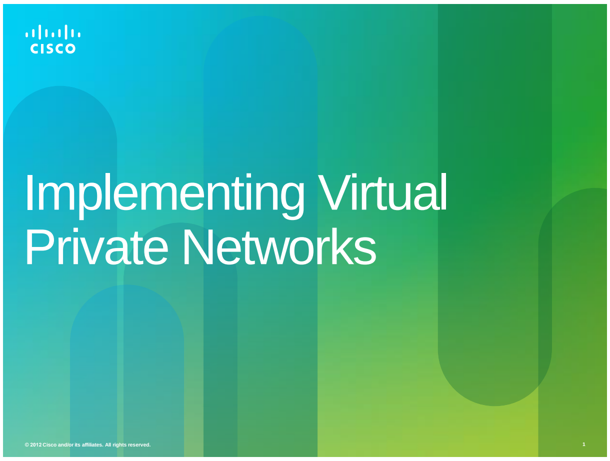
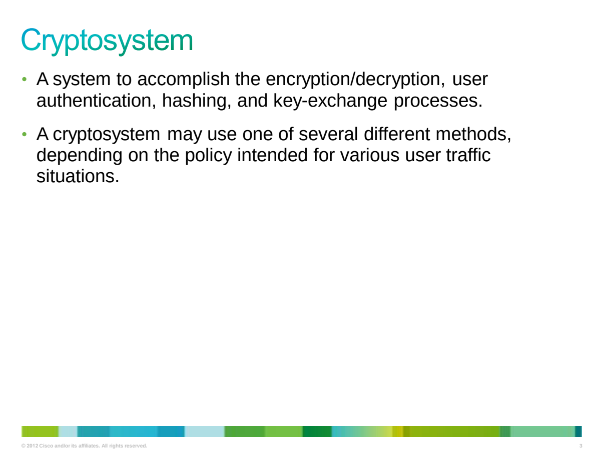


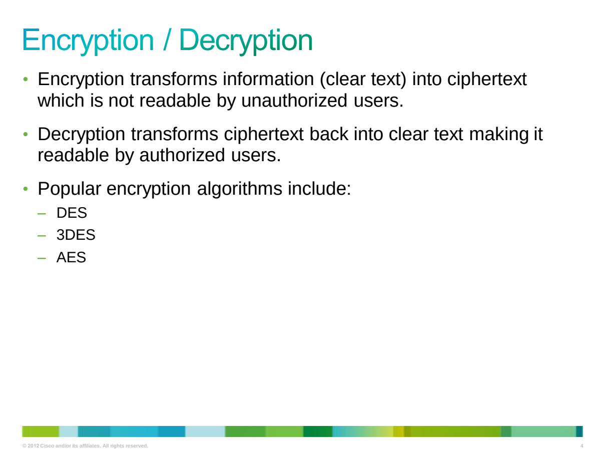
Implementing Virtual Private Networks

VPN Terminology



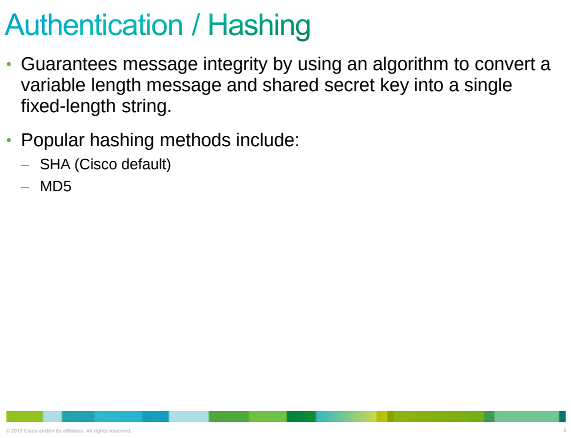
Cryptosystem

- A system to accomplish the encryption/decryption, user authentication, hashing, and key-exchange processes.
- A cryptosystem may use one of several different methods, depending on the policy intended for various user traffic situations.



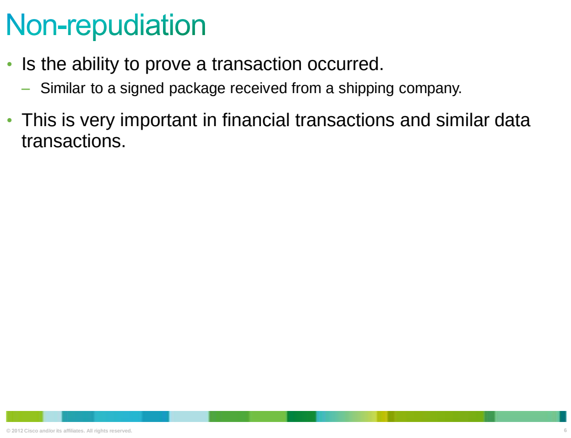
Encryption / Decryption

- Encryption transforms information (clear text) into ciphertext which is not readable by unauthorized users.
- Decryption transforms ciphertext back into clear text making it readable by authorized users.
- Popular encryption algorithms include:
  - DES
  - 3DES
  - AES



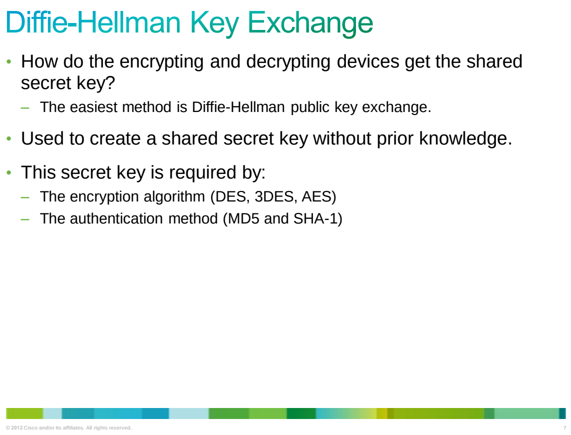
Authentication / Hashing

- Guarantees message integrity by using an algorithm to convert a variable length message and shared secret key into a single fixed-length string.
- Popular hashing methods include:
  - SHA (Cisco default)
  - MD5



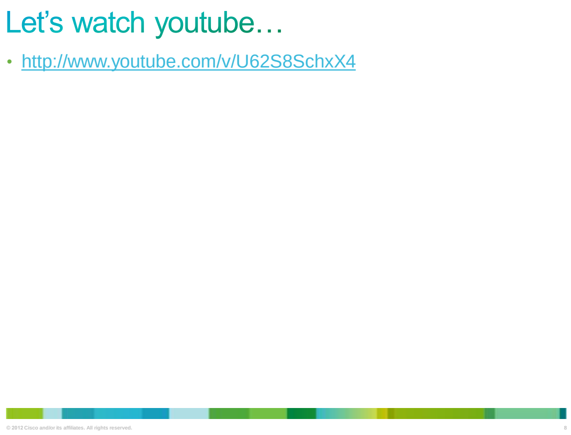
Non-repudiation

- Is the ability to prove a transaction occurred.
  - Similar to a signed package received from a shipping company.
- This is very important in financial transactions and similar data transactions.



Diffie-Hellman Key Exchange

- How do the encrypting and decrypting devices get the shared secret key?
  - The easiest method is Diffie-Hellman public key exchange.
- Used to create a shared secret key without prior knowledge.
- This secret key is required by:
  - The encryption algorithm (DES, 3DES, AES)
  - The authentication method (MD5 and SHA-1)



Let's watch youtube…

- http://www.youtube.com/v/U62S8SchxX4

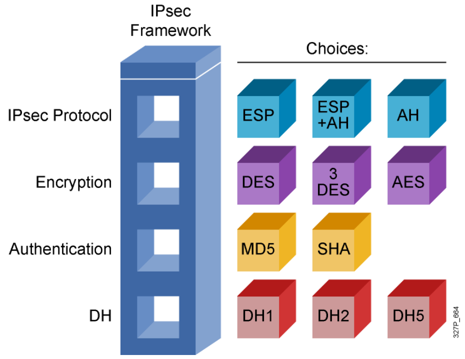
Pre-Shared Key

- Identifies a communicating party during a phase 1 IKE negotiation.
- The key must be pre-shared with another party before the peers routers can communicate.

IPsec - Internet Protocol Security

- A “framework” of open standards developed by the IETF to create a secure tunnel at the network (IP) layer.
  - It spells out the rules for secure communications.
- IPsec is not bound to any specific encryption or authentication algorithms, keying technology, or security algorithms.

IPsec Protocol Framework

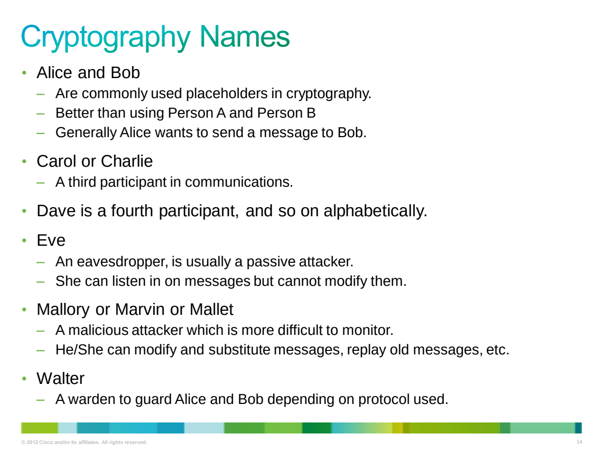


Crypto Map

- A Cisco IOS software configuration entity that performs two primary functions.
  - First, it selects data flows that need security processing.
  - Second, 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.

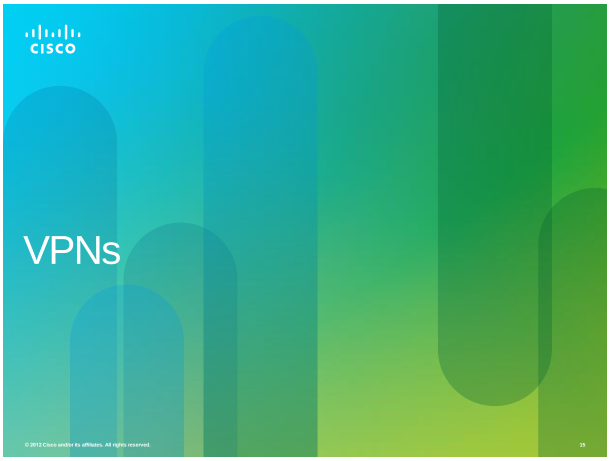
SA - Security Association

- Is a contract between two parties indicating what security parameters, such as keys and algorithms will be used.
- A Security Parameter Index (SPI) identifies each established SA.

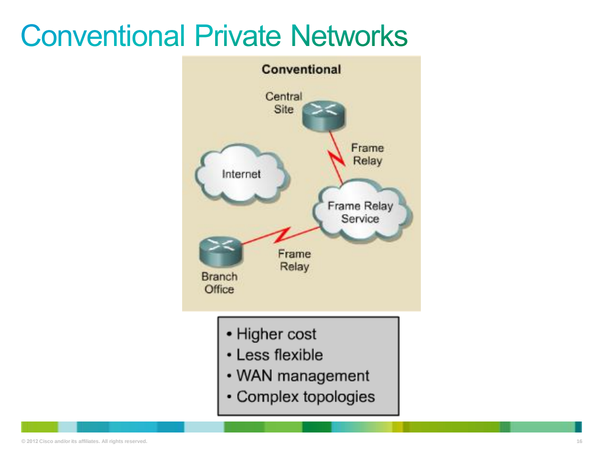


Cryptography Names

- Alice and Bob
  - Are commonly used placeholders in cryptography.
  - Better than using Person A and Person B
  - Generally Alice wants to send a message to Bob.
- Carol or Charlie
  - A third participant in communications.
- Dave is a fourth participant, and so on alphabetically.
- Eve
  - An eavesdropper, is usually a passive attacker.
  - She can listen in on messages but cannot modify them.
- Mallory or Marvin or Mallet
  - A malicious attacker which is more difficult to monitor.
  - He/She can modify and substitute messages, replay old messages, etc.
- Walter
  - A warden to guard Alice and Bob depending on protocol used.



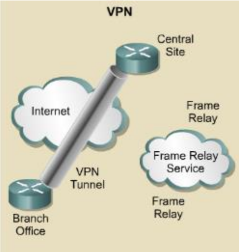
VPNs



Conventional Private Networks

- Higher cost
- Less flexible
- WAN management
- Complex topologies

Virtual Private Networks



- Lower cost
- More flexible
- Simpler management
- Tunnel topology

VPNs

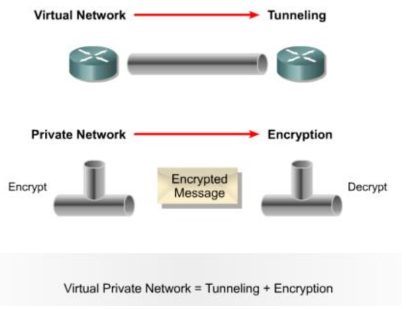
- A Virtual Private Network (VPN) provides the same network connectivity for remote users over a public infrastructure as they would have over a private network.
- VPN services for network connectivity include:
  - Authentication
  - Data integrity
  - Confidentiality

Characteristics of VPNs

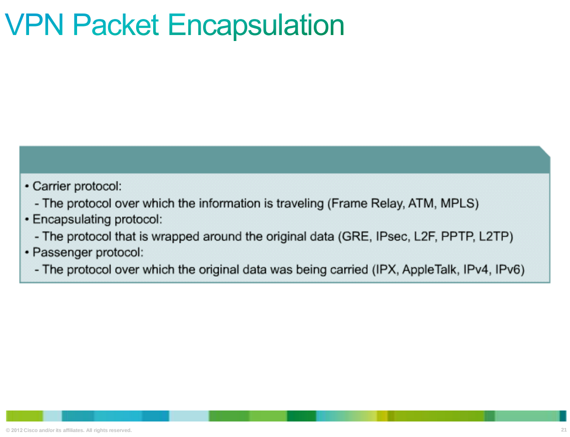
Characteristic	Purpose
Authentication	Ensures that only authorized senders and devices enter the network
Data confidentiality	Protects data from eavesdroppers (spoofing)
Data integrity	Guarantees that no tampering or alterations occur

VPN Concepts

- A secure VPN is a combination of concepts:

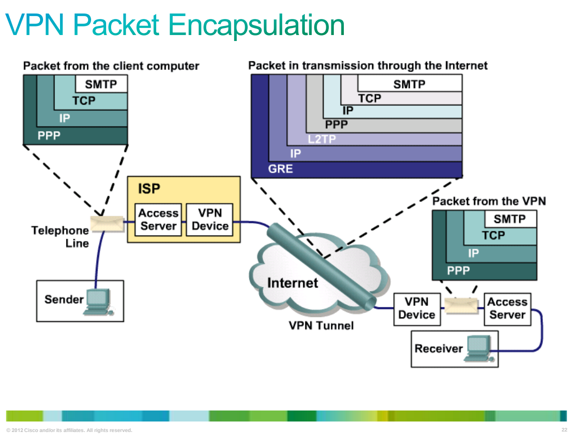


Virtual Private Network = Tunneling + Encryption



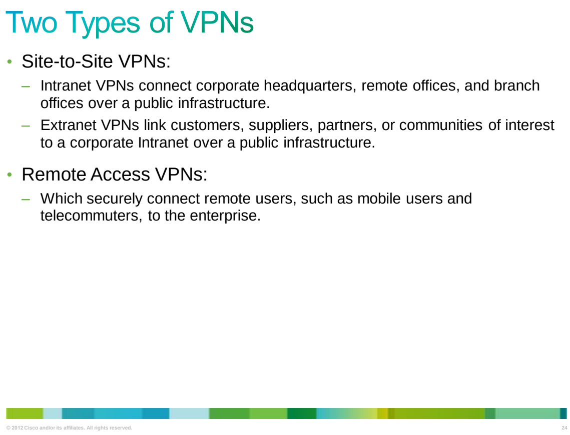
VPN Packet Encapsulation

- Carrier protocol:
  - The protocol over which the information is traveling (Frame Relay, ATM, MPLS)
- Encapsulating protocol:
  - The protocol that is wrapped around the original data (GRE, IPsec, L2F, PPTP, L2TP)
- Passenger protocol:
  - The protocol over which the original data was being carried (IPX, AppleTalk, IPv4, IPv6)



VPN Packet Encapsulation

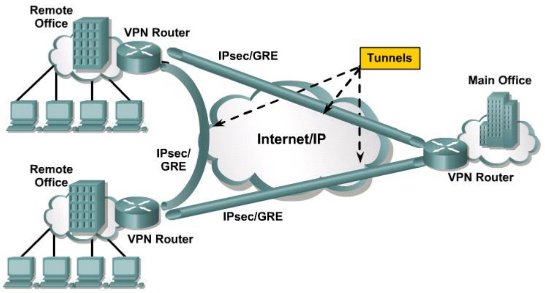
VPN Topologies



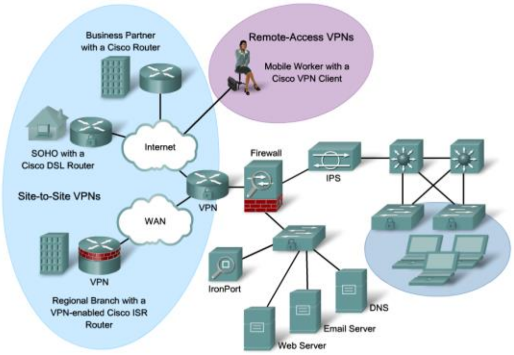
Two Types of VPNs

- Site-to-Site VPNs:
  - Intranet VPNs connect corporate headquarters, remote offices, and branch offices over a public infrastructure.
  - Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate Intranet over a public infrastructure.
- Remote Access VPNs:
  - Which securely connect remote users, such as mobile users and telecommuters, to the enterprise.

