



IPsec Security Association Idle Timers

When a router running the Cisco IOS software creates an IPsec security association (SA) for a peer, resources must be allocated to maintain the SA. The SA requires both memory and several managed timers. For idle peers, these resources are wasted. If enough resources are wasted by idle peers, the router could be prevented from creating new SAs with other peers. The IPsec Security Association Idle Timers feature introduces a configurable idle timer to monitor SAs for activity, allowing SAs for idle peers to be deleted. Benefits of this feature include:

- Increased availability of resources
- Improved scalability of Cisco IOS IPsec deployments

Feature Specifications for IPsec Security Association Idle Timers

Feature History

Release	Modification
12.2(15)T	This feature was introduced.
12.3(14)T	The set security-association idle-time command was added, allowing for the configuration of an IPsec idle timer for a specified crypto map.

Supported Platforms

Cisco 1700 series access routers, Cisco 2400 series integrated access devices, Cisco 2600 series multiservice platforms, Cisco 3600 series multiservice platforms, Cisco 3700 series multiservice access routers, Cisco 7100 series VPN routers, Cisco 7200 series routers, Cisco 7400 series routers, Cisco 7500 series routers, Cisco 801–804 ISDN routers, Cisco 805 serial router, Cisco 806 broadband router, Cisco 811, Cisco 813, Cisco 820, Cisco 827 ADSL router, Cisco 828 G.SHDSL router, Cisco 8850-RPM, Cisco 950, Cisco AS5350 universal gateway, Cisco AS5400 series universal gateways, Cisco integrated communications system 7750, Cisco MC3810 series multiservice access concentrators, Cisco ubr7200, Cisco ubr900 series cable access routers

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for IPsec Security Association Idle Timers, page 2](#)
- [Information About IPsec Security Association Idle Timers, page 2](#)
- [Information About IPsec Security Association Idle Timers, page 2](#)
- [How to Configure IPsec Security Association Idle Timers, page 3](#)
- [Configuration Examples for IPsec Security Association Idle Timers, page 5](#)
- [Additional References, page 5](#)
- [Command Reference, page 7](#)

Prerequisites for IPsec Security Association Idle Timers

You must configure Internet Key Exchange (IKE) as described in the “[Configuring Internet Key Exchange Security Protocol](#)” chapter of the *Cisco IOS Security Configuration Guide*, Release 12.2.

Information About IPsec Security Association Idle Timers

To configure the IPsec Security Association Idle Timers feature, you must understand the following concepts:

- [Lifetimes for IPsec Security Associations, page 2](#)
- [IPsec Security Association Idle Timers, page 2](#)
- [Benefits of IPsec Security Association Idle Timers, page 3](#)

Lifetimes for IPsec Security Associations

The Cisco IOS software currently allows the configuration of lifetimes for IPsec SAs. Lifetimes can be configured globally or per crypto map. There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. A security association expires after the first of these lifetimes is reached.

IPsec Security Association Idle Timers

The IPsec SA idle timers are different from the global lifetimes for IPsec SAs. The expiration of the global lifetime is independent of peer activity. The IPsec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.

If the IPsec SA idle timers are not configured, only the global lifetimes for IPsec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.

**Note**

If the last IPsec SA to a given peer is deleted due to idle timer expiration, the Internet Key Exchange (IKE) SA to that peer will also be deleted.

Benefits of IPsec Security Association Idle Timers

Increased Availability of Resources

Configuring the IPsec Security Association Idle Timers feature increases the availability of resources by deleting SAs associated with idle peers.

Improved Scalability of Cisco IOS IPsec Deployments

Because the IPsec Security Association Idle Timers feature prevents the wasting of resources by idle peers, more resources will be available to create new SAs as required.

How to Configure IPsec Security Association Idle Timers

- [Configuring the IPsec SA Idle Timer Globally, page 3](#)
- [Configuring the IPsec SA Idle Timer per Crypto Map, page 4](#)

Configuring the IPsec SA Idle Timer Globally

This task configures the IPsec SA idle timer globally. The idle timer configuration will be applied to all SAs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association idle-time *seconds***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec security-association idle-time <i>seconds</i> Example: Router(config)# crypto ipsec security-association idle-time 600	Configures the IPsec SA idle timer. <ul style="list-style-type: none"> • The <i>seconds</i> argument specifies the time, in seconds, that the idle timer will allow an inactive peer to maintain an SA. Valid values for the <i>seconds</i> argument range from 60 to 86400.

Configuring the IPsec SA Idle Timer per Crypto Map

This task configures the IPsec SA idle timer for a specified crypto map. The idle timer configuration will be applied to all SAs under the specified crypto map.


