



Call Admission Control for IKE

First Published: May 17, 2004

Last Updated: August 20, 2007

The Call Admission Control for IKE feature describes the application of Call Admission Control (CAC) to the Internet Key Exchange (IKE) protocol in Cisco IOS. CAC limits the number of simultaneous IKE security associations (SAs) (that is, calls to CAC) that a router can establish.

History for the Call Admission Control for IKE Feature

Release	Modification
12.3(8)T	This feature was introduced.
12.2(18)SXD1	This feature was integrated into Cisco IOS Release 12.2(18)SXD1 on the Cisco 6500 and Cisco 7600.
12.4(6)T	This feature was integrated into Cisco IOS Release 12.4(6)T. The ability to configure a limit on the number of in-negotiation IKE connections was added only to this and subsequent T-train releases.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA on the Cisco 7600. The in-negotiation IKE connection feature was not added to this SRA release.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH. The in-negotiation IKE connection feature was not added to this SXH release.

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 Call Admission Control for IKE, page 2](#)
- [Information About Call Admission Control for IKE, page 2](#)



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2004, 2006 Cisco Systems, Inc. All rights reserved.

- [How to Configure Call Admission Control for IKE, page 3](#)
- [Verifying the Call Admission Control for IKE Configuration, page 5](#)
- [Configuration Examples for Call Admission Control for IKE, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)

Prerequisites for Call Admission Control for IKE

- Configure IKE on the router. Refer to the *Cisco IOS Security Configuration Guide*, Release 12.3.

Information About Call Admission Control for IKE

To configure CAC for IKE, you need to understand the following concepts:

- [IKE Session, page 2](#)
- [Security Association Limit, page 2](#)
- [System Resource Usage, page 3](#)

IKE Session

There are two ways to limit the number of IKE SAs that a router can establish to or from another router:

- Configure the absolute IKE SA limit by entering the **crypto call admission limit** command. The router drops new IKE SA requests when the value has been reached.
- Configure the system resource limit by entering the **call admission limit** command. The router drops new IKE SA requests when the specified percentage of system resources is being used.

For information about using these commands, see the “[Command Reference](#)” section on [page 8](#).

CAC is applied only to new SAs (that is, when an SA does not already exist between the peers). Every effort is made to preserve existing SAs. Only new SA requests will ever be denied due to a lack of system resources or because the configured IKE SA limit has been reached.

Security Association Limit

An SA is a description of how two or more entities will utilize security services to communicate securely on behalf of a particular data flow. IKE requires and uses SAs to identify the parameters of its connections. IKE can negotiate and establish its own SA. An IKE SA is used by IKE only, and it is bidirectional. An IKE SA cannot limit IPsec.

IKE drops SA requests based on a user-configured SA limit. To configure an IKE SA limit, enter the **crypto call admission limit** command. When there is a new SA request from a peer router, IKE determines if the number of active IKE SAs plus the number of SAs being negotiated meets or exceeds the configured SA limit. If the number is greater than or equal to the limit, the new SA request is rejected and a syslog is generated. This log contains the source destination IP address of the SA request.

Limit on Number of In-negotiation IKE Connections

Effective with Cisco IOS Release 12.4(6)T, a limit on the number of in-negotiation IKE connections can be configured. This type of IKE connection represents either an aggressive mode IKE SA or a main mode IKE SA prior to its authentication and actual establishment.

Using the **crypto call admission limit ike in-negotiation-sa** *{number}* command allows the configured number of in-negotiation IKE SAs to start negotiation without contributing to the maximum number of IKE SAs allowed.

System Resource Usage

CAC polls a global resource monitor so that IKE knows when the router is running short of CPU cycles or memory buffers. You can configure a resource limit, from 1 to 100, that represents a percentage of system resources. When that percentage of the system resources is being used, IKE drops (will not accept new) SA requests. For example, if you specify a resource limit of 90 percent, IKE stops accepting SA requests when 90 percent of the system resources is being used. To configure the system resource usage, enter the **call admission control** command.

How to Configure Call Admission Control for IKE

This section contains the following procedures:

- [Configure the IKE Security Association Limit, page 3](#) (optional)
- [Configure the System Resource Limit, page 4](#) (optional)



Note

You must perform one of the procedures.

Configure the IKE Security Association Limit

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto call admission limit {ike {in-negotiation-sa *number* | sa *number* } }**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>crypto call admission limit {ike {in-negotiation-sa number sa number}}</p> <p>Example: Router(config)# crypto call admission limit ike sa 25</p>	<p>Specifies the maximum number of IKE SAs that the router can establish before IKE begins rejecting new SA requests.</p> <p>Note An ISAKMP connection needs to be built in two directions. If you have 500 spokes in your network, you should set this value at a minimum of 1000 (500 x 2).</p>
Step 4	<p>exit</p> <p>Example: Router(config)# exit</p>	<p>Returns to privileged EXEC mode.</p>

Configure the System Resource Limit

SUMMARY STEPS

- enable
- configure terminal
- call admission limit *percent*
- exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	call admission limit percent Example: Router(config)# call admission limit 90	Instructs IKE to stop accepting new SA requests (that is, calls for CAC) when the specified percentage of system resources is being used.
Step 4	exit Example: Router(config)# exit	Returns to privileged EXEC mode.