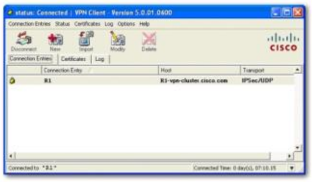
Site-to-Site VPNs



Remote Access VPNs


Business Partner with a Cisco Router
Remote-Access VPNs
Mobile Worker with a Cisco VPN Client
SOHO with a Cisco DSL Router
Internet
Firewall
IPS
Site-to-Site VPNs
VPN
WAN
VPN
Regional Branch with a VPN-enabled Cisco ISR Router
IronPort
DNS
Email Server
Web Server

Remote Access VPNs

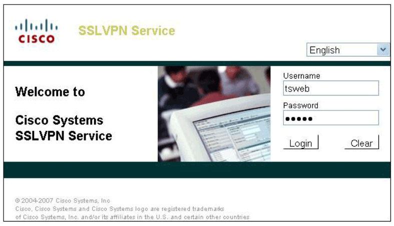


	Connection Entry	Host	Transport
	R1	R1-vpn-cluster.cisco.com	IPSec/UDP

Connected to "R1"

Connected Time: 0 day(s), 07:10.15

Remote Access VPNs



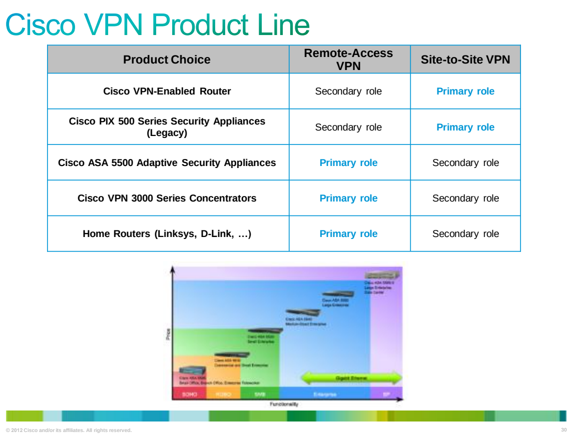
Welcome to

Cisco Systems SSLVPN Service

Username: tsweb

Password: •••••

© 2004-2007 Cisco Systems, Inc
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks
of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries



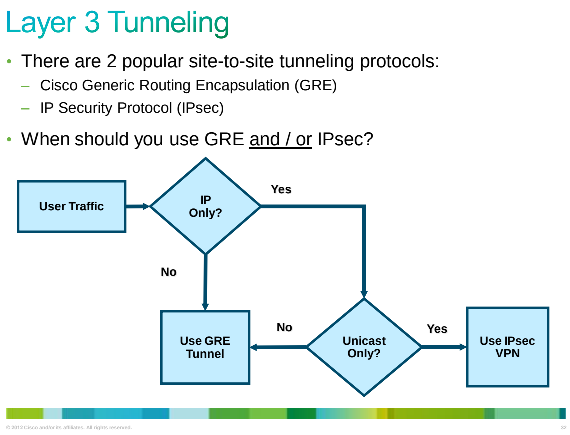
Cisco VPN Product Line

Product Choice	Remote-Access VPN	Site-to-Site VPN
Cisco VPN-Enabled Router	Secondary role	Primary role
Cisco PIX 500 Series Security Appliances (Legacy)	Secondary role	Primary role
Cisco ASA 5500 Adaptive Security Appliances	Primary role	Secondary role
Cisco VPN 3000 Series Concentrators	Primary role	Secondary role
Home Routers (Linksys, D-Link, …)	Primary role	Secondary role

30

GRE Tunnel

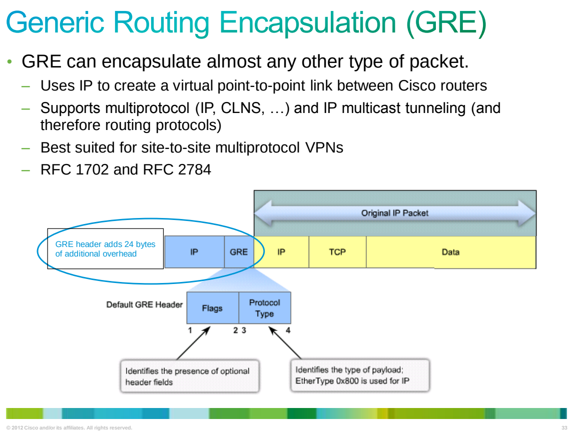
31



Layer 3 Tunneling

- There are 2 popular site-to-site tunneling protocols:
  - Cisco Generic Routing Encapsulation (GRE)
  - IP Security Protocol (IPsec)
- When should you use GRE <u>and / or</u> IPsec?

32



Generic Routing Encapsulation (GRE)

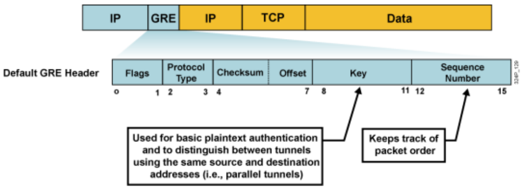
- GRE can encapsulate almost any other type of packet.
  - Uses IP to create a virtual point-to-point link between Cisco routers
  - Supports multiprotocol (IP, CLNS, …) and IP multicast tunneling (and therefore routing protocols)
  - Best suited for site-to-site multiprotocol VPNs
  - RFC 1702 and RFC 2784

Original IP Packet
GRE header adds 24 bytes of additional overhead
IP
GRE
IP
TCP
Data
Default GRE Header
Flags
Protocol Type
1
2 3
4
Identifies the presence of optional header fields
Identifies the type of payload; EtherType 0x800 is used for IP

33

Optional GRE Extensions

- GRE can optionally contain any one or more of these fields:
  - Tunnel checksum
  - Tunnel key
  - Tunnel packet sequence number
- GRE keepalives can be used to track tunnel path status.



Used for basic plaintext authentication and to distinguish between tunnels using the same source and destination addresses (i.e., parallel tunnels)

Keeps track of packet order

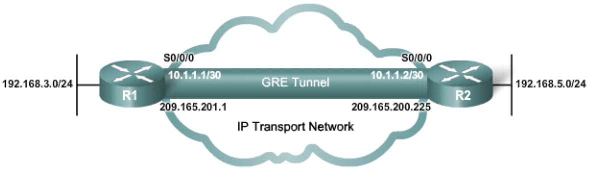
Generic Routing Encapsulation (GRE)

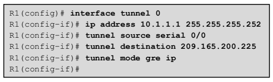
- GRE does not provide encryption!
  - It can be monitored with a protocol analyzer.
- However, GRE and IPsec can be used together.
- IPsec does not support multicast / broadcast and therefore does not forward routing protocol packets.
  - However IPsec can encapsulate a GRE packet that encapsulates routing traffic (GRE over IPsec).

Five Steps to Configuring a GRE Tunnel

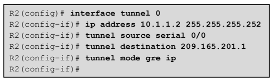
1. Create a tunnel interface: **`interface tunnel 0`**
2. Assign the tunnel an IP address.
3. Identify the source tunnel interface: **`tunnel source`**
4. Identify the tunnel destination: **`tunnel destination`**
5. (Optional) Identify the protocol to encapsulate in the GRE tunnel: **`tunnel mode gre ip`**
   - By default, GRE is tunneled in an IP packet.

Five Steps to Configuring a GRE Tunnel

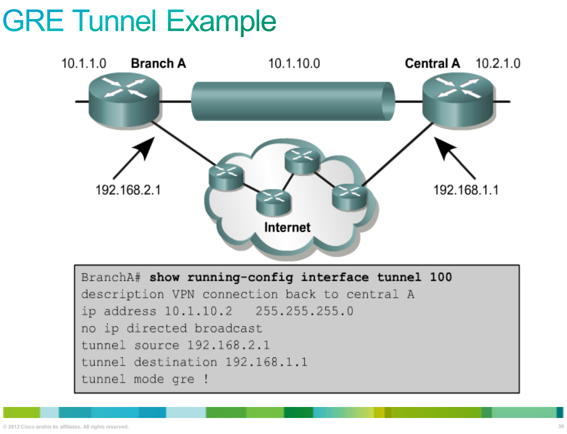




```
R1(config)# interface tunnel 0
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# tunnel source serial 0/0
R1(config-if)# tunnel destination 209.165.200.225
R1(config-if)# tunnel mode gre ip
R1(config-if)#
```



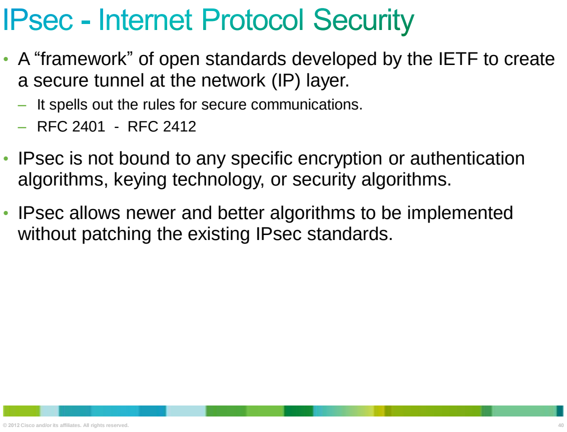
```
R2(config)# interface tunnel 0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
R2(config-if)# tunnel source serial 0/0
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# tunnel mode gre ip
R2(config-if)#
```



GRE Tunnel Example

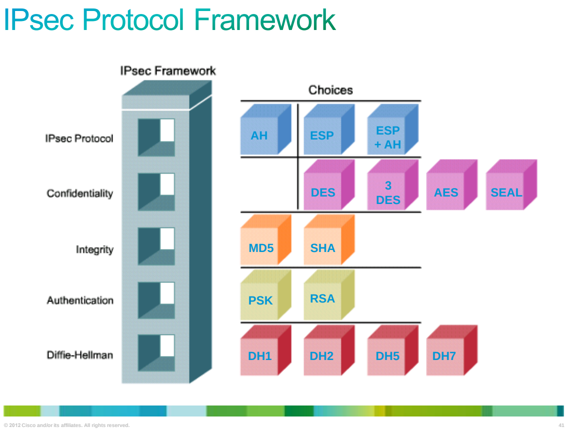
```
BranchA# show running-config interface tunnel 100
description VPN connection back to central A
ip address 10.1.10.2   255.255.255.0
no ip directed broadcast
tunnel source 192.168.2.1
tunnel destination 192.168.1.1
tunnel mode gre !
```

IPsec



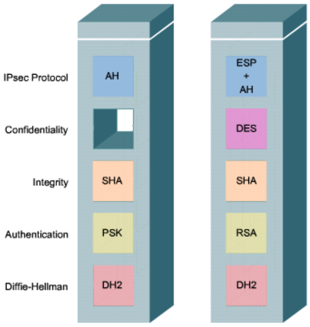
IPsec - Internet Protocol Security

- A “framework” of open standards developed by the IETF to create a secure tunnel at the network (IP) layer.
  - It spells out the rules for secure communications.
  - RFC 2401 - RFC 2412
- IPsec is not bound to any specific encryption or authentication algorithms, keying technology, or security algorithms.
- IPsec allows newer and better algorithms to be implemented without patching the existing IPsec standards.



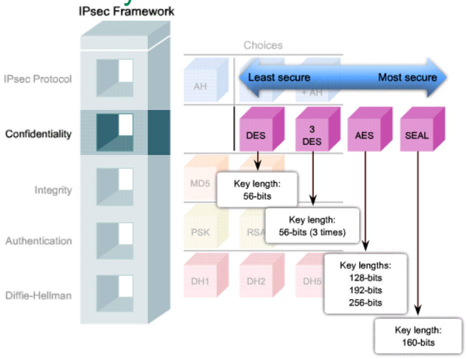
IPsec Protocol Framework

IPsec Protocol Framework



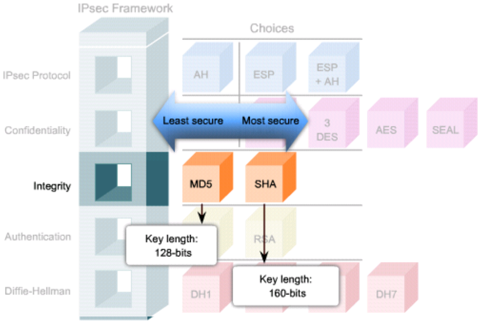
42

Confidentiality



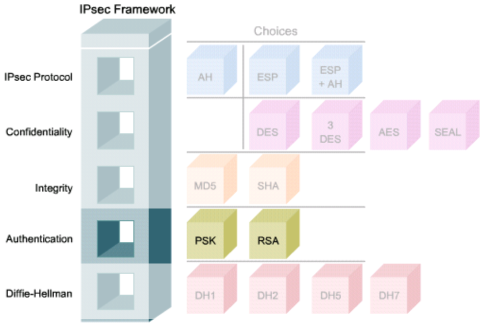
43

Integrity



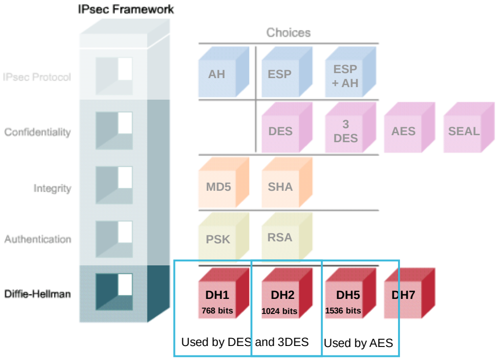
44

Authentication



45

Secure Key Exchange



Used by DES and 3DES

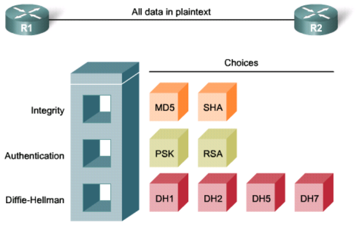
Used by AES

IPsec Framework Protocols

- IPsec uses two main protocols to create a security framework:
  - AH: Authentication Header
  - ESP: Encapsulating Security Payload

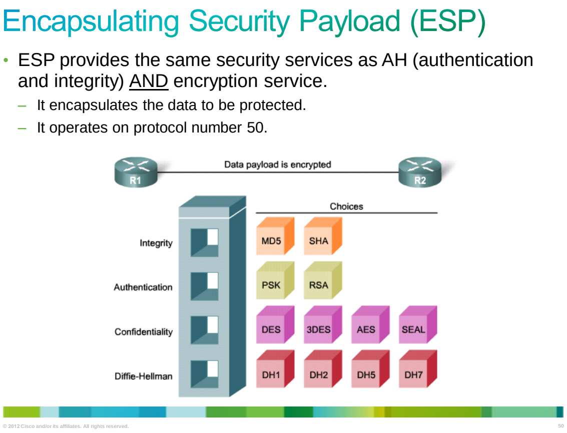
Authentication Header (AH)

- AH provides authentication and optional replay-detection services.
  - It authenticates the sender of the data.
  - AH operates on protocol number 51.
  - AH supports the HMAC-MD5 and HMAC-SHA-1 algorithms.



