



## DATA SHEET

# CISCO IOS CERTIFICATION AUTHORITY SERVER PERFORMANCE, SCALABILITY, AND FAULT TOLERANCE

## INTRODUCTION

Cisco first introduced Cisco IOS® Certification Authority (CA) Server in Cisco IOS Software Release 12.3(4), and now supports this feature on all hardware that runs security images\*: Cisco 800 through 7400 Series Routers.

Cisco IOS CA Server performance is not a gating factor for IPsec network availability; however, deploying the right router for CA server applications can optimize performance and reliability for digital certificate operations, such as certificate enrollment and Certificate Revocation List (CRL) publishing and checking. Deploying the best router as the Cisco IOS CA Server can minimize the cost and maximize network performance and availability.

This document offers guidelines for selecting the appropriate router platform, as well as insight into the criteria that influences the selection of the most appropriate model of router to issue digital certificates for a network security infrastructure.

## FACTORS AFFECTING SELECTION

Following is a list of key issues that impact selection of an appropriate router for Public Key Infrastructure (PKI) CA Server support:

- **Key length**

- Larger RSA cryptographic keys are more computationally intensive, and will thus drive CPU utilization to a greater level for a longer period of time. A long enrollment queue can develop when a large keypair is used and the device receives a large number of certificate enrollment/re-enrollment requests in a short period of time. As a result, certain devices may encounter a longer wait than usual to receive their certificate.

- **Duration of certificate validity**

- Short certificate-validity periods (several days to a few weeks), particularly in large networks that have many devices enrolled with the CA, will cause higher loads on the Cisco IOS CA device. Short certificate validity periods causes heavy loads because the devices must enroll more frequently in a given time period, causing greater enrollment activity on the Cisco IOS CA. This is particularly relevant in networks where Cisco IOS CA functionality is combined with the IPsec head-end in the same device.

- **Maximum simultaneous enrollments**

- Large network deployments or frequent certificate re-enrollments may lead to circumstances in which a large number of devices enrolls simultaneously. Low-performance routers, including the Cisco 800, 1700, and 2600 Series, may experience long wait times for device enrollment/re-enrollment as the enrollment queue lengthens on the Cisco IOS CA.

- **CRL Location**

- Routers that support Cisco IOS Software offer excellent packet-forwarding and service performance, but the Flash file system on routers is not a focus for high performance during hardware platform development. If the Cisco IOS CA is storing the database on the local Flash, it will reduce the CA performance to a degree, as the individual database files must be written to the filesystem before the next certificate enrollment in the queue may be serviced.

\* Security images are frequently denoted with a "k9" in the image name.

- **CRL Query Rate**

- Traditional hub-and-spoke networks commonly employ CRL checking on the IPsec head-end. However, a network that checks CRLs on every IPsec node will impose a greater load on the Cisco IOS CA if the Cisco IOS CA router serves the CRL Distribution Point (CDP). This will only increase the router's load if a very short CRL validity period is used or sites must query the CRL every time an IPsec tunnel is negotiated. By default, Cisco IOS Software caches CRLs when a router retrieves them, so the current CRL only needs to be downloaded once. It may be examined any time a certificate is presented, until the CRL expires.

## **PKI ACTIVITY EXAMPLES**

The following example will illustrate activity that burdens the Cisco IOS CA Server. The basic recommended values for certificate enrollment on a Cisco IOS CA are a one-year certificate lifetime and a seven-day CRL lifetime. The Cisco 831 Router takes between five and ten seconds to sign a certificate enrollment request with 1024 bit keys. A network with one hundred remote sites will therefore require between eight and sixteen minutes of actual CPU time per year to process enrollments. Signing a CRL will take roughly the same amount of time, so a CRL per week amounts to (52 weeks \* 5–10 seconds) 4–8 minutes of CPU time.

## **SELECTING THE RIGHT ROUTER FOR A CISCO IOS CA**

Router selection and Cisco IOS CA Server deployment can be categorized based on the network size:

- **Small Businesses: up to twenty-five peers; cost is critical**

- Small IPsec networks can likely integrate Cisco IOS CA functionality in the IPsec head end device. However, if the VPN imposes a heavy load on the router by carrying a high traffic volume, or if frequent certificate enrollment/re-enrollment or a large keypair will heavily load the router, a dedicated Cisco IOS CA router offers a better solution. A Cisco 800, 1700, or 1800 Series Router will be adequate if a dedicated router is used. Cisco 800 and 1700 Series Routers do not offer removable non-volatile storage such as Compactflash or Flash disk/Flash card. A manual or scripted backup mechanism will be required to back up the certificate database if the Cisco IOS CA database is in the router's Flash. The Cisco 1800 Series offers removable USB storage as well as compact Flash memory, offering a simple mechanism to transfer the Cisco IOS CA database to a different device in the event a device replacement or upgrade is required.