Verifying the Call Admission Control for IKE Configuration

To verify the CAC for IKE configuration, perform the following steps.

SUMMARY STEPS

1. show call admission statistics
2. show crypto call admission statistics

DETAILED STEPS

**Note**

For detailed field descriptions of the command output, see the [“Command Reference” section on page 8](#).

Step 1 show call admission statistics

Use this command to monitor the global CAC configuration parameters and the behavior of CAC.

```
Router# show call admission statistics
```

```
Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

Step 2 show crypto call admission statistics

Use this command to monitor Crypto CAC statistics.

```
Router# show crypto call admission statistics
```

```
-----
Crypto Call Admission Control Statistics
-----
System Resource Limit: 0   Max IKE SAs 0
Total IKE SA Count:    0   active:      0   negotiating: 0
Incoming IKE Requests: 0   accepted:   0   rejected:   0
Outgoing IKE Requests: 0   accepted:   0   rejected:   0
Rejected IKE Requests: 0   rsrc low:   0   SA limit:   0
-----
```

Configuration Examples for Call Admission Control for IKE

This section provides the following configuration examples:

- [Configuring the IKE Security Association Limit: Example, page 6](#)
- [Configuring the System Resource Limit: Example, page 6](#)

Configuring the IKE Security Association Limit: Example

The following example shows how to specify that there can be a maximum of 25 SAs before IKE starts rejecting new SA requests:

```
Router(config)# crypto call admission limit ike sa 25
```

Configuring the System Resource Limit: Example

The following example shows how to specify that IKE should drop SA requests when 90 percent of system resources are being used:

```
Router(config)# call admission limit 90
```

Additional References

The following sections provide references related to Call Admission Control for IKE.

Related Documents

Related Topic	Document Title
IKE	<ul style="list-style-type: none"> • Cisco IOS Security Command Reference, Release 12.3T • Cisco IOS Security Configuration Guide, Release 12.3

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC #2409	<i>The Internet Key Exchange</i>

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of 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/techsupport

Command Reference

This section documents modified commands only.

- [call admission limit](#)
- [clear crypto call admission statistics](#)
- [crypto call admission limit](#)
- [show call admission statistics](#)
- [show crypto call admission statistics](#)

call admission limit

To instruct Internet Key Exchange (IKE) to drop security association (SA) requests (that is, calls for Call Admission Control [CAC]) when a specified percentage of system resources is being consumed, use the **call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

call admission limit *percent*

no call admission limit *percent*

Syntax Description	<i>percent</i>	Percentage of the system resources that, when used, causes IKE to stop accepting new SA requests. Valid values are 1 to 100.
---------------------------	----------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.	
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.	
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.	

Usage Guidelines	It is recommended that initially you specify a value of 90. You will have to alter the value depending on the network topology, the capabilities of the router, and the traffic patterns.
-------------------------	---

Examples	The following example causes IKE to drop calls when 90 percent of system resources are being used:
-----------------	--

```
Router(config)# call admission limit 90
```

Related Commands	Command	Description
	show call admission statistics	Monitors the global CAC configuration parameters and the behavior of CAC.

clear crypto call admission statistics

To clear the counters that track the number of accepted and rejected Internet Key Exchange (IKE) requests, use the **call admission limit** command in global configuration mode.

clear crypto call admission statistics

Syntax Description This command has no arguments or keywords.

Command Modes Global configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples The following example sets to zero the number of accepted and rejected IKE requests:

```
Router(config)# clear crypto call admission statistics
```

Related Commands	Command	Description
	show crypto call admission statistics	Monitors Crypto CAC statistics.

crypto call admission limit

To specify the maximum number of Internet Key Exchange (IKE) security associations (SAs) that the router can establish before IKE begins rejecting new SA requests, use the **crypto call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
crypto call admission limit {ike {in-negotiation-sa number | sa number}}
```

```
no crypto call admission limit {ike {in-negotiation-sa number | sa number}}
```

Syntax Description

ike	Configures the crypto Call Admission Control active IKE SA limit.
in-negotiation-sa number	Maximum number of in-negotiation IKE SAs allowed. <ul style="list-style-type: none"> <i>number</i>—Value = 10 through 99999
sa number	Number of active IKE SAs allowed on the router. <ul style="list-style-type: none"> <i>number</i>—Value = 0 through 99999

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1 on the Cisco 6500 and Cisco 7600.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T, and the in-negotiation-sa keyword and <i>number</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA on the Cisco 7600. The in-negotiation-sa keyword and <i>number</i> argument were not added to this release.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The in-negotiation-sa keyword and <i>number</i> argument were not added to this release.