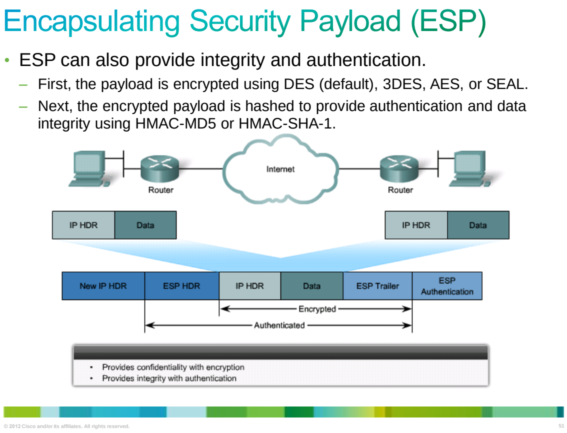
Authentication Header (AH)

- AH does not provide confidentiality (encryption).
  - It is appropriate to use when confidentiality is not required or permitted.
  - All text is transported unencrypted.
- It only ensures the origin of the data and verifies that the data has not been modified during transit.
- If the AH protocol is used alone, it provides weak protection.
- AH can have problems if the environment uses NAT.



Encapsulating Security Payload (ESP)

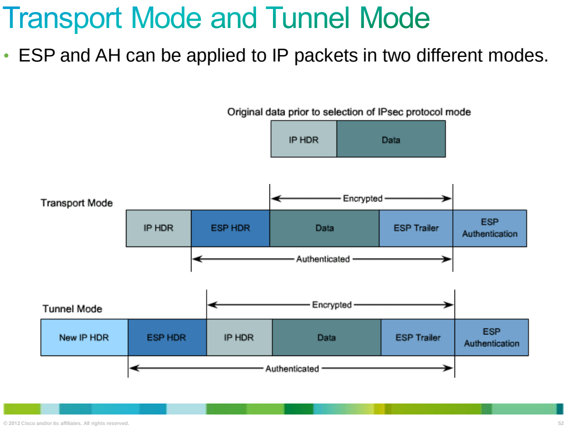
- ESP provides the same security services as AH (authentication and integrity) AND encryption service.
  - It encapsulates the data to be protected.
  - It operates on protocol number 50.



Encapsulating Security Payload (ESP)

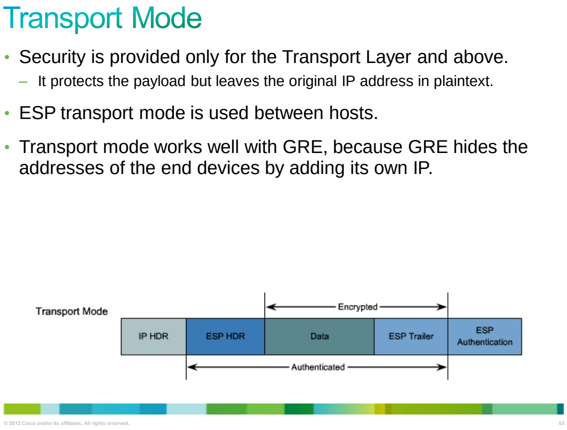
- ESP can also provide integrity and authentication.
  - First, the payload is encrypted using DES (default), 3DES, AES, or SEAL.
  - Next, the encrypted payload is hashed to provide authentication and data integrity using HMAC-MD5 or HMAC-SHA-1.

- Provides confidentiality with encryption
- Provides integrity with authentication



Transport Mode and Tunnel Mode

- ESP and AH can be applied to IP packets in two different modes.

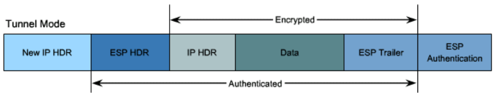


Transport Mode

- Security is provided only for the Transport Layer and above.
  - It protects the payload but leaves the original IP address in plaintext.
- ESP transport mode is used between hosts.
- Transport mode works well with GRE, because GRE hides the addresses of the end devices by adding its own IP.

Tunnel Mode

- Tunnel mode provides security for the complete original IP packet.
  - The original IP packet is encrypted and then it is encapsulated in another IP packet (IP-in-IP encryption).
- ESP tunnel mode is used in remote access and site-to-site implementations.



Key Exchange

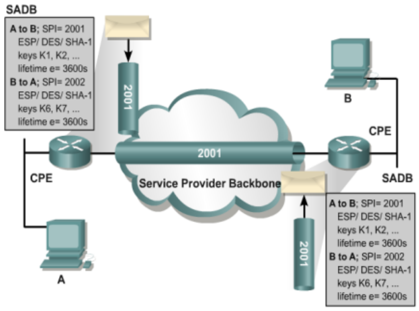
Key Exchange

- The IPsec VPN solution:
  - Negotiates key exchange parameters (IKE).
  - Establishes a shared key (DH).
  - Authenticates the peer.
  - Negotiates the encryption parameters.
- The negotiated parameters between two devices are known as a security association (SA).

Security Associations (SAs)

- SAs represent a policy contract between two peers or hosts, and describe how the peers will use IPsec security services to protect network traffic.
- SAs contain all the security parameters needed to securely transport packets between the peers or hosts, and practically define the security policy used in IPsec.

SA Security Parameters



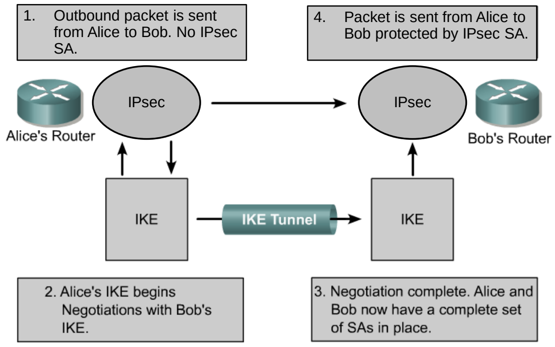
A to B; SPI= 2001
ESP/ DES/ SHA-1
keys K1, K2, ...
lifetime e= 3600s
B to A; SPI= 2002
ESP/ DES/ SHA-1
keys K6, K7, ...
lifetime e= 3600s

A to B; SPI= 2001
ESP/ DES/ SHA-1
keys K1, K2, ...
lifetime e= 3600s
B to A; SPI= 2002
ESP/ DES/ SHA-1
keys K6, K7, ...
lifetime e= 3600s

IKE - Internet Key Exchange

- IKE helps IPsec securely exchange cryptographic keys between distant devices.
  - Combination of the ISAKMP and the Oakley Key Exchange Protocol.
- Key Management can be preconfigured with IKE (ISAKMP) or with a manual key configuration.
  - IKE and ISAKMP are often used interchangeably.
- The IKE tunnel protects the SA negotiations.
  - After the SAs are in place, IPsec protects the data that Alice and Bob exchange.

How IPsec uses IKE



1. Outbound packet is sent from Alice to Bob. No IPsec SA.

4. Packet is sent from Alice to Bob protected by IPsec SA.

2. Alice's IKE begins Negotiations with Bob's IKE.

3. Negotiation complete. Alice and Bob now have a complete set of SAs in place.

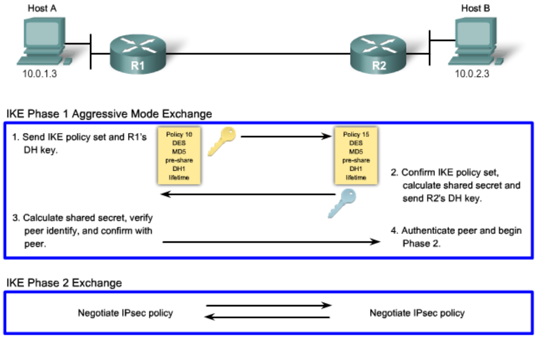
IKE - Internet Key Exchange

- There are two phases in every IKE negotiation
  - Phase 1 (Authentication)
  - Phase 2 (Key Exchange)
- IKE negotiation can also occur in:
  - Main Mode
  - Aggressive mode
- The difference between the two is that Main mode requires the exchange of 6 messages while Aggressive mode requires only 3 exchanges.

IKE Main Mode Phases

- IKE Phase One:
  - Negotiates an IKE protection suite.
  - Exchanges keying material to protect the IKE session (DH).
  - Authenticates each other.
  - Establishes the IKE SA.
  - Main Mode requires the exchange of 6 messages while Aggressive mode only uses 3 messages.
- IKE Phase Two:
  - Negotiates IPsec security parameters, known as IPsec transform sets.
  - Establishes IPsec SAs.
  - Periodically renegotiates IPsec SAs to ensure security.
  - Optionally performs an additional DH exchange.

IKE Phases



IKE Phase 1 Aggressive Mode Exchange

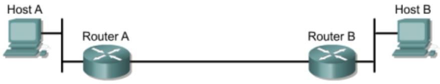
1. Send IKE policy set and R1's DH key.
2. Confirm IKE policy set, calculate shared secret and send R2's DH key.
3. Calculate shared secret, verify peer identify, and confirm with peer.
4. Authenticate peer and begin Phase 2.

IKE Phase 2 Exchange

Negotiate IPsec policy

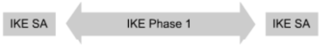
Negotiate IPsec policy

Five Steps of IPsec

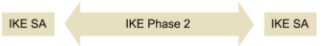


Step 1 Host A sends interesting traffic destined for Host B.

Step 2 **IKE Phase 1** authenticates IPsec peers and negotiates IKE SAs to create a secure communications channel for negotiating IPsec SAs in Phase 2.



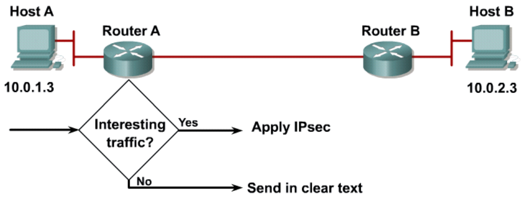
Step 3 **IKE Phase 2** negotiates IPsec SA parameters and creates matching IPsec SAs in the peers to protect data and messages exchanged between endpoints.

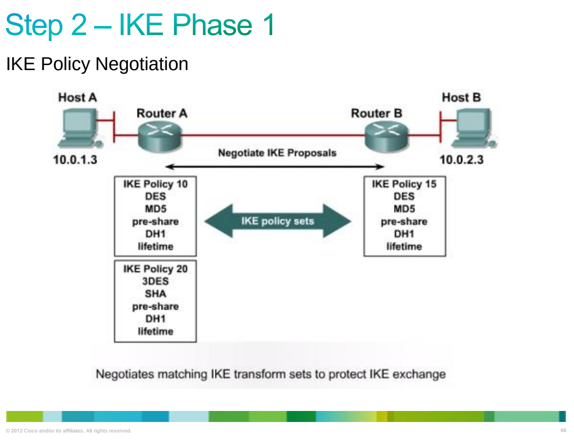


Step 4 Data transfer occurs between IPsec peers based on the IPsec parameters and keys stored in the SA database.

Step 5 IPsec tunnel termination occurs by SAs through deletion or by timing out.

Step 1 – Interesting Traffic

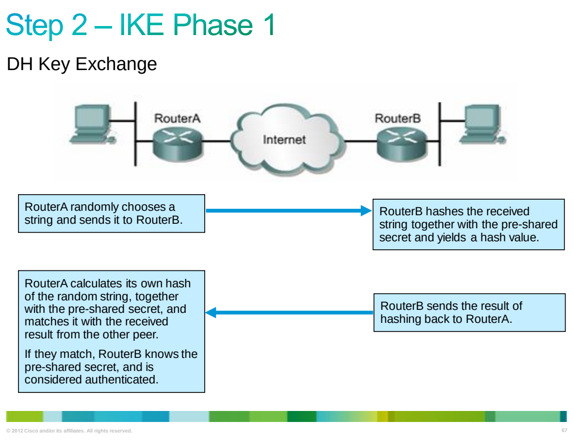




Step 2 – IKE Phase 1

IKE Policy Negotiation

Negotiates matching IKE transform sets to protect IKE exchange



Step 2 – IKE Phase 1

DH Key Exchange

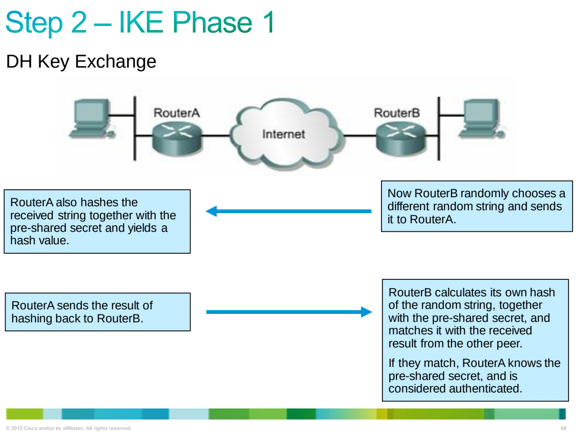
RouterA randomly chooses a string and sends it to RouterB.

RouterB hashes the received string together with the pre-shared secret and yields a hash value.

RouterA calculates its own hash of the random string, together with the pre-shared secret, and matches it with the received result from the other peer.

If they match, RouterB knows the pre-shared secret, and is considered authenticated.

RouterB sends the result of hashing back to RouterA.



Step 2 – IKE Phase 1

DH Key Exchange

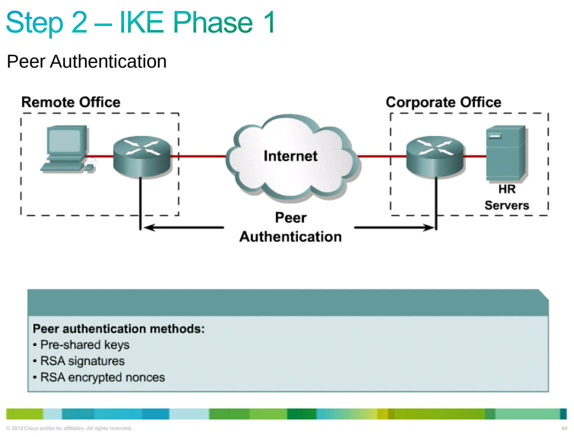
RouterA also hashes the received string together with the pre-shared secret and yields a hash value.

Now RouterB randomly chooses a different random string and sends it to RouterA.

RouterA sends the result of hashing back to RouterB.

RouterB calculates its own hash of the random string, together with the pre-shared secret, and matches it with the received result from the other peer.

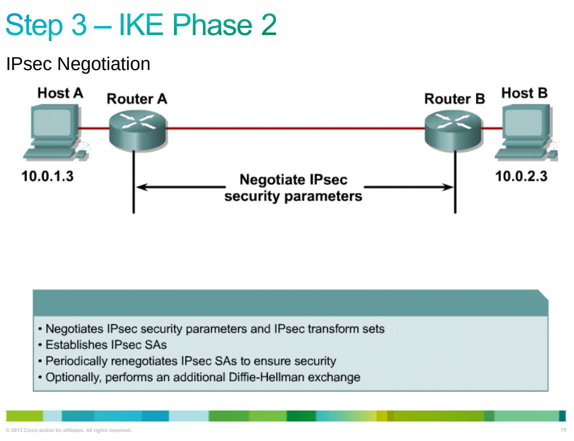
If they match, RouterA knows the pre-shared secret, and is considered authenticated.



