete system to provide confidentiality, integrity, and authenticity
- In particular, IPSec uses:
  - Diffie-Hellman key exchange for deriving key material between peers on a public network
  - Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks
  - Bulk encryption algorithms, such as DES, for encrypting the data
  - Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as MD5 or SHA for providing packet authentication
  - Digital certificates, signed by a certificate authority, to act as digital ID cards

Why Do We Need IPSec?

Loss of Privacy

- A perpetrator may be able to observe confidential data as it traverses the Internet
- This ability is probably the largest inhibitor of business-to-business communications today. Without encryption, every message sent may be read by an unauthorized party

Loss of Data Integrity

- Even for data that is not confidential, one must still take measures to ensure data integrity
- For example, you may not care if anyone sees your routine business transaction, but you would certainly care if the transaction were modified

Identity Spoofing

- Moving beyond the protection of data itself, you must also be careful to protect your identity on the Internet
- Many security systems today rely on IP addresses to uniquely identify users

Denial-of-service

- As organizations take advantage of the Internet, they must take measures to ensure that their systems are available
- Over the last several years attackers have found deficiencies in the TCP/IP protocol suite that allows them to arbitrarily cause computer systems to crash

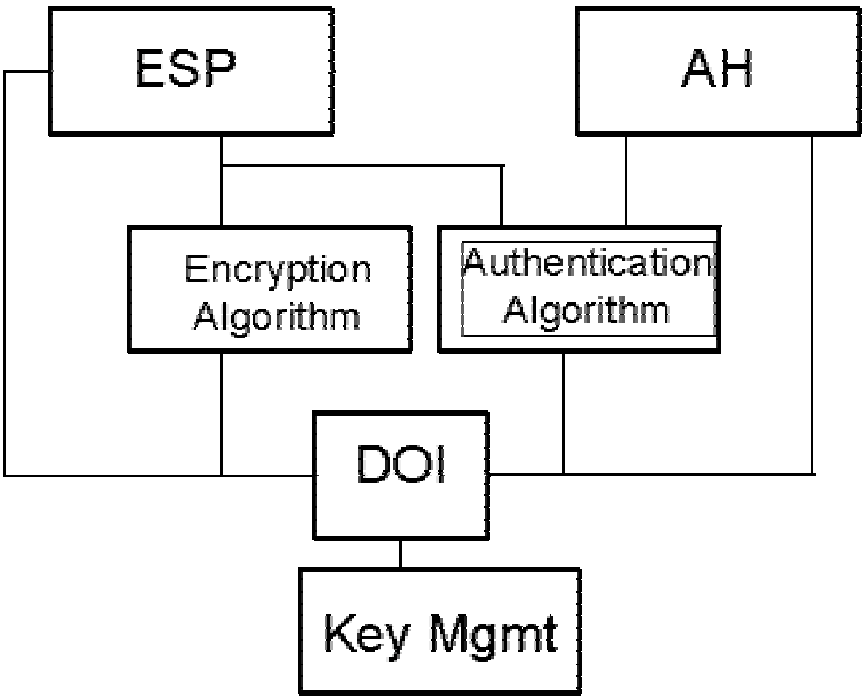
Cisco leveraged IPSec Benefits

- IPSec is a key technology component of Cisco's end-to-end network service offerings. Working with its partners in the Enterprise Security Alliance, Cisco ensures that IPSec is available for deployment wherever its customers need it. Cisco and its partners offer IPSec across a wide range of platforms that includes:
    - Cisco IOS software
    - Cisco PIX Firewall
    - Windows 9x, Windows NT4, and Windows 2000

- Cisco is working closely with the IETF to ensure that IPSec is quickly standardized and is available on all other platforms
- Customers who use Cisco's IPSec will be able to secure their network infrastructure without costly changes to every computer. Customers who deploy IPSec in their network applications gain privacy, integrity, and authenticity controls without affecting individual users or applications. Application modifications are not required, so there is no need to deploy and coordinate security on a per-application, per-computer basis
- IPSec provides an excellent remote user solution. Remote workers can use an IPSec client on their PC in combination with the Layer 2 Tunneling Protocol (L2TP) to connect back to the enterprise network. The cost of remote access is decreased dramatically, and the security of the connection actually improves over that of dialup lines

IPSec Architecture

This is a General Diagram of all the IPSec architecture components, each described below. The two main functions you need to know well are the ESP and AH for the exam. They appear at the top of the following diagram.



