



# IPsec Security Association Idle Timers

**Last Updated: June 28, 2011**

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.

With the introduction of the IPsec Security Association Idle Timers feature, there is now an idle timer that can be configured to monitor SAs for activity, allowing SAs for idle peers to be deleted and new SAs to be created as required to increase the availability of resources. This feature also improves the scalability of Cisco IOS IPsec deployments.

- [Finding Feature Information, page 1](#)
- [Prerequisites for 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 2](#)
- [Configuration Examples for IPsec Security Association Idle Timers, page 4](#)
- [Additional References, page 5](#)
- [Feature Information for IPsec Security Association Idle Timers, page 5](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

# Prerequisites for IPsec Security Association Idle Timers

You must configure Internet Key Exchange (IKE) as described in [Internet Key Exchange for IPsec VPNs](#)

## Information About IPsec Security Association Idle Timers

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

## 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.

---

## How to Configure IPsec Security Association Idle Timers

- [Configuring the IPsec SA Idle Timer Globally, page 2](#)
- [Configuring the IPsec SA Idle Timer per Crypto Map, page 3](#)

## 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
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>crypto ipsec security-association idle-time <i>seconds</i></code>  <b>Example:</b> <pre>Router(config)# crypto ipsec security-association idle-time 600</pre>	Configures the IPsec SA idle timer. <ul style="list-style-type: none"> <li>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.</li> </ul>

## 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

- `enable`
- `configure terminal`
- `crypto map map-name seq-number ipsec-isakmp`
- `set security-association idle-time seconds`

## DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>

Command or Action	Purpose
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b>  <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>crypto map map-name seq-number ipsec-isakmp</code>  <b>Example:</b>  <pre>Router(config)# crypto map test 1 ipsec-isakmp</pre>	Creates or modifies a crypto map entry and enters crypto map configuration mode.
<b>Step 4</b> <code>set security-association idle-time seconds</code>  <b>Example:</b>  <pre>Router(config-crypto-map)# set security-association idle-time 600</pre>	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"> <li>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.</li> </ul>

## Configuration Examples for IPsec Security Association Idle Timers

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

### 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

### Related Documents

Related Topic	Document Title
Additional information about configuring IKE	Internet Key Exchange for IPsec VPNs
Additional information about configuring global lifetimes for IPsec SAs	<ul style="list-style-type: none"> <li>Configuring Security for VPNs with IPsec</li> <li>IPsec Preferred Peer</li> </ul>
Additional Security commands	Cisco IOS Security Command Reference

### MIBs

MIBs	MIBs Link
None	<p>To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

### Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for IPsec Security Association Idle Timers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software

release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1** Feature Information for IPsec Security Association Idle Timers

Feature Name	Releases	Feature Information
IPsec Security Association Idle Timers	12.2(15)T 12.3(14)T	<p>With the introduction of the IPsec Security Association Idle Timers feature, there is now an idle timer that can be configured to monitor SAs for activity, allowing SAs for idle peers to be deleted and new SAs to be created as required to increase the availability of resources. This feature also improves the scalability of Cisco IOS IPsec deployments.</p> <p>This feature was introduced in Cisco IOS Release 12.2(15)T.</p> <p>In Cisco IOS Release 12.3(14)T, the <b>set security-association idle-time</b> command was added, allowing for the configuration of an IPsec idle timer for a specified crypto map.</p> <p>The following commands were introduced or modified: <b>crypto ipsec security-association idle-time</b>, <b>set security-association idle-time</b> .</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.