Step 2 – IKE Phase 1

Peer Authentication

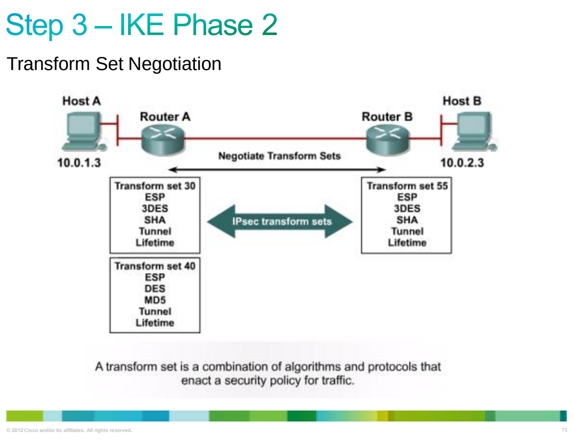
Peer authentication methods:
- Pre-shared keys
- RSA signatures
- RSA encrypted nonces



Step 3 – IKE Phase 2

IPsec Negotiation

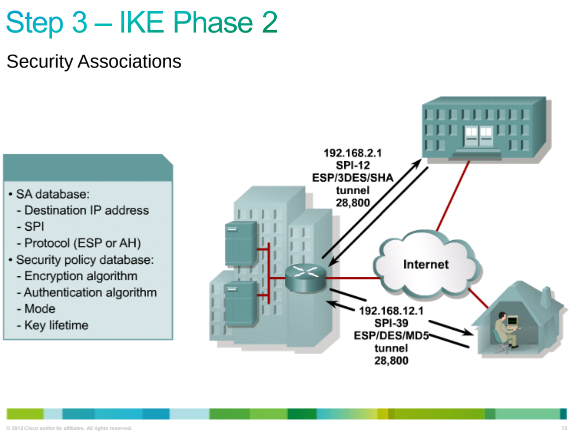
- Negotiates IPsec security parameters and IPsec transform sets
- Establishes IPsec SAs
- Periodically renegotiates IPsec SAs to ensure security
- Optionally, performs an additional Diffie-Hellman exchange



Step 3 – IKE Phase 2

Transform Set Negotiation

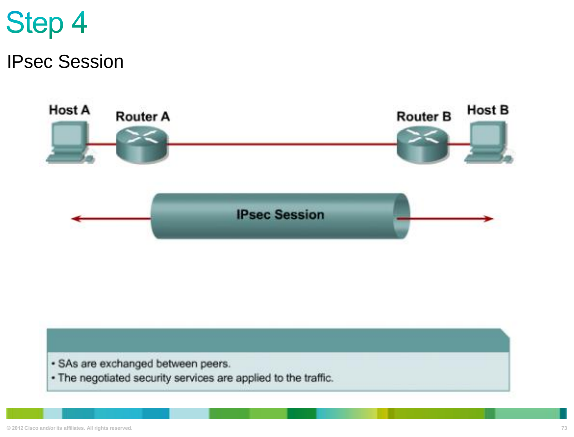
A transform set is a combination of algorithms and protocols that enact a security policy for traffic.



Step 3 – IKE Phase 2

Security Associations

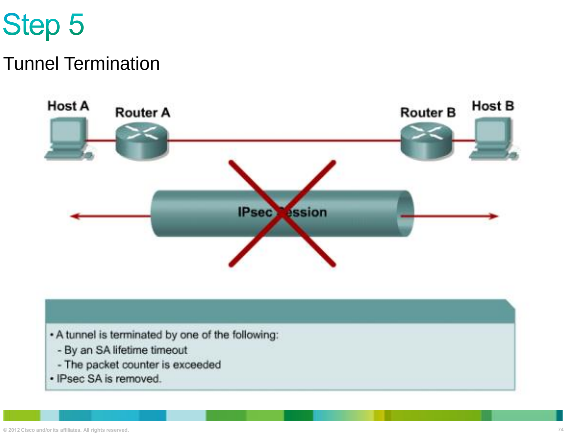
- SA database:
  - Destination IP address
  - SPI
  - Protocol (ESP or AH)
- Security policy database:
  - Encryption algorithm
  - Authentication algorithm
  - Mode
  - Key lifetime



Step 4

IPsec Session

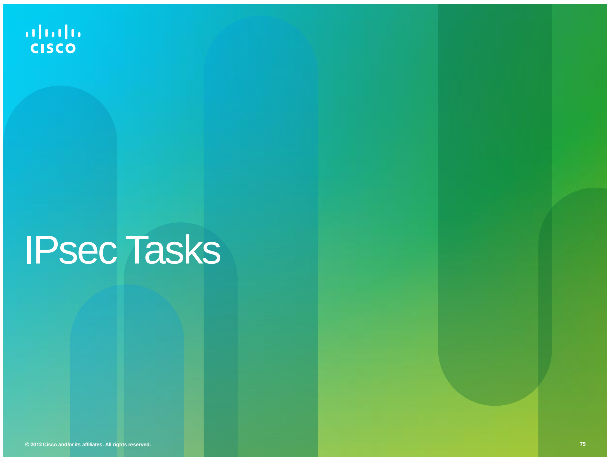
- SAs are exchanged between peers.
- The negotiated security services are applied to the traffic.



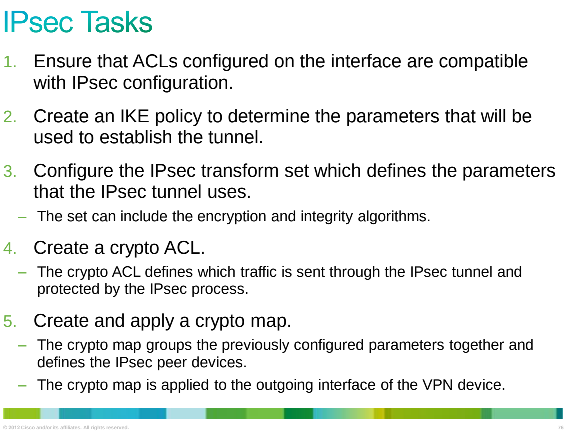
Step 5

Tunnel Termination

- A tunnel is terminated by one of the following:
  - By an SA lifetime timeout
  - The packet counter is exceeded
- IPsec SA is removed.

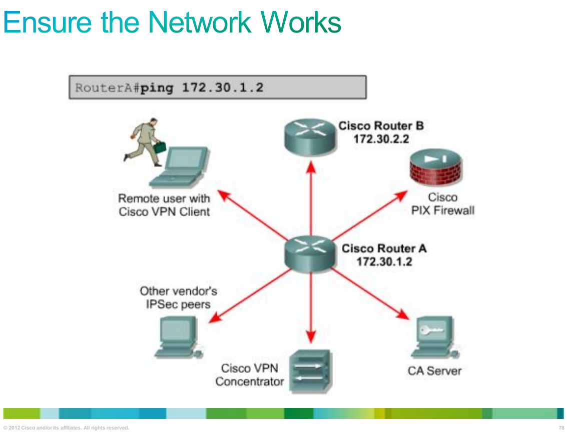


IPsec Tasks



IPsec Tasks

1. Ensure that ACLs configured on the interface are compatible with IPsec configuration.
2. Create an IKE policy to determine the parameters that will be used to establish the tunnel.
3. Configure the IPsec transform set which defines the parameters that the IPsec tunnel uses.
   – The set can include the encryption and integrity algorithms.
4. Create a crypto ACL.
   – The crypto ACL defines which traffic is sent through the IPsec tunnel and protected by the IPsec process.
5. Create and apply a crypto map.
   – The crypto map groups the previously configured parameters together and defines the IPsec peer devices.
   – The crypto map is applied to the outgoing interface of the VPN device.

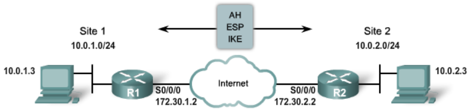


Ensure the Network Works

```
RouterA#ping 172.30.1.2
```

Task 1: Ensure ACLs are Compatible

ESP = protocol # 50, AH = protocol # 51, ISAKMP = UDP port 500



```
R1(config)# access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq isakmp
R1(config)# interface Serial0/0/0
R1(config-if)# ip address 172.30.1.2 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# ip access-group 102 in
R1(config-if)# exit
R1(config)# exit
R1#
R1# show access-lists
    access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
    access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
    access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq isakmp
```

Task 2: Configure IKE

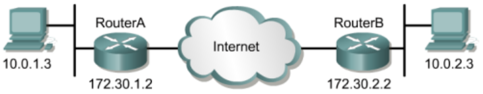
- Creating a plan in advance is mandatory to configure IPsec encryption correctly to minimize misconfiguration.
- Determine the following policy details:
  - Key distribution method
  - Authentication method
  - IPsec peer IP addresses and hostnames
  - IKE phase 1 policies for all peers
  - Encryption algorithm, Hash algorithm, IKE SA lifetime
- Goal: Minimize misconfiguration.

IKE Phase 1 Policy Parameters

Parameter	Strong	Stronger
Encryption Algorithm	DES	3-DES or AES
Hash Algorithm	MD5	SHA-1
Authentication Method	Pre-share	RSA Encryption RSA Signature
Key Exchange	D-H Group 1	D-H Group 2 or D-H 5
IKE SA Lifetime	86400 seconds	less than 86400 seconds

Parameters		R2 Site	R3 Office
Key distribution method	Manual or **ISAKMP**	ISAKMP	ISAKMP
Encryption algorithm	**DES** or 3DES	DES	DES
Hash algorithm	MD5 or **SHA-1**	SHA-1	SHA-1
Authentication method	Pre-share or **RSA**	Pre-Share	Pre-Share
Key exchange	D-H **Group 1** or 2	Group 1	Group 1
IKE SA Lifetime	**86400** seconds or less	86400	86400

Enable IKE



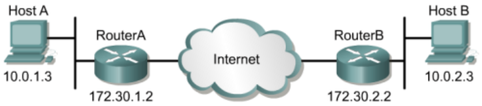
```
router(config)#
```

```
[no] crypto isakmp enable
```

```
RouterA(config)#crypto isakmp enable
```

- This command globally enables or disables IKE at the router
- IKE is enabled by default
- IKE is enabled globally for all interfaces at the router
- Use the no form of the command to disable IKE
- An ACL can be used to block IKE on a particular interface

Create an IKE Policy



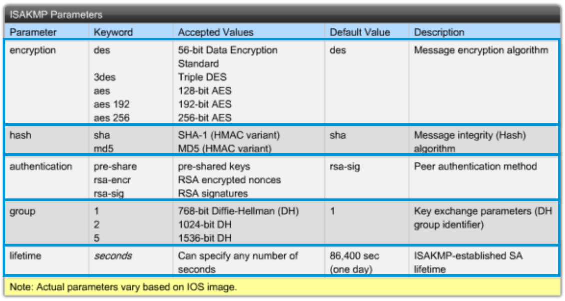
```
router(config)#
```

```
crypto isakmp policy priority
```

- Defines an IKE policy, which is a set of parameters used during IKE negotiation
- Invokes the config-isakmp command mode

```
RouterA(config)#crypto isakmp policy 110
```

Default ISAKMP Settings

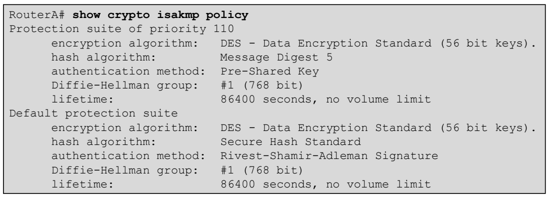


ISAKMP Parameters

Parameter	Keyword	Accepted Values	Default Value	Description
encryption	des 3des aes aes 192 aes 256	56-bit Data Encryption Standard Triple DES 128-bit AES 192-bit AES 256-bit AES	des	Message encryption algorithm
hash	sha md5	SHA-1 (HMAC variant) MD5 (HMAC variant)	sha	Message integrity (Hash) algorithm
authentication	pre-share rsa-encr rsa-sig	pre-shared keys RSA encrypted nonces RSA signatures	rsa-sig	Peer authentication method
group	1 2 5	768-bit Diffie-Hellman (DH) 1024-bit DH 1536-bit DH	1	Key exchange parameters (DH group identifier)
lifetime	*seconds*	Can specify any number of seconds	86,400 sec (one day)	ISAKMP-established SA lifetime

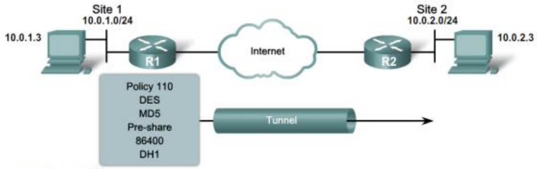
Note: Actual parameters vary based on IOS image.

Default ISAKMP Settings



```
RouterA# show crypto isakmp policy
Protection suite of priority 110
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Message Digest 5
      authentication method:  Pre-Shared Key
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
Default protection suite
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Secure Hash Standard
      authentication method:  Rivest-Shamir-Adleman Signature
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
```

Create an IKE Policy



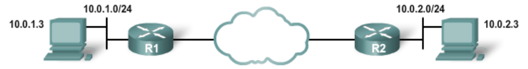
```
router(config)#
```

```
crypto isakmp policy priority
```

Defines the parameters within the IKE policy

```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption des
R1(config-isakmp)# group 1
R1(config-isakmp)# hash md5
R1(config-isakmp)# lifetime 86400
```

ISAKMP Policy Negotiation



R1#

```
crypto isakmp policy 100
  hash md5
  authentication pre-share
!
crypto isakmp policy 200
  hash sha
  authentication rsa-sig
!
crypto isakmp policy 300
  hash md5
  authentication pre-share
```

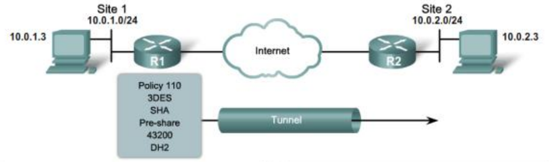
R2#

```
crypto isakmp policy 100
  hash md5
  authentication pre-share
!
crypto isakmp policy 200
  hash sha
  authentication rsa-sig
!
crypto isakmp policy 300
  hash md5
  authentication rsa-sig
```

Policy 100 and 200 can be successfully negotiated, but policy 300 cannot.

Note: smaller priority numbers have higher priority.

ISAKMP Policy Negotiation



```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# group 2
R1(config-isakmp)# hash sha
R1(config-isakmp)# lifetime 43200
```

```
R2(config)# crypto isakmp policy 100
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# group 2
R2(config-isakmp)# hash sha
R2(config-isakmp)# lifetime 43200
```

- R1 attempts to establish a VPN tunnel with R2 because it has interesting traffic destined for R2 and therefore sends its IKE policy parameters.
- R2 must have an ISAKMP policy configured with the same parameters. Notice however, that policy numbers are only locally significant and do not have to match between IPsec peers.

Configure Pre-Shared Keys

```
router(config)#
crypto isakmp key keystring address peer-address
```

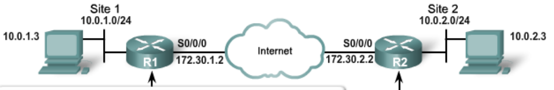
```
router(config)#
crypto isakmp key keystring hostname hostname
```

Parameter	Description
keystring	This parameter specifies the PSK. Use any combination of alphanumeric characters up to 128 bytes. This PSK must be identical on both peers.
peer-address	This parameter specifies the IP address of the remote peer.
hostname	This parameter specifies the hostname of the remote peer. This is the peer hostname concatenated with its domain name (for example, myhost.domain.com).

- The *peer-address* or *hostname* can be used, but must be used consistently between peers.
- If the *hostname* is used, then the **crypto isakmp identity hostname** command must also be configured.

- By default, the ISAKMP identity is set to use the IP address.

Configure Pre-Shared Keys



```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# group 2
R1(config-isakmp)# hash sha
R1(config-isakmp)# lifetime 43200
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco123 address 172.30.2.2
R1(config)#
```

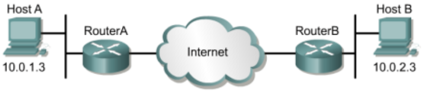
Note:

- The keystring cisco123 matches.
- The address identity method is specified.
- The ISAKMP policies are compatible.
- Default values do not have to be configured.

```
R2(config)# crypto isakmp policy 110
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# group 2
R2(config-isakmp)# hash sha
R2(config-isakmp)# lifetime 43200
R2(config-isakmp)# exit
R2(config)# crypto isakmp key cisco123 address 172.30.1.2
R2(config)#
```

Configure ISAKMP Identity

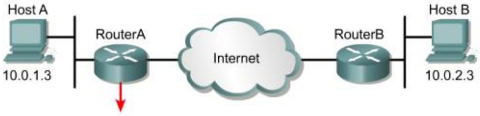
- To use the **`hostname`** parameter, configure the **`crypto isakmp identity`** *`hostname`* global configuration mode command.
  - In addition, DNS must be accessible to resolve the hostname.



```
router(config)#
crypto isakmp identity {address | hostname}
```

- Defines whether ISAKMP identity is done by IP address or hostname
- Use consistency across ISAKMP peers

Verify IKE Configuration



```
RouterA# show crypto isakmp policy
Protection suite of priority 110
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Message Digest 5
      authentication method:  Pre-Shared Key
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
Default protection suite
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Secure Hash Standard
      authentication method:  Rivest-Shamir-Adleman Signature
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
```

Task 3: Configure the Transform Sets

- Determine the following policy details:
  - IPsec algorithms and parameters for optimal security and performance
  - Transforms sets
  - IPsec peer details
  - IP address and applications of hosts to be protected
  - Manual or IKE-initiated SAs
- Goal: Minimize misconfiguration.