IPSec Packets

- IPSec defines a new set of headers that are added to IP Datagrams
- These new headers are placed after the IP header and before the Layer 4 protocol (TCP or UDP)

Authentication header (AH)

- This header will ensure the integrity and authenticity of the data when it is added to the datagram
- It **does not** provide confidentiality protection
- AH uses a keyed hash function rather than digital signatures and this is because digital signature technology is way too slow and would reduce network throughput
- AH is also embedded in the data for protection purposes

Encapsulating security payload (ESP)

- This header protects the confidentiality, integrity, and authenticity of the data when added to the datagram
- AH and ESP can be used independently or together, although for most applications just one of them is sufficient
- For both of these protocols, IPSec does not define the specific security algorithms to use, but rather provides an open framework for implementing industry standard algorithms
- ESP **encapsulates** the data to be protected

Note: Ensure that, when configuring your access lists, protocol 50 and 51 as well as UDP port 500 traffic is not blocked at interfaces used by IPSec. Otherwise, you may have a problem

IPSec provides two modes of operation

Transport Mode

- An encapsulation mode for AH and ESP
- When using transport mode only the payload is encrypted and that means that the original IP headers are left fully intact

- The advantage of Transport mode is that it only adds a few bytes to each packet
- This mode also allows devices on the public network to view the source and destination of each packet
- The disadvantage of Transport mode is that passing the IP header in the clear allows an attacker to capture the packet and perform some traffic analysis

Source	Destination	**Encrypted Data**

Tunnel Mode

- With tunnel mode the **entire** IP datagram is encrypted and it then becomes the **payload** in a newly constructed IP packet
- Tunnel mode also allows a router to act as an IPSec proxy, which means that the router performs encryption on behalf of the hosts
- A great advantage is that the source and the destination addresses **are not** visible while encrypted
- **Remember: Tunnel Mode is used to protect Datagrams sourced from or destined to non-IPSec systems**

Tunnel Source	Tunnel Destination	**Encrypted Source**	**Encrypted Dest**	**Encrypted Data**

For excellent diagrams, explanations and more information on the IPSec Packet structure for Transport and Tunnel mode visit the AT&T IPSec Link below:

AT&T IPSec Information

Cryptology Basics

Advantages and Disadvantages

Type	Advantages	Disadvantages
Public Key	Usage of two different keys Pretty easy to distribute keys Uses digital signatures to provide integrity	Does not support digital signatures Slow
Symmetric	Very fast Can be implemented in hardware very easily	Uses two of the same key Not easy to distribute keys

Certification Authority (CA)

- A certificate authority is the authority in a network that issues and manages security credentials and public keys for message encryption
- As part of a public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate so if the RA verifies the requestor's information, the CA can then issue a certificate
- Depending on the public key infrastructure implementation, the certificate includes the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner

Message Digest 5 (MD5)

- MD5 is a one-way hashing algorithm that produces a 128-bit hash. Cisco uses hashes for authentication for IPSec
- Remember that SHA is more secure than MD4 and MD5

VeriSign, Inc.

- VeriSign
- VeriSign is the leading provider of digital certificate solutions for extranets and intranets, including IPSec

Common Algorithms

DES	Data Encryption Standard Uses 56 bit key
3DES	Encrypts a block 3 times with 3 different keys
RSA	Rivest, Shamir, and Adelman Common key is 512 bits
Diffie-Hellman	Very old Does not support Digital Signatures and encryption

Note: Remember these basic facts

Command reference for IPSec, IKE and CA

If you need to configure any of these technologies, use this command reference on the Cisco web site for all your needs:

Command Reference

Cisco VPN 3000 Concentrator Overview

Cisco VPN 3000 Concentrator

Cisco Documentation

Note: This used to be an Altiga product until Cisco bought it

What is the Concentrator?

