

# Internet Key Exchange Mode Configuration

---

## Feature Overview

Internet Key Exchange (IKE) Mode Configuration, as defined by the Internet Engineering Task Force (IETF), allows a gateway to download an IP address (and other network level configuration) to the client as part of an IKE negotiation. Using this exchange, the gateway gives IP addresses to the IKE client to be used as an “inner” IP address encapsulated under IPSec. This provides a known IP address for the client which can be matched against Internet Protocol Security (IPSec) policy.

This feature implements IKE Mode Configuration into existing Cisco IOS IPSec software images. Using IKE Mode Configuration, you can configure a Cisco access server to download an IP address to a client as part of an IKE transaction.

## Benefits

To implement IPSec Virtual Private Networks (VPNs) between remote access clients with dynamic IP addresses and a corporate gateway, you have to dynamically administer scalable IPSec policy on the gateway once each client is authenticated. With IKE Mode Configuration, the gateway can set up scalable policy for a very large set of clients irrespective of the IP addresses of those clients.

## Restrictions

IKE Mode Configuration has the following restrictions:

- Interfaces with crypto maps which are configured for IKE Mode Configuration may experience a slightly longer connection set up time. This is true even for IKE peers that refuse to be configured or do not respond to the configuration mode request. In both cases, the gateway initiates the configuration of the client.
- At the time of this publication, this feature is an IETF draft with limited support. Therefore, this feature was not designed to enable the configuration mode for every IKE connection by default. For more information, see the “Command Reference”.
- The following items in the IETF draft are not currently supported:
  - Configuration attributes other than INTERNAL\_IP\_ADDRESS
  - Unprotected exchanges



**Caution** Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to United States government export controls, and have a limited distribution. Images to be installed outside the United States require an export license. Customer orders might be denied or subject to delay due to United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to [export@cisco.com](mailto:export@cisco.com).

## Related Documents

For related information on the IKE Mode Configuration feature, refer to the following documents:

- Cisco IOS Release 12.0 *Security Configuration Guide*
- Cisco IOS Release 12.0 *Security Command Reference*
- *Internet Key Exchange Security Protocol* feature module

## Supported Platforms

- Cisco 1600 series routers
- Cisco 1700 series routers
- Cisco 2500 series routers
- Cisco 2600 series routers
- Cisco 3600 series routers
- Cisco MC3810 multiservice access concentrators
- Cisco 4000 series routers (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
- Cisco 7100 series routers
- Cisco 7200 series routers
- Cisco 7500 series routers
- Cisco AS5300 universal access servers

## Prerequisites

- Before configuring IKE Mode Configuration, you must have an IPSec software image that supports the IKE Mode Configuration feature downloaded on to your router. For more information on downloading a software image, see the following publications:
  - “Loading and Maintaining System Images and Microcode” chapter of the Cisco IOS Release 12.0 *Configuration Fundamentals Configuration Guide*
  - “System Image and Microcode Commands” chapter of the Cisco IOS Release 12.0 *Configuration Fundamentals Command Reference*

## Supported MIBs and RFCs

MIBs  
None

For descriptions of supported MIBs and how to use MIBs, see Cisco's MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

### RFCs

RFC 2119

RFC 2131

RFC 2251

RFC 2138

## List of Terms and Acronyms

**client**—Node or software program (front-end device) that requests services from a server.

**gateway**—A device, usually a Cisco access server, that performs an application layer conversion from one protocol stack to another.

**IP Security Protocol**—See IPsec.

**IPsec**—A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

**IKE**—A key management protocol standard which is used in conjunction with the IPsec standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

**Internet Key Exchange**—See IKE.

**VPN**—Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

**Virtual Private Network**—See VPN.

## Configuration Tasks

To configure a Cisco router to support IKE Mode Configuration, perform the following tasks:

- Configuring Internet Key Exchange Mode Configuration
- Verifying Internet Key Exchange Mode Configuration

## Configuring Internet Key Exchange Mode Configuration

There are two types of IKE Mode Configuration for VPN:

- Gateway initiation—Gateway initiates the configuration mode with the client. Once the client responds, the IKE modifies the sender’s identity, the message is processed, and the client receives a response.
- Client initiation—Client initiates the configuration mode with the gateway. The gateway responds with an IP address it has allocated for the client.

There are two steps to configuring IKE Mode Configuration on your router:

- Define the pool of IP addresses.
- Define which crypto maps should attempt to configure clients.