IPsec Transforms Supported in IOS

- Cisco IOS software supports the following IPsec transforms:

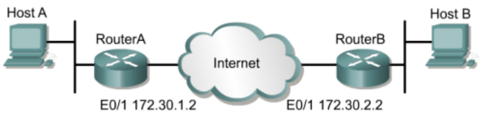
```
CentralA(config)# crypto ipsec transform-set transform-set-name ?
ah-md5-hmac   AH-HMAC-MD5 transform
ah-sha-hmac   AH-HMAC-SHA transform
esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
esp-des       ESP transform using DES cipher (56 bits)
esp-md5-hmac  ESP transform using HMAC-MD5 auth
esp-sha-hmac  ESP transform using HMAC-SHA auth
esp-null      ESP transform w/o cipher
```

Note:

esp-md5-hmac and **esp-sha-hmac** provide more data integrity.

They are compatible with NAT/PAT and are used more frequently than **ah-md5-hmac** and **ah-sha-hmac**.

IPsec Policy Example



Policy	Host A	Host B
Transform set	ESP-DES, Tunnel	ESP-DES, Tunnel
Peer hostname	RouterB	RouterA
Peer IP address	172.30.2.2	172.30.1.2
Hosts to be encrypted	10.0.1.3	10.0.2.3
Traffic (packet) type to be encrypted	TCP	TCP
SA establishment	ipsec-isakmp	ipsec-isakmp

Specific IPsec **show** Commands

```
RouterA# show crypto isakmp policy
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys)
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman Group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
```

```
RouterA# show crypto map
Crypto Map “MYMAP” 10 ipsec-isakmp
Peer = 172.30.2.2
Extended IP access list 102
access-list 102 permit ip host 172.30.1.2 host 172.30.2.2
Current peer: 172.30.2.2
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={ MY-SET, }
```

```
RouterA# show crypto ipsec transform-set MY-SET
Transform set MY-SET: { esp-des }
will negotiate = { Tunnel, },
```

Configure Transform Sets

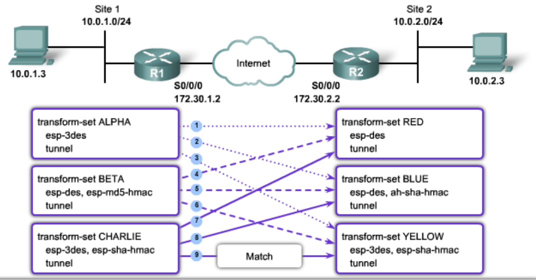
```
router(config)#
crypto ipsec transform-set transform-set-name transform1 [transform2]
[transform3][transform4]
```

crypto ipsec transform-set Parameters

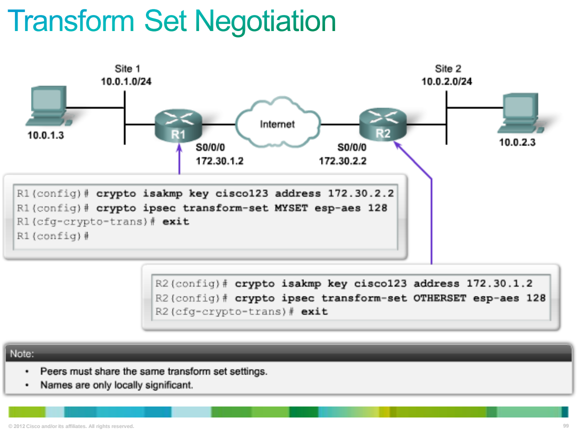
Command	Description
transform-set-name	This parameter specifies the name of the transform set to create (or modify).
transform1, transform2, transform3, transform4	Type of transform set. Specify up to four "transforms": one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication. These transforms define the IP Security (IPsec) security protocols and algorithms.

- A transform set is a combination of IPsec transforms that enact a security policy for traffic.
- A transform set can have one AH transform and up to two ESP transforms.

Transform Set Negotiation



- Transform sets are negotiated during IKE Phase 2.
- The 9th attempt found matching transform sets (CHARLIE - YELLOW).



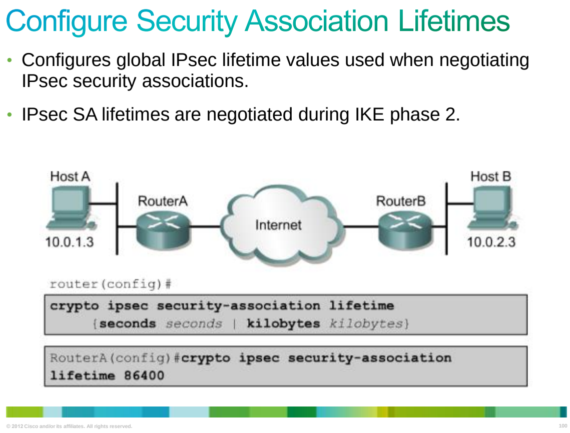
Transform Set Negotiation

```
R1(config)# crypto isakmp key cisco123 address 172.30.2.2
R1(config)# crypto ipsec transform-set MYSET esp-aes 128
R1(cfg-crypto-trans)# exit
R1(config)#
```

```
R2(config)# crypto isakmp key cisco123 address 172.30.1.2
R2(config)# crypto ipsec transform-set OTHERSET esp-aes 128
R2(cfg-crypto-trans)# exit
```

Note:

- Peers must share the same transform set settings.
- Names are only locally significant.



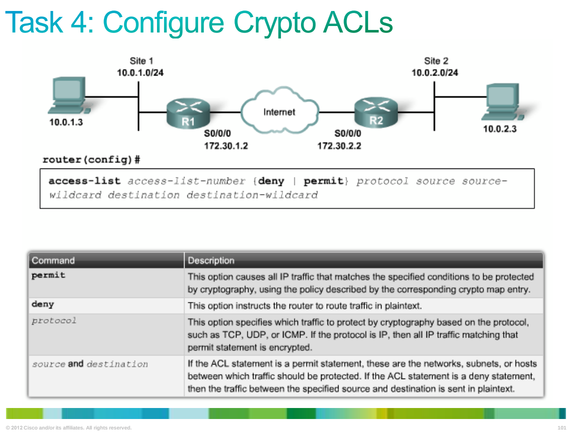
Configure Security Association Lifetimes

- Configures global IPsec lifetime values used when negotiating IPsec security associations.
- IPsec SA lifetimes are negotiated during IKE phase 2.

```
router(config)#
```

```
crypto ipsec security-association lifetime
      {seconds seconds | kilobytes kilobytes}
```

```
RouterA(config)#crypto ipsec security-association
lifetime 86400
```

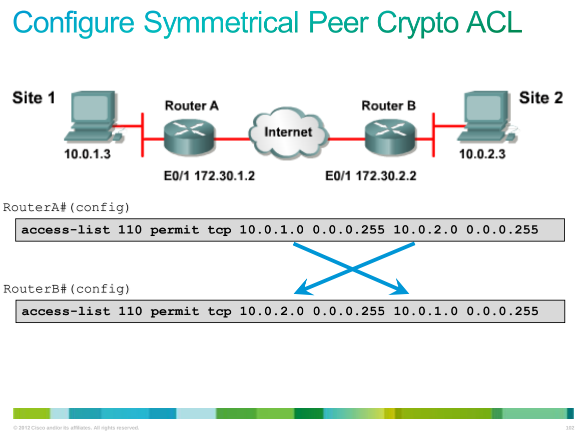


Task 4: Configure Crypto ACLs

```
router(config)#
```

```
access-list access-list-number {deny | permit} protocol source source-
wildcard destination destination-wildcard
```

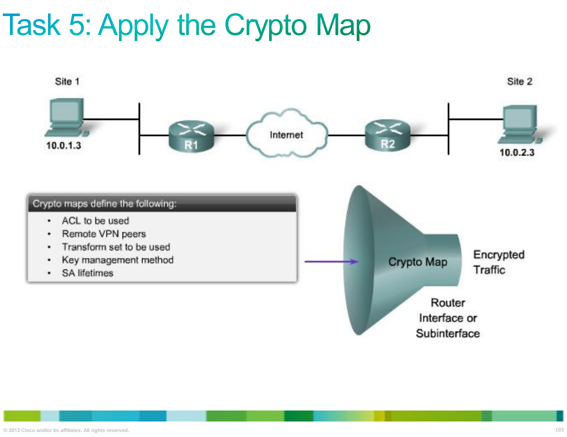
Command	Description
permit	This option causes all IP traffic that matches the specified conditions to be protected by cryptography, using the policy described by the corresponding crypto map entry.
deny	This option instructs the router to route traffic in plaintext.
protocol	This option specifies which traffic to protect by cryptography based on the protocol, such as TCP, UDP, or ICMP. If the protocol is IP, then all IP traffic matching that permit statement is encrypted.
source and *destination*	If the ACL statement is a permit statement, these are the networks, subnets, or hosts between which traffic should be protected. If the ACL statement is a deny statement, then the traffic between the specified source and destination is sent in plaintext.



Configure Symmetrical Peer Crypto ACL

```
RouterA#(config)
access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

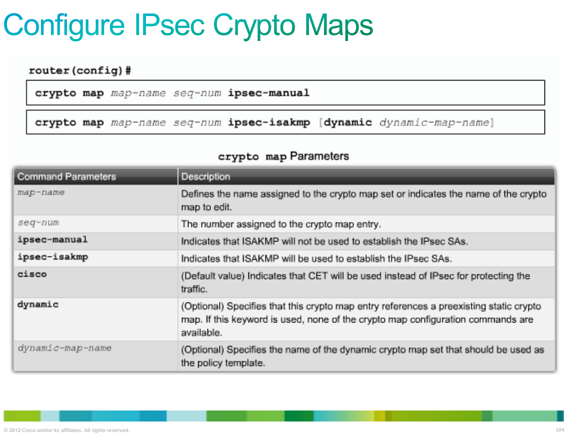
```
RouterB#(config)
access-list 110 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
```



Task 5: Apply the Crypto Map

Crypto maps define the following:

- ACL to be used
- Remote VPN peers
- Transform set to be used
- Key management method
- SA lifetimes

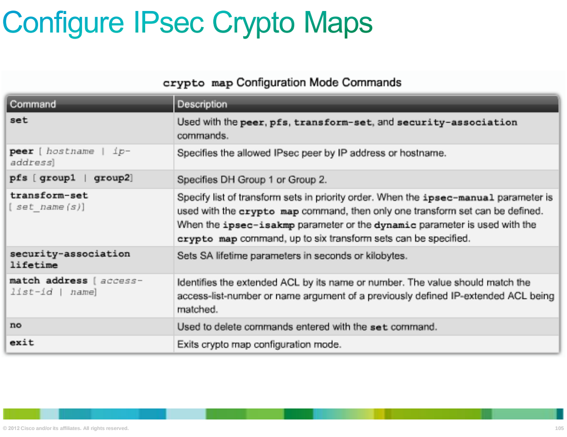


Configure IPsec Crypto Maps

```
router(config)#
crypto map map-name seq-num ipsec-manual
crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name]
```

crypto map Parameters

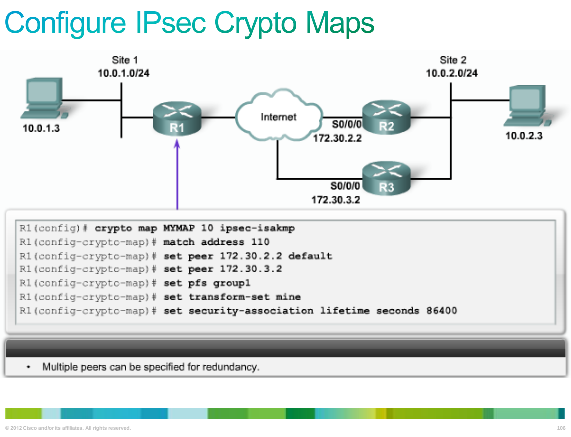
Command Parameters	Description
map-name	Defines the name assigned to the crypto map set or indicates the name of the crypto map to edit.
seq-num	The number assigned to the crypto map entry.
ipsec-manual	Indicates that ISAKMP will not be used to establish the IPsec SAs.
ipsec-isakmp	Indicates that ISAKMP will be used to establish the IPsec SAs.
cisco	(Default value) Indicates that CET will be used instead of IPsec for protecting the traffic.
dynamic	(Optional) Specifies that this crypto map entry references a preexisting static crypto map. If this keyword is used, none of the crypto map configuration commands are available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.



Configure IPsec Crypto Maps

crypto map Configuration Mode Commands

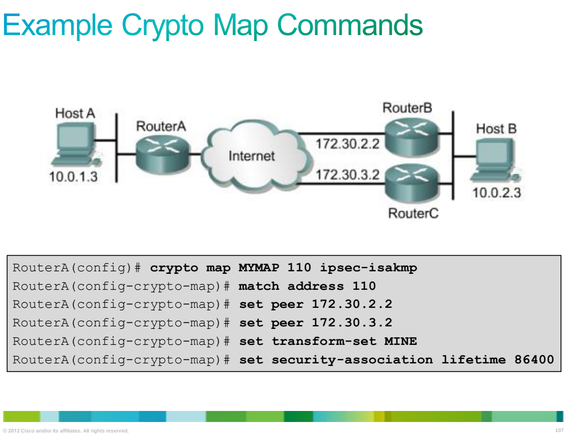
Command	Description
set	Used with the **peer**, **pfs**, **transform-set**, and **security-association** commands.
peer [*hostname* | *ip-address*]	Specifies the allowed IPsec peer by IP address or hostname.
pfs [**group1** | **group2**]	Specifies DH Group 1 or Group 2.
transform-set [*set_name(s)*]	Specify list of transform sets in priority order. When the **ipsec-manual** parameter is used with the **crypto map** command, then only one transform set can be defined. When the **ipsec-isakmp** parameter or the **dynamic** parameter is used with the **crypto map** command, up to six transform sets can be specified.
security-association lifetime	Sets SA lifetime parameters in seconds or kilobytes.
match address [*access-list-id* | *name*]	Identifies the extended ACL by its name or number. The value should match the access-list-number or name argument of a previously defined IP-extended ACL being matched.
no	Used to delete commands entered with the **set** command.
exit	Exits crypto map configuration mode.



Configure IPsec Crypto Maps

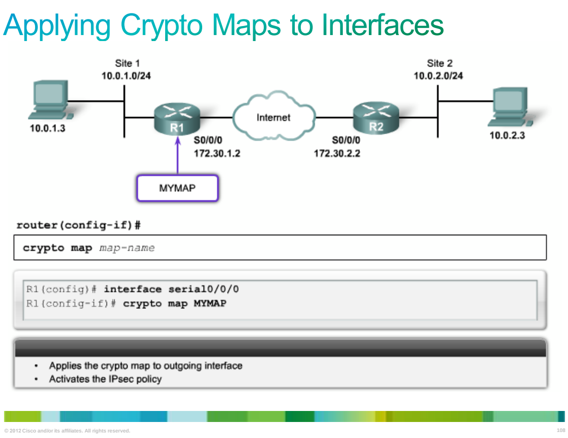
```
R1(config)# crypto map MYMAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# set peer 172.30.2.2 default
R1(config-crypto-map)# set peer 172.30.3.2
R1(config-crypto-map)# set pfs group1
R1(config-crypto-map)# set transform-set mine
R1(config-crypto-map)# set security-association lifetime seconds 86400
```

- Multiple peers can be specified for redundancy.



Example Crypto Map Commands