Usage Guidelines

Use this command to limit the number of IKE SAs permitted to or from a router. By limiting the amount of dynamic tunnels that can be created to the router, you can prevent the router from being overwhelmed if it is suddenly inundated with IKE SA requests. The ideal limit depends on the particular platform, the network topology, the application, and traffic patterns. When the specified limit is reached, IKE rejects all new SA requests. If you specify an IKE SA limit that is less than the current number of active IKE SAs, a warning is displayed, but SAs are not terminated. New SA requests are rejected until the active SA count is below the configured limit.

Examples

The following example specifies that there can be a maximum of 50 IKE SAs before IKE begins rejecting new SA requests.

```
Router(config)# crypto call admission limit ike sa 50
```

The following example specifies that there can be a maximum of 100 in-negotiation IKE SAs before IKE begins rejecting new SA requests.

```
Router (config)# crypto call admission limit ike in-negotiation-sa 100
```

Related Commands

Command	Description
show crypto call admission statistics	Monitors Crypto CAC statistics.

show call admission statistics

To monitor the global Call Admission Control (CAC) configuration parameters and the behavior of CAC, use the **show call admission statistics** command in user EXEC or privileged EXEC mode.

show call admission statistics

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples The following is sample output from the **show call admission statistics** command:

```
Router# show call admission statistics

Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

[Table 1](#) describes the significant fields shown in the display.

Table 1 *show call admission statistics* Field Descriptions

Field	Description
Total call admission charges	Percentage of system resources being charged to the system. If you configured a resource limit, SA requests are dropped when this field is equal to that limit.
limit	Maximum allowed number of total call admission charges. Valid values are 0 to 100000.
Total calls rejected	Number of SA requests that were not accepted.
accepted	Number of SA requests that were accepted.
unscaled	Not related to IKE. This value always is 0.

Related Commands	Command	Description
	call admission limit	Instructs IKE to drop calls when a specified percentage of system resources are being consumed.
	crypto call admission limit	Specifies the maximum number of IKE SA requests allowed before IKE begins rejecting new IKE SA requests.

show crypto call admission statistics

To monitor Crypto Call Admission Control (CAC) statistics, use the **show crypto call admission statistics** command in user EXEC or privileged EXEC mode.

show crypto call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Enter this command to display information about the Crypto CAC configuration parameters and their history, including statistics regarding the current security association (SA) count, SAs being negotiated, total new SA requests, the number of Internet Key Exchange (IKE) SA requests accepted and rejected, and details regarding why requests were rejected.

Examples

The following example shows sample output from the **show crypto call admission statistics** command:

```
Router# show crypto call admission statistics

Crypto Call Admission Control Statistics
-----
System Resource Limit: 0      Max IKE SAs 0
Total IKE SA Count:      0      active:      0      negotiating: 0
Incoming IKE Requests: 0      accepted:    0      rejected:    0
Outgoing IKE Requests: 0      accepted:    0      rejected:    0
Rejected IKE Requests: 0      rsrc low:   0      SA limit:   0
```

[Table 2](#) describes the significant fields shown in the display.

Table 2 *show crypto call admission statistics Field Descriptions*

Field	Description
System resource limit	Percentage of system resources that the router can be using before IKE starts dropping all SA requests.
Max IKE SAs	Number of active IKE SA requests allowed on the router.
Total IKE SA Count	Number of IKE SAs.

Table 2 *show crypto call admission statistics Field Descriptions (continued)*

Field	Description
active	Number of active SAs.
negotiating	Number of SA requests being negotiated.
Incoming IKE Requests	Number of incoming IKE SA requests.
Incoming IKE Requests accepted	Number of accepted IKE SA requests.
Incoming IKE Requests rejected	Number of rejected incoming IKE SA requests.
Outgoing IKE Requests	Number of outgoing IKE SA requests.
Outgoing IKE requests accepted	Number of accepted outgoing IKE SA requests.
Outgoing IKE requests rejected	Number of rejected outgoing IKE SA requests.
Rejected IKE Requests	Number of IKE requests that were rejected.
rsrc low	Number of IKE requests that were rejected because system resources were low or the preconfigured system resource limit was exceeded.
SA limit	Number of IKE SA requests that were rejected because the SA limit has been reached.

Related Commands

Command	Description
clear crypto call admission statistics	Clears the counters that track the number of accepted and rejected IKE SA requests.

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)

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

© 2004, 2006 Cisco Systems, Inc. All rights reserved.