To configure IKE Mode Configuration on your Cisco router, use the following commands in global configuration mode:

Step	Command	Purpose
1	<code>router(config)# ip local pool &lt;pool-name&gt; &lt;start-addr&gt; &lt;end-addr&gt;</code>	Existing local address pools are used to define a set of addresses. To define a local address pool, use the existing <b>ip local pool</b> command. For more information on the <b>ip local pool</b> command, refer to the Cisco IOS Release 12.0 command references.
2	<code>router(config)# crypto isakmp client configuration address-pool local &lt;pool-name&gt;</code>	The local pool references the IKE configuration. To reference this local address pool in the IKE configuration, use the new <b>crypto isakmp client configuration address-pool local</b> command. For more information on the <b>crypto isakmp client configuration address-pool local</b> command, refer to the “Command Reference”.
3	<code>router(config)# crypto map &lt;map-name&gt; client configuration address &lt; initiate   respond &gt;</code>	To configure IKE Mode Configuration, use the new <b>crypto map client configuration address</b> command. For more information on the <b>crypto map client configuration address</b> command, refer to the “Command Reference”.

## Verifying Internet Key Exchange Mode Configuration

**Step 1** To verify IKE Mode Configuration is configured, you must check the router’s running configuration. Enter the **show running-config** command on the router in global configuration mode.

**Step 2** Verify IKE Mode Configuration by comparing the configuration with the example shown in “Configuration Example”.

## Configuration Example

The following example is partial output from the **show running-config** global configuration command. This configuration shows a Cisco router with IPsec that has been configured to do the following:

- Set IP addresses to clients.
- Respond to IP address requests from clients whose packets arrive on the Ethernet0 interface.

```
crypto isakmp client configuration address-pool local ire

crypto ipsec transform-set pc esp-des esp-md5-hmac

crypto dynamic-map dyn 10
set transform-set pc
match address 103

crypto map dyn client configuration address initiate
crypto map dyn client configuration address respond
crypto map dyn 10 ipsec-isakmp dynamic dyn

interface Ethernet1/0
ip address 172.21.230.34 255.255.255.224
crypto map dyn

ip local pool ire 171.72.1.1 171.72.1.254

access-list 103 permit ip host 172.21.230.34 171.72.1.0 0.0.0.255
```

## Command Reference

This section documents new commands for this feature. All other commands used to configure this feature are documented in the Cisco IOS Release 12.0 command references.

- `crypto isakmp client configuration address-pool local`
- `crypto map client configuration address`

## crypto isakmp client configuration address-pool local

To configure the IP address local pool to reference IKE on your router, use the **crypto isakmp client configuration address-pool local** global configuration command. Use the **no** form of this command to restore the default value.

**crypto isakmp client configuration address-pool local** *<pool-name>*

### Syntax Description

*pool-name* Specifies the name of a local address pool.

### Defaults

IP address local pools do not reference IKE.

### Command Modes

Global configuration.

### Command History

Release	Modification
12.0(4)XE	This command was first introduced into Cisco IOS Release 12.0(4)XE.
12.0(7)T	This command was first introduced into Cisco IOS Release 12.0(7)T.

### Usage Guidelines

None.

### Examples

The following example references IP address local pools to IKE on your router, with “ire” as the *pool-name*.

```
router(config)# crypto isakmp client configuration address-pool local ire
```

### Related Commands

Command	Description
<b>ip local pool</b>	Configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface using the <b>ip local pool</b> command. To delete an address pool, use the <b>no</b> form of this command.

## crypto map client configuration address

To configure IKE Mode Configuration on your router, use the **crypto map client-configuration address** global configuration command. Use the **no** form of this command to restore the default value.

```
crypto map <map-name> client configuration address < initiate | respond >
```

### Syntax Description

<i>map-name</i>	The name which identifies the crypto map set. This is the name assigned when the crypto map was created.
<i>initiate</i>	A keyword that indicates the router will attempt to set IP addresses for each peer.
<i>respond</i>	A keyword that indicates the router will accept requests for IP addresses from any requesting peer.

### Defaults

IKE Mode Configuration is not enabled.

### Command Modes

Global configuration.

### Command History

Release	Modification
12.0(4)XE	This command was first introduced into Cisco IOS Release 12.0(4)XE.
12.0(7)T	This command was first introduced into Cisco IOS Release 12.0(7)T.

### Usage Guidelines

At the time of this publication, this feature is an IETF draft with limited support. Therefore this feature was not designed to enable the configuration mode for every IKE connection by default.

### Examples

The following examples configure IKE Mode Configuration on your router, with “dyn” as the *map-name*.

```
router(config)# crypto map dyn client configuration address initiate
router(config)# crypto map dyn client configuration address respond
```

Related Commands

<b>Command</b>	<b>Description</b>
<b>crypto map (global configuration)</b>	Create or modify a crypto map definition and enter the crypto map configuration mode using the <b>crypto map global configuration</b> command. Use the <b>no</b> form of this command to delete a crypto map definition.