Note

This configuration task was available effective with Cisco IOS Release 12.3(14)T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-number ipsec-isakmp*
4. **set security-association idle-time** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-number ipsec-isakmp</i> Example: Router(config)# crypto map test 1 ipsec-isakmp	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 4	set security-association idle-time <i>seconds</i> Example: Router(config-crypto-map)# set security-association idle-time 600	Specifies the maximum amount of time for which the current peer can be idle before the default peer is used. <ul style="list-style-type: none"> • The <i>seconds</i> argument is the number of seconds for which the current peer can be idle before the default peer is used. Valid values are 60 to 86400.

Configuration Examples for IPSec Security Association Idle Timers

- [Configuring the IPsec SA Idle Timer Globally Example, page 5](#)
- [Configuring the IPsec SA Idle Timer per Crypto Map Example, page 5](#)

Configuring the IPsec SA Idle Timer Globally Example

The following example globally configures the IPsec SA idle timer to drop SAs for inactive peers after 600 seconds:

```
crypto ipsec security-association idle-time 600
```

Configuring the IPsec SA Idle Timer per Crypto Map Example

The following example configures the IPsec SA idle timer for the crypto map named test to drop SAs for inactive peers after 600 seconds:

```
crypto map test 1 ipsec-isakmp  
set security-association idle-time 600
```

**Note**

The above configuration was not available until Cisco IOS Release 12.3(14)T.

Additional References

For additional information related to IPSec Security Association Idle Timers, see the following sections:

- [Related Documents, page 6](#)
- [Standards, page 6](#)
- [MIBs, page 6](#)
- [RFCs, page 7](#)
- [Technical Assistance, page 7](#)

Related Documents

Related Topic	Document Title
Additional information about configuring IKE	“Configuring Internet Key Exchange Security Protocol” chapter of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
Additional information about configuring global lifetimes for IPsec SAs	“Configuring IPSec Network Security” chapter of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
Additional Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.2 T

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents the new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

- [crypto ipsec security-association idle-time](#)
- [set security-association idle-time](#)

crypto ipsec security-association idle-time

To configure the IP security (IPsec) security association (SA) idle timer, use the **crypto ipsec security-association idle-time** command in global configuration mode or crypto map configuration mode. To inactivate the IPsec SA idle timer, use the **no** form of this command.

crypto ipsec security-association idle-time *seconds*

no crypto ipsec security-association idle-time *seconds*

Syntax Description	<i>seconds</i>	Time, in seconds, that the idle timer will allow an inactive peer to maintain an SA. Valid values for the seconds argument range from 60 to 86400.
---------------------------	----------------	--

Command Default IPsec SA idle timers are disabled.

Command Modes Global configuration
Crypto map configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines Use the **crypto ipsec security-association idle-time** command to configure the IPsec SA idle timer. This timer controls the amount of time that an SA will be maintained for an idle peer. Use the **crypto ipsec security-association lifetime** command to configure global lifetimes for IPsec SAs. There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. A security association expires after the first of these lifetimes is reached.

The IPsec SA idle timers are different from the global lifetimes for IPsec SAs. The expiration of the global lifetimes is independent of peer activity. The IPsec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.

If the IPsec SA idle timers are not configured with the **crypto ipsec security-association idle-time** command, only the global lifetimes for IPsec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.

If the last IPsec SA to a given peer is deleted due to idle timer expiration, the Internet Key Exchange (IKE) SA to that peer will also be deleted.

Examples The following example configures the IPsec SA idle timer to drop SAs for inactive peers after 600 seconds:

```
crypto ipsec security-association idle-time 600
```

Related Commands	Command	Description
	clear crypto sa	Deletes IPsec SAs.
	crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating IPsec SAs.

set security-association idle-time

To specify the maximum amount of time for which the current peer can be idle before the default peer is used, use the **set security-association idle-time** command in crypto map configuration mode. To disable this feature, use the **no** form of this command.

set security-association idle-time *seconds* [**default**]

no set security-association idle-time *seconds* [**default**]

Syntax Description

<i>seconds</i>	Number of seconds for which the current peer can be idle before the default peer is used. Valid values are 60 to 86400.
default	(Optional) Specifies that the next connection is directed to the default peer.

Defaults

If the **default** keyword is not specified and there is a connection timeout, the current peer remains unchanged.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is optional. Use this command if you want the default peer to be used if the current peer times out. If there is a timeout to the current peer, the connection to that peer is closed. The next time a connection is initiated, it is directed to the default peer specified in the **set peer** command.

Examples

In the following example, if the current peer is idle for 120 seconds, the default peer 10.1.1.1 (which was specified in the **set peer** command) is used for the next attempted connection:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
 set security-association idle-time 120 default
```

Related Commands

Command	Description
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2005 Cisco Systems, Inc. All rights reserved.