```
RouterA(config)# crypto map MYMAP 110 ipsec-isakmp
RouterA(config-crypto-map)# match address 110
RouterA(config-crypto-map)# set peer 172.30.2.2
RouterA(config-crypto-map)# set peer 172.30.3.2
RouterA(config-crypto-map)# set transform-set MINE
RouterA(config-crypto-map)# set security-association lifetime 86400
```

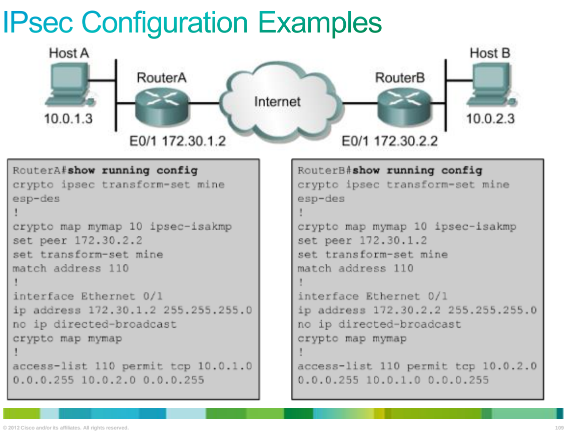


Applying Crypto Maps to Interfaces

```
router(config-if)#
crypto map map-name
```

```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map MYMAP
```

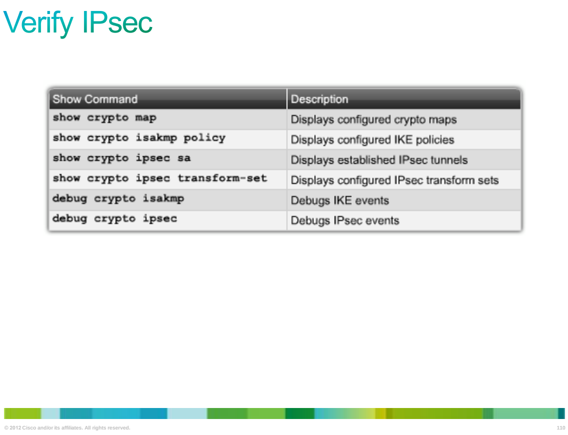
- Applies the crypto map to outgoing interface
- Activates the IPsec policy



IPsec Configuration Examples

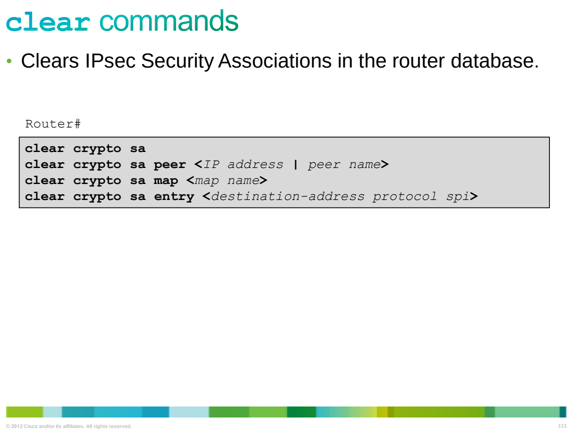
```
RouterA#show running config
crypto ipsec transform-set mine
esp-des
!
crypto map mymap 10 ipsec-isakmp
set peer 172.30.2.2
set transform-set mine
match address 110
!
interface Ethernet 0/1
ip address 172.30.1.2 255.255.255.0
no ip directed-broadcast
crypto map mymap
!
access-list 110 permit tcp 10.0.1.0
0.0.0.255 10.0.2.0 0.0.0.255
```

```
RouterB#show running config
crypto ipsec transform-set mine
esp-des
!
crypto map mymap 10 ipsec-isakmp
set peer 172.30.1.2
set transform-set mine
match address 110
!
interface Ethernet 0/1
ip address 172.30.2.2 255.255.255.0
no ip directed-broadcast
crypto map mymap
!
access-list 110 permit tcp 10.0.2.0
0.0.0.255 10.0.1.0 0.0.0.255
```



Verify IPsec

Show Command	Description
`show crypto map`	Displays configured crypto maps
`show crypto isakmp policy`	Displays configured IKE policies
`show crypto ipsec sa`	Displays established IPsec tunnels
`show crypto ipsec transform-set`	Displays configured IPsec transform sets
`debug crypto isakmp`	Debugs IKE events
`debug crypto ipsec`	Debugs IPsec events

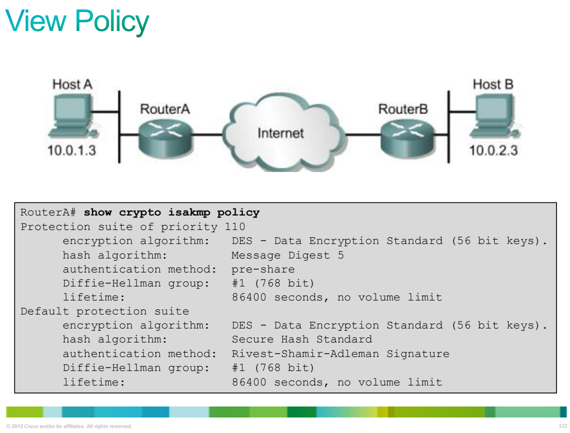


`clear` commands

- Clears IPsec Security Associations in the router database.

```
Router#
clear crypto sa
clear crypto sa peer <IP address | peer name>
clear crypto sa map <map name>
clear crypto sa entry <destination-address protocol spi>
```

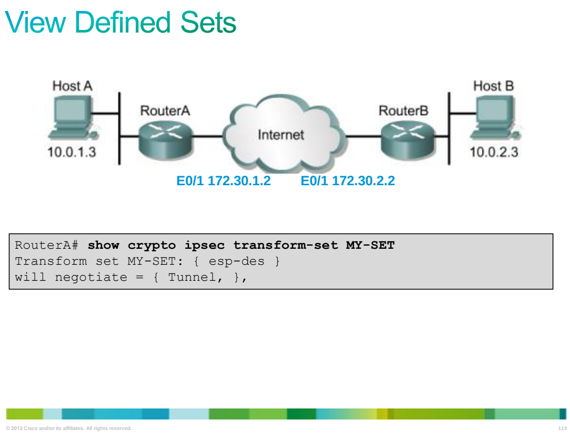
© 2012 Cisco and/or its affiliates. All rights reserved. 111



View Policy

```
RouterA# show crypto isakmp policy
Protection suite of priority 110
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Message Digest 5
      authentication method:  pre-share
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
Default protection suite
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Secure Hash Standard
      authentication method:  Rivest-Shamir-Adleman Signature
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
```

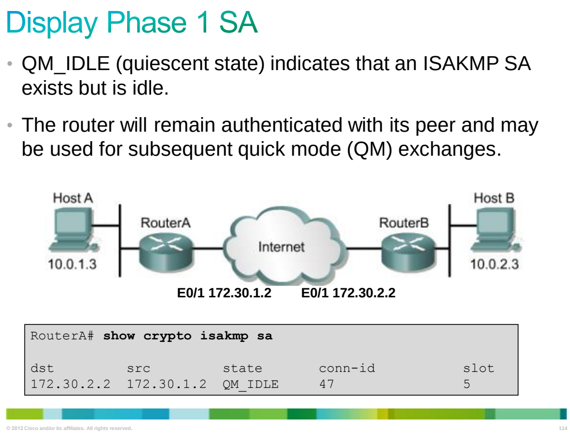
© 2012 Cisco and/or its affiliates. All rights reserved. 112



View Defined Sets

```
RouterA# show crypto ipsec transform-set MY-SET
Transform set MY-SET: { esp-des }
will negotiate = { Tunnel, },
```

© 2012 Cisco and/or its affiliates. All rights reserved. 113



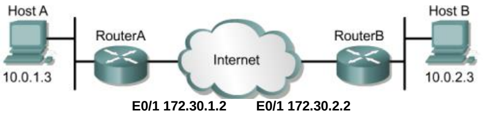
Display Phase 1 SA

- QM_IDLE (quiescent state) indicates that an ISAKMP SA exists but is idle.
- The router will remain authenticated with its peer and may be used for subsequent quick mode (QM) exchanges.

```
RouterA# show crypto isakmp sa

dst         src         state       conn-id          slot
172.30.2.2  172.30.1.2  QM_IDLE     47               5
```

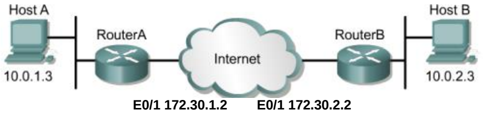
© 2012 Cisco and/or its affiliates. All rights reserved. 114

View Crypto IPsec SA



```
RouterA# show crypto ipsec sa
interface: Ethernet0/1
     Crypto map tag: MYMAP, local addr. 172.30.1.2
     local  ident (addr/mask/prot/port): (172.30.1.2/255.255.255.255/0/0)
     remote ident (addr/mask/prot/port): (172.30.2.2/255.255.255.255/0/0)
     current_peer: 172.30.2.2
      PERMIT, flags={origin_is_acl,}
        #pkts encaps: 21, #pkts encrypt: 21, #pkts digest 0
        #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 0
        #send errors 0, #recv errors 0
        local crypto endpt.: 172.30.1.2, remote crypto endpt.: 172.30.2.2
        path mtu 1500, media mtu 1500
        current outbound spi: 8AE1C9C
```

View Configured Crypto Maps



```
RouterA# show crypto map
Crypto Map “MYMAP" 10 ipsec-isakmp
          Peer = 172.30.2.2
          Extended IP access list 102
            access-list 102 permit ip host 172.30.1.2 host 172.30.2.2
          Current peer: 172.30.2.2
          Security association lifetime: 4608000 kilobytes/3600 seconds
          PFS (Y/N): N
          Transform sets={ MINE, }
```

Crypto System Error Messages for ISAKMP

- To display debug messages about all IPsec actions, use the global command **`debug crypto ipsec`**.
- To display debug messages about all ISAKMP actions, use the global command **`debug crypto isakmp`**.

Crypto System Error Messages for ISAKMP

- ISAKMP SA with the remote peer was not authenticated.

```
%CRYPTO-6-IKMP_SA_NOT_AUTH: Cannot accept Quick Mode exchange
from %15i if SA is not authenticated!
```

- ISAKMP peers failed protection suite negotiation for ISAKMP.

```
%CRYPTO-6-IKMP_SA_NOT_OFFERED: Remote peer %15i responded with
attribute [chars] not offered or changed
```

Crypto System Error Messages for ISAKMP

- This is an example of the Main Mode error message.
- The failure of Main Mode suggests that the Phase I policy does not match on both sides.

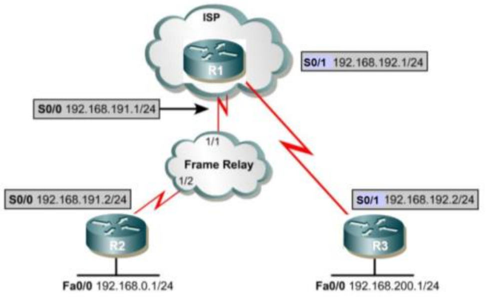
```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0 1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer at 150.150.150.1
```

- Verify that the Phase I policy is on both peers and ensure that all the attributes match.
  - Encryption: DES or 3DES
  - Hash: MD5 or SHA
  - Diffie-Hellman: Group 1 or 2
  - Authentication: rsa-sig, rsa-encr or pre-share

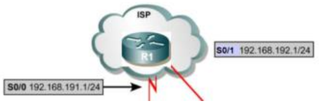
VPN Lab

VPN Lab Example

Configuring a Site-to-Site IPsec VPN Using Pre-Shared Keys



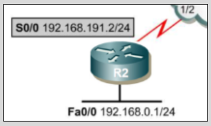
ISP Router



```
hostname R1
!
interface Serial0/0
 ip address 192.168.191.1 255.255.255.0
 encapsulation frame-relay
!
interface Serial0/1
 ip address 192.168.192.1 255.255.255.0
!
ip route 192.168.0.0 255.255.255.0 192.168.191.2
ip route 192.168.200.0 255.255.255.0 192.168.192.2
```

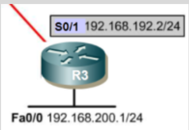
Lab Example

```
hostname R2
!
crypto isakmp policy 100
 authentication pre-share
crypto isakmp key CISCO1234 address 192.168.192.2
!
crypto ipsec transform-set MYSET esp-des
!
crypto map MYMAP 110 ipsec-isakmp
 set peer 192.168.192.2
 set transform-set MYSET
 match address 120
!
interface Serial0/0
 ip address 192.168.191.2 255.255.255.0
 encapsulation frame-relay
 crypto map MYMAP

ip route 0.0.0.0 0.0.0.0 192.168.191.1
!
access-list 120 permit ip 192.168.0.0 0.0.0.255 192.168.200.0 0.0.0.255
```



Lab Example

```
hostname R3
!
crypto isakmp policy 100
 authentication pre-share
crypto isakmp key CISCO1234 address 192.168.191.2
!
crypto ipsec transform-set MYSET esp-des
!
crypto map MYMAP 110 ipsec-isakmp
 set peer 192.168.191.2
 set transform-set MYSET
 match address 120

interface Serial0/1
 ip address 192.168.192.2 255.255.255.0
 clockrate 56000
 crypto map MYMAP
!
ip route 0.0.0.0 0.0.0.0 192.168.192.1
!
access-list 120 permit ip 192.168.200.0 0.0.0.255 192.168.0.0 0.0.0.255
```



Verify the VPN Configuration

- Clear the crypto security associations.
  - R2# **clear crypto sa**
  - R2# **clear crypto isakmp**

Verify the VPN Configuration

- Verify that the IPSEC SAs have been cleared.

```
R2# sho crypto ipsec sa

interface: Serial0/0
    Crypto map tag: MYMAP, local addr. 192.168.191.2

   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
   current_peer: 192.168.192.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.191.2, remote crypto endpt.: 192.168.192.2
     path mtu 1500, media mtu 1500
     current outbound spi: 0
```

Verify the VPN Configuration

- Initiate an extended ping from each respective LAN, to test the VPN configuration.

```
R2# ping
Protocol [ip]:
Target IP address: 192.168.200.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
132/135/136 ms
```

Verify the VPN Configuration

- After the extended ping, verify IPSEC SAs.