- The VPN 3000 Concentrator Series is a remote access VPN platform and client software solution that incorporates very high availability, high performance and scalability with encryption and authentication

- It is unique in that it can offer field swappable components called Scalable Encryption Processing or SEP modules. It is also customer upgradeable
- The specialized SEP modules perform hardware based acceleration
- Only the VPN **3080** Concentrator is available in a fully redundant configuration at this time
- Special features:
    - Broadband performance
    - Scalable encryption
    - Redundant, hot swap SEPs with stateful SEP failover
    - Stateless chassis failover (VRRP)
    - Redundant power supplies
    - Full instrumentation

Configurations guide for the 3000 series

Configuration	Events
Interfaces	General
System Configuration	User Management
Servers	Policy Management
Address Management	Administration
Tunneling Protocols	Monitoring
IP Routing	Using the Command Line Interface
Management Protocols	Errors and troubleshooting

Note: All information on the concentrator can be found within these links

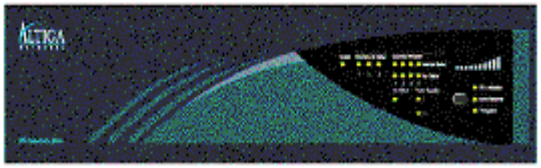
Although this is not on the exam, you may find this link VERY helpful if you are implementing a VPN solution with the 3000 and Microsoft Technologies

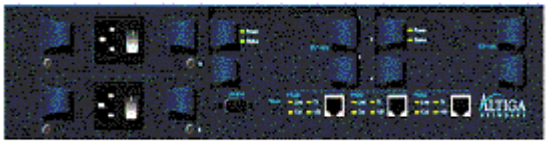
How to Configure the VPN 3000 Concentrator with Microsoft Certificates

Click Here

3000 Concentrator Shots:

Front and back views





For all Concentrator based information

Concentrator Documentation

Client based Documentation

Other Cisco VPN Products and Solutions

- Cisco provides a suite of VPN-optimized routers that run the range of VPN applications from telecommuter applications with the Cisco 800 for ISDN access to remote office connectivity with the Cisco 1700, 2600, and 3600 to head-end connectivity with the Cisco 7200 & 7500
- Furthermore, Cisco product breadth extends into the new world of broadband telecommuter and small office VPN connectivity with the Cisco UBr900 cable access router/modem and the Cisco 1400 DSL router/modem. Providing DSL and cable solutions is unique in the VPN market
- The Cisco 7100 Series VPN Router is an “integrated VPN router” that provides solutions for VPN-centric environments. VPN-optimized routers provide VPN solutions for hybrid VPN environments where modularity, port density, and flexibility is required for private WAN aggregation and other classic WAN applications
- The Cisco 7100 provides solutions for VPN-centric environments where WAN density requirements are lower as only one or two connections to the VPN cloud are required for VPN connectivity. I/O of the 7100 is focused for this

single or dual homing WAN configurations and it provides high performance for robust VPN services throughput

- You can also look at the 5000 series concentrator, but it is not listed on the testable objectives at this time

Cisco VPN 3000 Concentrator Configurations Guide

Configurations

You can use the below links and guides to look at all the different configurations that you can apply in your design. Look at each link and make sure that you are comfortable with all the configurations listed below.

Advanced Configurations:

- Cisco VPN 3000 Concentrator - Blocking with Filters and RADIUS Filter Assignment
- Cisco VPN 3000 Concentrator Series Group Lock Feature
- How to Configure the Cisco VPN 3000 Client to VPN 3000 Concentrator with Microsoft Windows NT Domain Authentication
- VPN 3000 Client to Concentrator with IPSec SDI Authentication
- How to Configure the VPN 3000 Concentrator with Microsoft Certificates
- Cisco VPN 3000 Concentrator to Cisco IOS
- Cisco VPN 3000 Concentrator to PIX Firewall
- How to Configure the Cisco VPN 3000 Concentrator with MS RADIUS
- Configuring the Cisco VPN 3000 Concentrator and the Network Associates PGP Client
- How to Configure IPSec Clients to Authenticate to and Receive Addresses from a Funk RADIUS Server

Advanced Encryption Configurations:

- Configuring and Troubleshooting Cisco's Proprietary Network-Layer Encryption (Part I)
- Configuring and Troubleshooting Cisco's Proprietary Network-Layer Encryption (Part II): IPSec and ISAKMP
- GRE and IPSec with IPX Routing
- IPSec Between Three Routers Using Private Addresses
- IPSec - Cisco Secure VPN Client to Central Router Controlling Access
- IPSec Between Cisco Secure PIX Firewall 5.1 and a VPN Client with Extended Authentication
- IPSec/GRE with NAT
- IPSec Manual Keying

- IPSec Over Cable Sample Configurations and Debugs
- IPSec Router-to-PIX Configuration: Using the **nat 0 access-list** Command
- IPSec Router-to-Router Fully Meshed
- IPSec Router-to-Router Hub and Spoke
- IPSec Router-to-Router, Pre-shared, NAT Overload Between a Private and a Public Network
- IPSec Router-to-Router, Pre-shared, NAT Overload Between Private Networks
- IPSec Router-to-Router with NAT Overload and Cisco Secure VPN Client
- IPSec: Simple PIX-to-PIX VPN Configuration
- IPSec Tunnel - Cisco Router to Checkpoint Firewall 4.1
- IPSec Tunnel Through Firewall with NAT
- IPSec - Wild-card Pre-shared Keys with Cisco Secure VPN Client and No-mode Config
- IPSec with Routing Protocols Using GRE Tunneling
- IP Security Tunnel End-point Discovery
- L2TP Over IPSec
- PIX-to-VPN Client Wild-card, Pre-shared, No Mode Configuration
- Router IPSec Tunnel Private-to-Private Network with NAT and a Static
- Router Mode Configuration
- Router-to-Router - Dynamic to Static IPSec with NAT
- Router to VPN Client, Mode-config, Wild-card Pre-shared Key with NAT

Crypto Maps

Crypto map

A Cisco IOS software configuration tool that performs specific functions:

- It selects data flows that need security processing
- It defines the policy for these flows and the crypto peer that traffic needs to go to
- A crypto map is applied to an interface
- The concepts of the crypto map was introduced in classic crypto but expanded for IPSec

Creating Crypto Maps

- To configure a router for encryption, a "crypto map" must be defined
- This crypto map specifies the access list to be used to define the traffic to encrypt, the algorithm that will be used in encrypting data, and the peer with whom the router will exchange this data
- Extended IP access lists describe the traffic that will be encrypted; the inverse of this access list is used to decrypt

- IP encryption is supported, and users can tunnel other protocols inside of IP and encrypt the encapsulating IP packets and payload
- This procedure can be done using the keyword **GRE** in access-list entries
- The algorithm specified in this map must be running on the router in order to use it, so if the map specifies "**40-bit-des cfb-64**," the global command "**algorithm 40-bit-des cfb-64**" must be in the configuration in order to encrypt data
- By default, the 56-bit image runs **56-bit-DES CFB-64**, and the 40-bit image runs **40-bit-DES CFB-64**
- As with any route map configurations, crypto maps have to be carefully written before applying them to the interface in order to verify what will be encrypted
- Console access is recommended for application of the map

Command reference

Crypto key generate rsa	Generate a RSA key pair
Crypto ca certificate query	Enables query more / causes certificates and CRL (Certificate Revocation List) to be stored locally
Crypto ca identity	Declare a ca
Enrollment url	Specifies the url of the ca
Enrollment mode ra	Specified that the ca system provides a registration authority
Crl optional	Even if the appropriate CRL is not accessible, other peer certificates can still be accepted
Exit	This will exit ca/identity config mode
Crypto ca authenticate	Get the ca public key
Crypto ca enroll	Requests certificates for all the RSA key pairs
Crypto ca Crl request	Requests an updated CRL

Reference for Maps

Crypto map	Apply a crypto map set to the interface
Crypto dynamic-map	Create a dynamic map entry

Set transform-set	Specify which transform sets are allowed for the map entry
Match address	Name an extended access list to use (optional)
Set peer	Specifies a remote IPSec peer
Set pfs	Specify that IPSec should ask for perfect forward secrecy