

Call Admission Control for IKE

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 software. CAC limits the number of simultaneous IKE and IPsec security associations (SAs) that is, calls to CAC that a router can establish.

- Prerequisites for Call Admission Control for IKE, on page 1
- Information About Call Admission Control for IKE, on page 1
- How to Configure Call Admission Control for IKE, on page 3
- Configuration Examples for Call Admission Control for IKE, on page 6
- Additional References, on page 7
- Feature Information for Call Admission Control for IKE, on page 8

Prerequisites for Call Admission Control for IKE

- Configure IKE on the device.

Information About Call Admission Control for IKE

IKE Session

There are two ways to limit the number of Internet Key Exchange (IKE) security associations (SAs) that a device can establish to or from another device:

- Configure the absolute IKE SA limit by entering the **crypto call admission limit** command. The device drops new IKE SA requests when the configured limit is reached.
- Configure the system resource limit by entering the **call admission limit** command. The device drops new IKE SA requests when the level of system resources that are configured in the unit of charge is being used.

Call Admission Control (CAC) is applied only to new SAs (that is, when an SA does not already exist between peers). Every effort is made to preserve existing SAs. New SA requests are denied due to a lack of system resources or because the configured IKE SA limit is 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 whether 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.

The **ipsec sa** *number* and **ike sa** *number* keyword and argument pairs in the **crypto call admission limit**command set the limit for the number of established IPsec SAs and IKE SAs.

Limit on Number of In-Negotiation IKE Connections

You can limit the number of in-negotiation IKE connections that can be configured on a device based on your Cisco release. 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. The default value for maximum in-negotiation CAC for IKEv2 is 40.

You can use the **crypto call admission limit ike in-negotiation-sa** *number* command to specify the maximum number of Internet Key Exchange (IKE) and IPsec security associations (SAs) that the device can establish before IKE begins rejecting the new SA requests.

The **all in-negotiation-sa** *number* and **ike in-negotiation-sa** *number* keyword and argument pairs in the **crypto call admission limit** command limit all SAs in negotiation and IKE SAs in negotiation.

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 limit, in the range 1 to 100000, that represents the level of system resource usage in system resource usage units. When that level of resources is being used, IKE drops (will not accept new) SA requests. To configure the system resource usage limit, enter the **call admission limit** command.

For each incoming new SA request, the current load on the router is converted into a numerical value, representing the system resource usage level, and is compared to the resource limit set by the **call admission limit** command. If the current load is more than the configured resource limit, IKE drops the new SA request. Load on the router includes active SAs, CPU usage, and SA requests being considered.

The **call admission load** command configures a multiplier value from 0 to 1000 that represents a scaling factor for current system resource usage and a load metric poll rate of 1 to 32 seconds. The numerical value for the system resource usage level is calculated by the formula (scaling factor * current system resource usage) / 100. It is recommended that the **call admission load** command not be used unless advised by a Cisco Technical Assistance Center (TAC) engineer.

How to Configure Call Admission Control for IKE

Configuring the IKE Security Association Limit

Perform this task to configure the absolute IKE SA limit. The router drops new IKE SA requests when the limit has been reached.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	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	**crypto call admission limit** {**all in-negotiation-sa** *number*	**ipsec sa** *number*	**ike** {**in-negotiation-sa** *number*	**sa** *number*}} **Example:** `Router(config)# crypto call admission limit ike sa 25`	Specifies the maximum number of IKE SAs or total SAs in negotiation or the maximum IKE SAs or IPsec SAs that can be established before IKE begins rejecting new SA requests. The recommended CAC value for IKEv1 is 40.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the IKEv2 Security Association Limit

Perform this task to configure the absolute IKEv2 SA limit. The router drops new IKE SA requests when the limit has been reached.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ikev2 limit** {**max-in-negotiation-sa limit** *number* | **max-sa limit** *number*}
4. **exit**

DETAILED STEPS

Procedure

	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	**crypto ikev2 limit** {**max-in-negotiation-sa limit** *number* | **max-sa limit** *number*} **Example:** `Router(config)# crypto ikev2 limit max-in-negotation-sa 5000`	Enables call admission control as follows: • max-in-negotation-sa limit: Limits the total number of in-negotiation IKEv2 SAs on the node. • max-sa limit: Limits the total number of IKEv2 SAs on the node.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the System Resource Limit

Perform this task to configure the system resource limit. The router drops new IKE SA requests when the level of system resources that are configured in the unit of charge is being used.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **call admission limit** *charge*
4. **exit**

DETAILED STEPS

Procedure

	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** *charge* **Example:** `Router(config)# call admission limit 1000`	Sets the level of the system resources that, when used, causes IKE to stop accepting new SA requests. • *charge* --Valid values are 1 to 100000.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and 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

Procedure

Step 1 **show call admission statistics**

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

Example:

```
Router# show call admission statistics
Total Call admission charges: 82, limit 1000
Total calls rejected 1430, accepted 0
Load metric: charge 82, unscaled 82%
```

Step 2 **show crypto call admission statistics**

Use this command to monitor crypto CAC statistics.

Example:

```
Router# show crypto call admission statistics
----------------------------------------------------------------------
               Crypto Call Admission Control Statistics
----------------------------------------------------------------------
System Resource Limit:      111 Max IKE SAs:     0 Max in nego:  1000
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 Active SA limit: 0
                                                   In-neg SA limit: 0
IKE packets dropped at dispatch:        0
Max IPSEC SAs:   111
Total IPSEC SA Count:           0 active:          0 negotiating:     0
Incoming IPSEC Requests:        0 accepted:        0 rejected:        0
Outgoing IPSEC Requests:        0 accepted:        0 rejected:        0
Phase1.5 SAs under negotiation:         0
```

Configuration Examples for Call Admission Control for IKE

Example Configuring the IKE Security Association Limit

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

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

Example Configuring the System Resource Limit

The following example shows how to specify that IKE should drop SA requests when the level of system resources that are configured in the unit of charge reaches 9000:

```
Router(config)# call admission limit 9000
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring IKE	Configuring Internet Key Exchange for IPsec VPNs
IKE commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
RFC 2409	*The Internet Key Exchange*

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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Call Admission Control for IKE

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. An account on Cisco.com is not required.

Table 1: Feature Information for Call Admission Control for IKE

Feature Name	Releases	Feature Information
Call Admission Control for IKE	12.3(8)T 12.2(18)SXD1 12.4(6)T 12.2(33)SRA 12.2(33)SXH	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 software. In Cisco IOS Release 12.3(8)T, this feature was introduced. This feature was integrated into Cisco IOS Release 12.2(18)SXD1 and implemented on the Cisco 6500 and Cisco 7600 routers. In Cisco IOS Release 12.4(6)T, the ability to configure a limit on the number of in-negotiation IKE connections was added. The following sections provide information about this feature: The following commands were introduced or modified: **call admission limit**, **clear crypto call admission statistics**, **crypto call admission limit**, **show call admission statistics**, **show crypto call admission statistics**.
IKEv1 Hardening	15.1(3)T	The IKEv1 hardening feature describes the enhancements made to the Call Admission Control (CAC) for IKE feature. In Cisco IOS Release 15.1(3)T, this feature was introduced. The following sections provide information about this feature: The following commands were introduced or modified: **crypto call admission limit**, **show crypto call admission statistics**.