```
R2# sho crypto ipsec sa

interface: Serial0/0
    Crypto map tag: MYMAP, local addr. 192.168.191.2

   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
   current_peer: 192.168.192.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 192.168.191.2, remote crypto endpt.:
192.168.192.2
     path mtu 1500, media mtu 1500
     current outbound spi: 126912DC
```

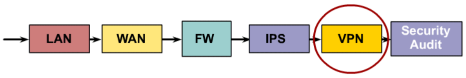
Configuring IPsec VPN using CCP

CCP 'Wizards'

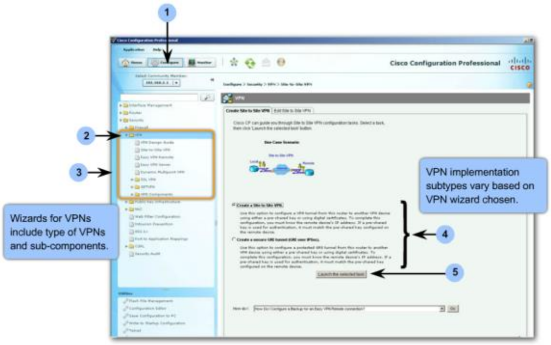
- Other intelligent Cisco wizards are available in CCP for these three tasks:
  - Auto detecting misconfiguration and proposing fixes.
  - Providing strong security and verifying configuration entries.
  - Using device and interface-specific defaults.

CCP ‘Wizards’

- Examples of CCP wizards include:
  - Startup wizard for initial router configuration
  - LAN and WAN wizards
  - Policy-based firewall and access-list management to easily configure firewall settings based on policy rules
  - IPS wizard
  - One-step site-to-site VPN wizard
  - One-step router lockdown wizard to harden the router



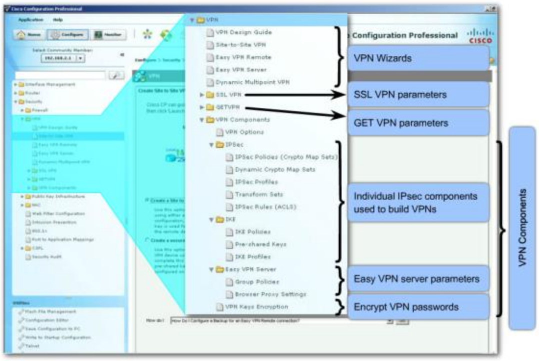
VPN Configuration Page



Wizards for VPNs include type of VPNs and sub-components.

VPN implementation subtypes vary based on VPN wizard chosen.

VPN Configuration Page



VPN Wizards

SSL VPN parameters

GET VPN parameters

Individual IPsec components used to build VPNs

Easy VPN server parameters

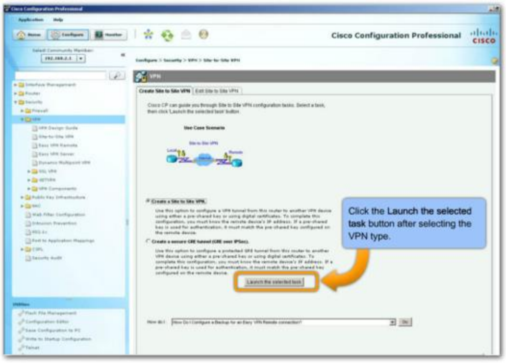
Encrypt VPN passwords

VPN Components

Site-to-Site VPN Components

- VPN wizards use two sources to create a VPN connection:
  - User input during the step-by-step wizard process
  - Preconfigured VPN components
- CCP provides some default VPN components:
  - IPsec transform set for Quick Setup wizard
- Other components are created by the VPN wizards:
  - Two IKE policies
- Some components (for example, PKI) must be configured before the wizards can be used.

VPN Configuration Page



Configure > Security > VPN > Site-to-Site VPN

VPN

Create Site to Site VPN | Edit Site to Site VPN

Cisco CP can guide you through Site to Site VPN configuration tasks. Select a task, then click 'Launch the selected task' button.

Use Case Scenario

● Create a Site to Site VPN.

Use this option to configure a VPN tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

○ Create a secure GRE tunnel (GRE over IPSec).

Use this option to configure a protected GRE tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

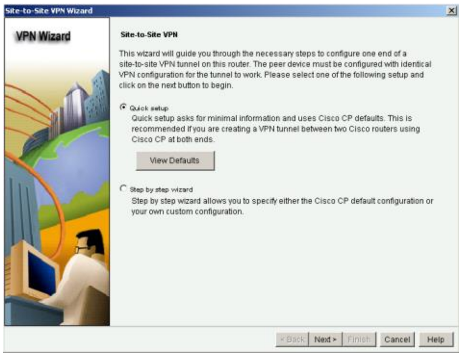
Launch the selected task

How do I: How Do I Configure a Backup for an Easy VPN Remote connection? Go

Click the Launch the selected task button after selecting the VPN type.

© 2012 Cisco and/or its affiliates. All rights reserved.

Quick Setup



Site-to-Site VPN

This wizard will guide you through the necessary steps to configure one end of a site-to-site VPN tunnel on this router. The peer device must be configured with identical VPN configuration for the tunnel to work. Please select one of the following setup and click on the next button to begin.

● Quick setup

Quick setup asks for minimal information and uses Cisco CP defaults. This is recommended if you are creating a VPN tunnel between two Cisco routers using Cisco CP at both ends.

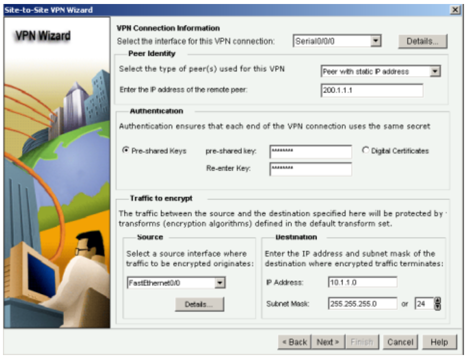
View Defaults

○ Step by step wizard

Step by step wizard allows you to specify either the Cisco CP default configuration or your own custom configuration.

© 2012 Cisco and/or its affiliates. All rights reserved.

Quick Setup



VPN Connection Information

Select the interface for this VPN connection: Serial0/0/0 Details...

Peer Identity

Select the type of peer(s) used for this VPN: Peer with static IP address

Enter the IP address of the remote peer: 200.1.1.1

Authentication

Authentication ensures that each end of the VPN connection uses the same secret

● Pre-shared Keys pre-shared key: ******** ○ Digital Certificates

Re-enter Key: ********

Traffic to encrypt

The traffic between the source and the destination specified here will be protected by transforms (encryption algorithms) defined in the default transform set.

Source

Select a source interface where traffic to be encrypted originates: FastEthernet0/0 Details...

Destination

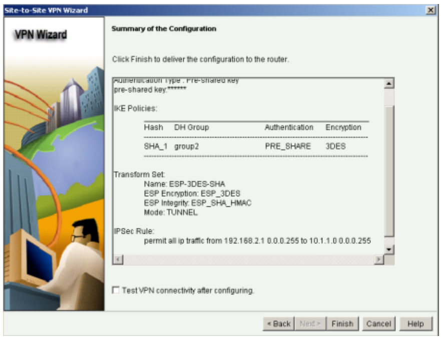
Enter the IP address and subnet mask of the destination where encrypted traffic terminates:

IP Address: 10.1.1.0

Subnet Mask: 255.255.255.0 or 24

© 2012 Cisco and/or its affiliates. All rights reserved.

Quick Setup



Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
Authentication Type : Pre-shared key
pre-shared key:******

IKE Policies:

          Hash    DH Group               Authentication    Encryption
          ----------------------------------------------------------
          SHA_1   group2                 PRE_SHARE         3DES
          ----------------------------------------------------------

Transform Set:
          Name: ESP-3DES-SHA
          ESP Encryption: ESP_3DES
          ESP Integrity: ESP_SHA_HMAC
          Mode: TUNNEL

IPSec Rule:
          permit all ip traffic from 192.168.2.1 0.0.0.255 to 10.1.1.0 0.0.0.255
```

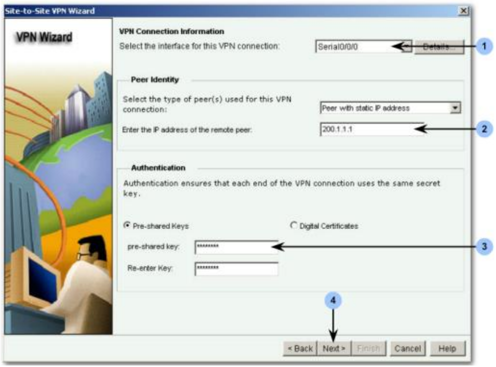
☐ Test VPN connectivity after configuring.

© 2012 Cisco and/or its affiliates. All rights reserved.

Step-by-Step Setup

- Multiple steps are required to configure the VPN connection:
  - Defining connection settings: Outside interface, peer address, authentication credentials
  - Defining IKE proposals: Priority, encryption algorithm, HMAC, authentication type, Diffie-Hellman group, lifetime
  - Defining IPsec transform sets: Encryption algorithm, HMAC, mode of operation, compression
  - Defining traffic to protect: Single source and destination subnets, ACL
  - Reviewing and completing the configuration

Configuring Connection Settings



VPN Connection Information

Select the interface for this VPN connection: Serial0/0/0

Peer Identity

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer: 200.1.1.1

Authentication

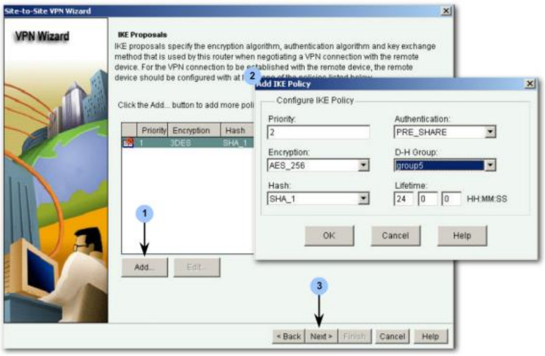
Authentication ensures that each end of the VPN connection uses the same secret key.

● Pre-shared Keys ○ Digital Certificates

pre-shared key: ********

Re-enter Key: ********

Configuring IKE Proposals



IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at l

Click the Add... button to add more poli

	Priority	Encryption	Hash
	1	3DES	SHA_1

Add IKE Policy

Configure IKE Policy

Priority: 2

Authentication: PRE_SHARE

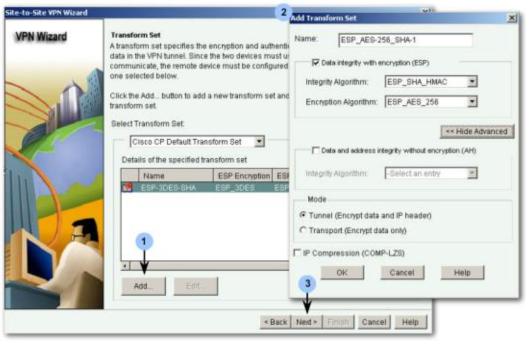
Encryption: AES_256

D-H Group: group5

Hash: SHA_1

Lifetime: 24 0 0 HH:MM:SS

Configuring the Transform Set



Transform Set

A transform set specifies the encryption and authenti data in the VPN tunnel. Since the two devices must u communicate, the remote device must be configured one selected below.

Click the Add... button to add a new transform set and transform set.

Select Transform Set: Cisco CP Default Transform Set

Details of the specified transform set

	Name	ESP Encryption	ESI
	ESP-3DES-SHA	ESP_3DES	ESP

Add Transform Set

Name: ESP_AES-256_SHA-1

☑ Data integrity with encryption (ESP)

Integrity Algorithm: ESP_SHA_HMAC

Encryption Algorithm: ESP_AES_256

☐ Data and address integrity without encryption (AH)

Integrity Algorithm: -Select an entry

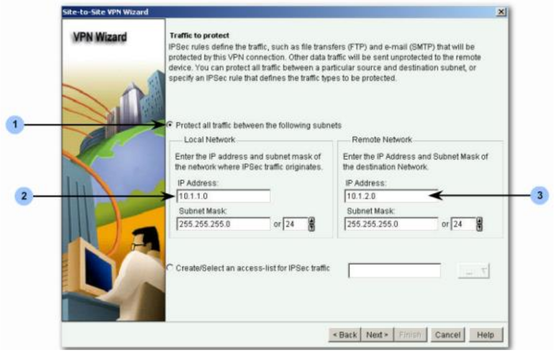
Mode

● Tunnel (Encrypt data and IP header)

○ Transport (Encrypt data only)

☐ IP Compression (COMP-LZS)

Defining Source and Destination Subnet



Site-to-Site VPN Wizard

VPN Wizard

Traffic to protect

IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected.

● Protect all traffic between the following subnets

Local Network

Enter the IP address and subnet mask of the network where IPSec traffic originates.

IP Address: 10.1.1.0

Subnet Mask: 255.255.255.0 or 24

Remote Network

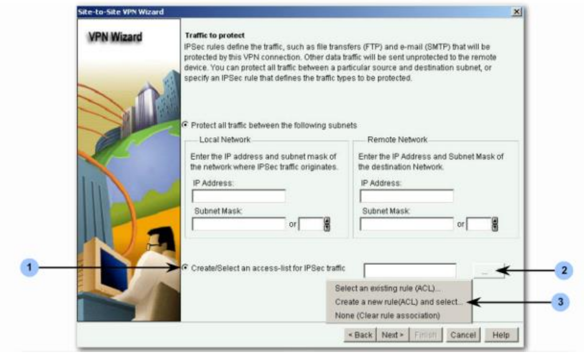
Enter the IP Address and Subnet Mask of the destination Network.

IP Address: 10.1.2.0

Subnet Mask: 255.255.255.0 or 24

○ Create/Select an access-list for IPSec traffic

Defining Interesting Traffic



Site-to-Site VPN Wizard

VPN Wizard

Traffic to protect

IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected.

○ Protect all traffic between the following subnets

Local Network

Enter the IP address and subnet mask of the network where IPSec traffic originates.

IP Address:

Subnet Mask: or

Remote Network

Enter the IP Address and Subnet Mask of the destination Network.

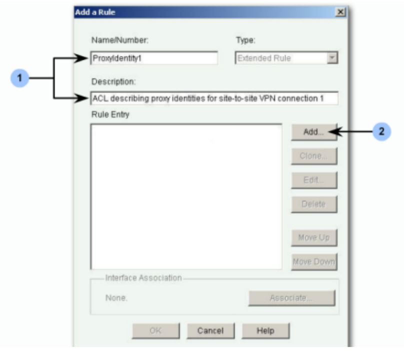
IP Address:

Subnet Mask: or

● Create/Select an access-list for IPSec traffic

...
Select an existing rule (ACL)...
Create a new rule(ACL) and select...
None (Clear rule association)
< Back
Next >
Finish
Cancel
Help

Adding Rules to ACLs



Add a Rule

Name/Number: ProxyIdentity1

Type: Extended Rule

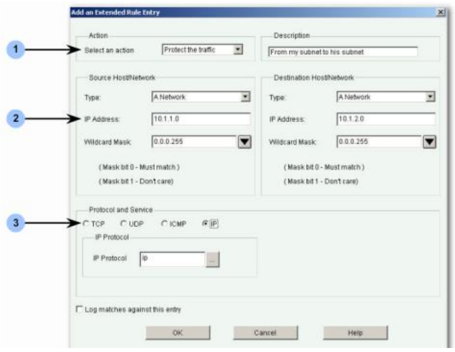
Description: ACL describing proxy identities for site-to-site VPN connection 1

Rule Entry

Interface Association

None.

Configuring a New ACL Rule Entry



Add an Extended Rule Entry

Action

Select an action: Protect the traffic

Description: From my subnet to his subnet

Source Host/Network

Type: A Network

IP Address: 10.1.1.0

Wildcard Mask: 0.0.0.255

(Mask bit 0 - Must match)

(Mask bit 1 - Don't care)

Destination Host/Network

Type: A Network

IP Address: 10.1.2.0

Wildcard Mask: 0.0.0.255

(Mask bit 0 - Must match)

(Mask bit 1 - Don't care)

Protocol and Service

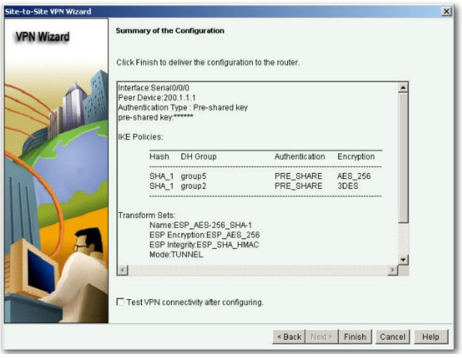
○ TCP ○ UDP ○ ICMP ● IP

IP Protocol

IP Protocol: IP

□ Log matches against this entry

Review the Generated Configuration



Site-to-Site VPN Wizard

VPN Wizard

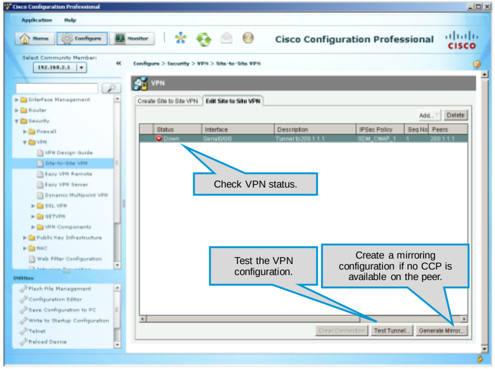
Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
Interface:Serial0/0/0
Peer Device:200.1.1.1
Authentication Type : Pre-shared key
pre-shared key:******

IKE Policies:

          Hash    DH Group              Authentication    Encryption
          -------------------------------------------------------------
          SHA_1   group5                PRE_SHARE         AES_256
          SHA_1   group2                PRE_SHARE         3DES
          -------------------------------------------------------------

Transform Sets:
          Name:ESP_AES-256_SHA-1
          ESP Encryption:ESP_AES_256
          ESP Integrity:ESP_SHA_HMAC
          Mode:TUNNEL
```

☐ Test VPN connectivity after configuring.

Test Tunnel Configuration and Operation



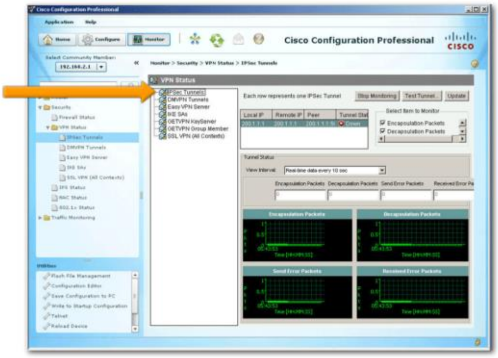
Status	Interface	Description	IPSec Policy	Seq No	Peers
Down	Serial0/0/0	Tunnel to 200.1.1.1	SDM_CMAP_1	1	200.1.1.1

Check VPN status.

Test the VPN configuration.

Create a mirroring configuration if no CCP is available on the peer.

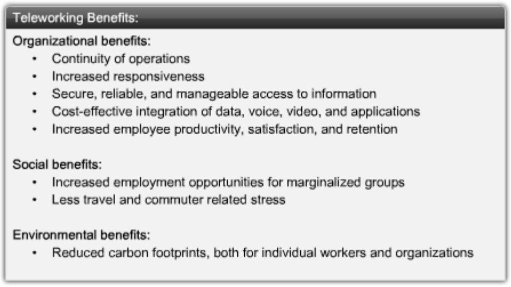
Test Tunnel Configuration and Operation



Local IP	Remote IP	Peer	Tunnel Stat
200.1.1.1	200.1.1.1	200.1.1.1:50	Down

Remote-Access VPNs

Teleworking Benefits



Teleworking Benefits:

Organizational benefits:

- Continuity of operations
- Increased responsiveness
- Secure, reliable, and manageable access to information
- Cost-effective integration of data, voice, video, and applications
- Increased employee productivity, satisfaction, and retention

Social benefits:

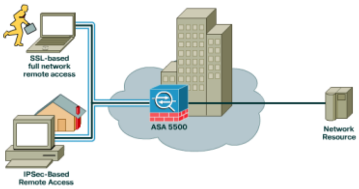
- Increased employment opportunities for marginalized groups
- Less travel and commuter related stress

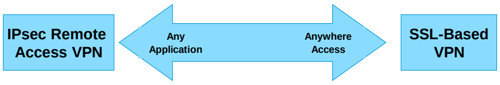
Environmental benefits:

- Reduced carbon footprints, both for individual workers and organizations

Remote-Access Solutions

- There are two primary methods for deploying remote-access VPNs:


SSL-based full network remote access
IPSec-Based Remote Access
ASA 5500
Network Resource



IPsec Remote Access VPN

Any Application

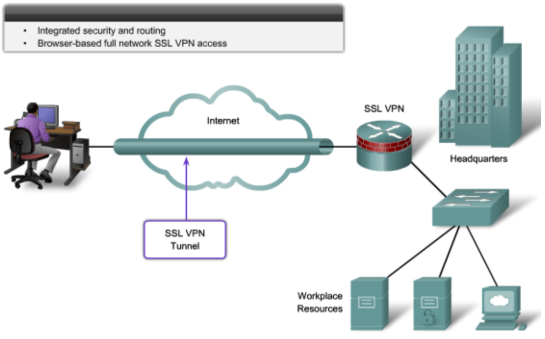
Anywhere Access

SSL-Based VPN

Remote-Access Solutions

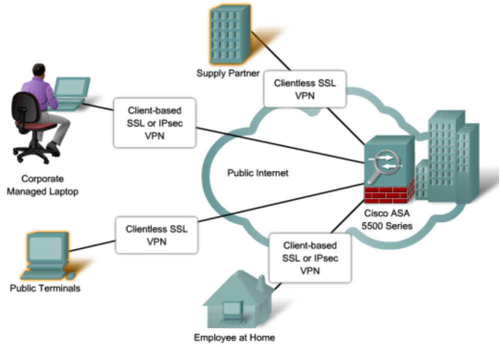
	SSL	IPsec
Applications	Web-enabled applications, file sharing, e-mail	All IP-based applications
Encryption	**Moderate** Key lengths from 40 bits to 128 bits	**Stronger** Key lengths from 56 bits to 256 bits
Authentication	**Moderate** One-way or two-way authentication	**Strong** Two-way authentication using shared secrets or digital certificates
Ease of Use	**Very high**	**Moderate** Can be challenging to nontechnical users
Overall Security	**Moderate** Any device can connect	**Strong** Only specific devices with specific configurations can connect

SSL VPN

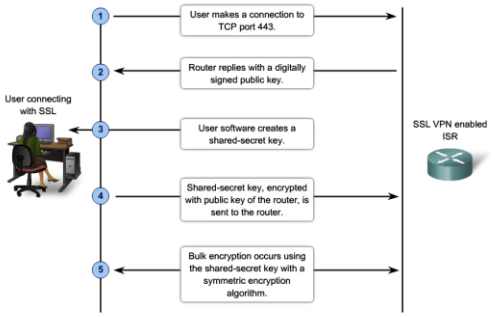


- Integrated security and routing
- Browser-based full network SSL VPN access

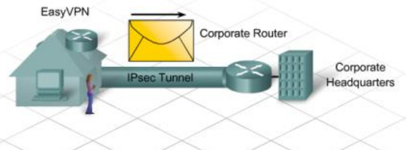
Clientless, Thin Client, or Full Client



Establishing SSL Session


1
User makes a connection to TCP port 443.
2
Router replies with a digitally signed public key.
User connecting with SSL
3
User software creates a shared-secret key.
SSL VPN enabled ISR
4
Shared-secret key, encrypted with public key of the router, is sent to the router.
5
Bulk encryption occurs using the shared-secret key with a symmetric encryption algorithm.

Cisco Easy VPN



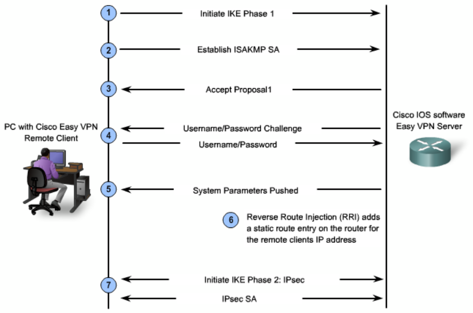
Cisco Easy VPN

- Negotiates tunnel parameters
- Establishes tunnels according to set parameters
- Authenticates users by usernames, group names, and passwords
- Manages security keys for encryption and decryption
- Authenticates, encrypts, and decrypts data through the tunnel

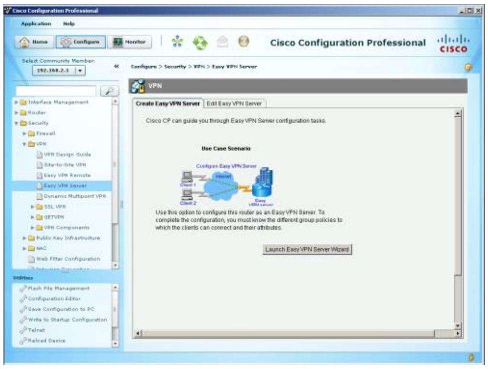
Cisco Easy VPN Components

- Cisco Easy VPN Server - A Cisco IOS router or Cisco PIX / ASA Firewall acting as the VPN head-end device in site-to-site or remote-access VPNs.
- Cisco Easy VPN Remote - A Cisco IOS router or Cisco PIX / ASA Firewall acting as a remote VPN client.
- Cisco Easy VPN Client - An application supported on a PC used to access a Cisco VPN server.

Cisco Easy VPN Exchange


1 Initiate IKE Phase 1
2 Establish ISAKMP SA
3 Accept Proposal1
4 Username/Password Challenge
Username/Password
5 System Parameters Pushed
6 Reverse Route Injection (RRI) adds a static route entry on the router for the remote clients IP address
7 Initiate IKE Phase 2: IPsec
IPsec SA
PC with Cisco Easy VPN Remote Client
Cisco IOS software Easy VPN Server

Configuring Easy VPN Server



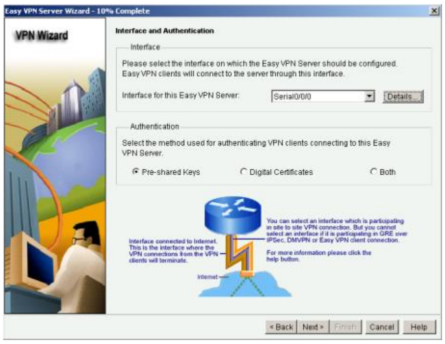
Configure > Security > VPN > Easy VPN Server

Cisco CP can guide you through Easy VPN Server configuration tasks.

Use Case Scenario

Use this option to configure this router as an Easy VPN Server. To complete the configuration, you must know the different group policies to which the clients can connect and their attributes.

Configuring Easy VPN Server Physical Interface



Interface and Authentication

Interface

Please select the interface on which the Easy VPN Server should be configured. Easy VPN clients will connect to the server through this interface.

Interface for this Easy VPN Server: Serial0/0/0

Authentication

Select the method used for authenticating VPN clients connecting to this Easy VPN Server.

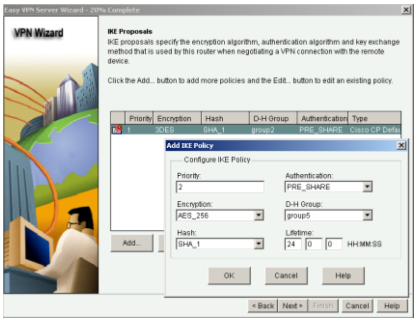
● Pre-shared Keys ○ Digital Certificates ○ Both

Interface connected to Internet. This is the interface where the VPN connections from the VPN clients will terminate.

You can select an interface which is participating in site to site VPN connection. But you cannot select an interface if it is participating in GRE over IPSec, DMVPN or Easy VPN client connection.

For more information please click the help button.

Configuring IKE Proposals



IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

Priority	Encryption	Hash	D-H Group	Authentication	Type
1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defau

Configure IKE Policy

Priority: 2

Authentication: PRE_SHARE

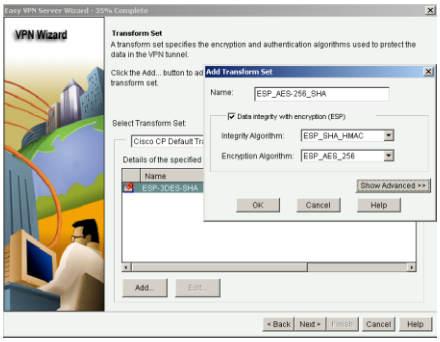
Encryption: AES_256

D-H Group: group5

Hash: SHA_1

Lifetime: 24 0 0 HH:MM:SS

Configuring Transform Set



Easy VPN Server Wizard - 35% Complete

Transform Set

A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel.

Click the Add... button to ad transform set.

Select Transform Set: Cisco CP Default Tr

Details of the specified

	Name
	ESP-3DES-SHA

Add Transform Set

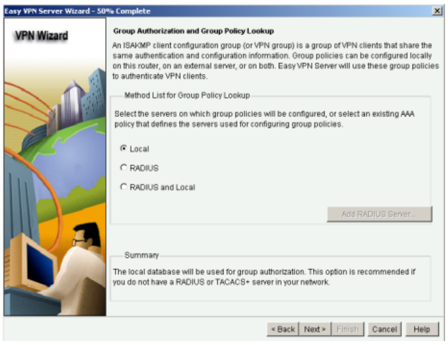
Name: ESP_AES-256_SHA

☑ Data integrity with encryption (ESP)

Integrity Algorithm: ESP_SHA_HMAC

Encryption Algorithm: ESP_AES_256

Configuring VPN Authentication Method List



Easy VPN Server Wizard - 50% Complete

Group Authorization and Group Policy Lookup

An ISAKMP client configuration group (or VPN group) is a group of VPN clients that share the same authentication and configuration information. Group policies can be configured locally on this router, on an external server, or on both. Easy VPN Server will use these group policies to authenticate VPN clients.

Method List for Group Policy Lookup

Select the servers on which group policies will be configured, or select an existing AAA policy that defines the servers used for configuring group policies.

● Local

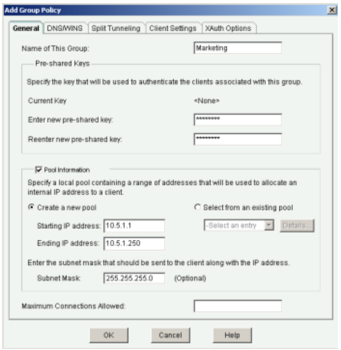
○ RADIUS

○ RADIUS and Local

Summary

The local database will be used for group authorization. This option is recommended if you do not have a RADIUS or TACACS+ server in your network.

Configuring VPN Authentication Group Policy



Add Group Policy

Name of This Group: Marketing

Pre-shared Keys

Specify the key that will be used to authenticate the clients associated with this group.

Current Key <None>

Enter new pre-shared key: *********

Reenter new pre-shared key: *********

☑ Pool Information

Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.

● Create a new pool ○ Select from an existing pool

Starting IP address: 10.5.1.1 -Select an entry

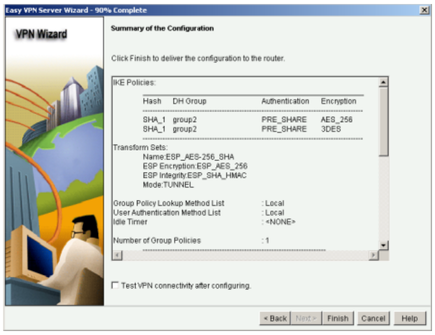
Ending IP address: 10.5.1.250

Enter the subnet mask that should be sent to the client along with the IP address.

Subnet Mask: 255.255.255.0 (Optional)

Maximum Connections Allowed:

Configuration Summary



Easy VPN Server Wizard - 90% Complete

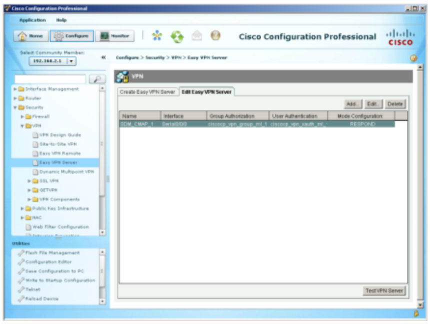
Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
IKE Policies:

          Hash    DH Group              Authentication    Encryption
          ---------------------------------------------------------
          SHA_1   group2                PRE_SHARE         AES_256
          SHA_1   group2                PRE_SHARE         3DES
          ---------------------------------------------------------
Transform Sets:
          Name:ESP_AES-256_SHA
          ESP Encryption:ESP_AES_256
          ESP Integrity:ESP_SHA_HMAC
          Mode:TUNNEL

Group Policy Lookup Method List          : Local
User Authentication Method List          : Local
Idle Timer                               : <NONE>

Number of Group Policies                 : 1
          ------------------------------------------------
```

☐ Test VPN connectivity after configuring.

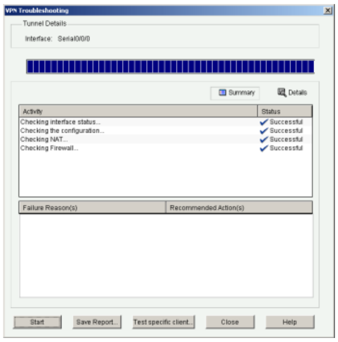
Edit Easy VPN Server



Configure > Security > VPN > Easy VPN Server

Name	Interface	Group Authorization	User Authentication	Mode Configuration
SDM_CMAP_1	Serial0/0/0	ciscocp_vpn_group_ml_1	ciscocp_vpn_xauth_ml_	RESPOND

Easy VPN Server Test

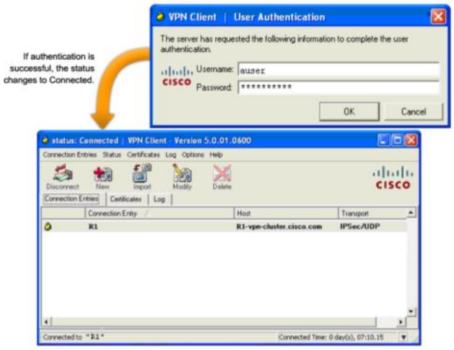


Interface: Serial0/0/0

Activity	Status
Checking interface status...	✓ Successful
Checking the configuration...	✓ Successful
Checking NAT...	✓ Successful
Checking Firewall...	✓ Successful

Failure Reason(s)	Recommended Action(s)

Connecting Using the Client



If authentication is successful, the status changes to Connected.

The server has requested the following information to complete the user authentication.

Username: auser

Password: **********

Connection Entry	Host	Transport
R1	R1-vpn-cluster.cisco.com	IPSec/UDP

Connected to "R1"

Connected Time: 0 day(s), 07:10.15