- **Medium-sized network or small enterprise: twenty-five to hundred IPsec nodes**

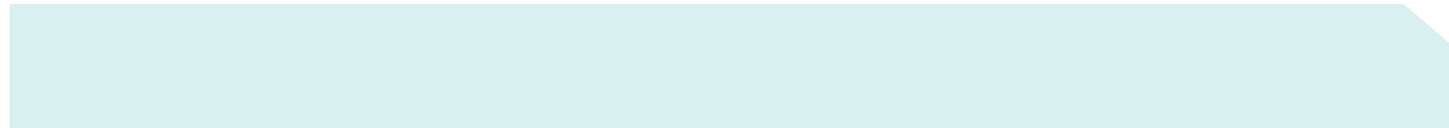
- Medium-sized IPsec networks can integrate Cisco IOS CA functionality in the IPsec head end only if the IPsec traffic volume will be of low volume and will not impose a substantial load on the router. A dedicated router is advisable for most medium-sized networks. Cisco recommends a Cisco 1700 or 1800 Series Router for networks with lower-performance PKI requirements. Conversely, Cisco 2600 and 2800 Series Routers offer sufficient performance for more demanding networks with frequent re-enrollment, large keypairs, and larger numbers of remote-site devices.
- Cisco 1800, 2800, and 3800 Series Integrated Services Routers provide a simple solution to the need for "portable" Cisco IOS CA database if the database is not stored on an external server: removable USB storage and compact Flash storage.

- **Large Enterprise or Service Provider**

- Large or busy networks using IPsec VPN technology require maximum performance, scalability, and availability. PKI operations may periodically impose fairly heavy loads on a CA, depending on enrollment cycles and deployment schedules. Even in these cases, a Cisco 2691 Router or Cisco 2800 Series will address requirements for Cisco IOS CA support in a large IPsec VPN. While a Cisco 3800 or 7200 Series will work very well, only the largest VPN networks require such advanced functionality. Large networks should strongly consider maintaining a spare router for backup in the event the primary router must be replaced.

## **CPU IMPACT OF CERTIFICATE ENROLLMENT AND CRL CHECKING**

Each certificate enrollment will drive Cisco IOS CA CPU activity to a high level for a short period of time. The length of time for high CPU varies depending on the length of the key and the speed of the processor. A lower-performance platform such as the Cisco 831 Router will exhibit longer periods of high CPU per certificate enrollment than a higher-performance platform such as a Cisco 2811 Router.



Cisco IOS CA can support CRL distribution on the Cisco IOS CA router; alternatively, an external http server can be used to eliminate load on the Cisco IOS CA router. An external CDP server improves network reliability because a network that retrieves CRLs from an external CDP server can still verify certificates, regardless of the status of the Cisco IOS CA Router. In this case, no impact would be observed on new tunnel establishment.

If the Cisco IOS CA is used as the CDP, it is important that the router have sufficient processing bandwidth to distribute CRLs if tunnel negotiation requires that the certificates' revocation status is verified. If the IPsec peers require CRLs before opening tunnels and are unable to retrieve the needed CRLs, tunnel negotiation will fail. CRL generation and distribution does not consume as much CPU time as certificate enrollment.

## **STORAGE CONSUMPTION OF CERTIFICATE AND CRL DATABASE**

The amount of storage that Cisco IOS CA consumes is dependent on the database logging level configured in the CA server. Setting the database level to "complete" consumes a fairly large amount of space, and using the "minimum" database setting makes troubleshooting difficult due to the small amount of relevant information in the database. "Names" database level is therefore the most efficient.

With a "names" database, the CA server will create a small file for each client enrolled with the CA server, roughly 100 bytes, depending on the amount of information included in the enrollment request. The "empty" CRL (before any revocations) is about 4 KB. The CRL grows by 20–30 bytes for each revoked certificate. The exported public and private key files for 512 byte keys are less than 1 KB each, but file size depends on the key length. The PEM-encoded public and private key files are roughly 300 bytes larger than the key length.

The Flash filesystem is inefficient enough that using a router's internal Flash memory resources allocates a large volume of storage space for small files. Testing has shown that creating a subdirectory in the Flash for CA Server database storage helps to address this issue to some degree, especially if more than 15–20 files will be stored in Flash.

## **HIGH AVAILABILITY**

Certificate enrollment/re-enrollment and CRL checking (if the IOS CA is the CDP) are the only circumstances that the network requires communication between IPsec end nodes and the CA server. Once a tunnel is established, the IPsec end nodes do not require any interaction with the CA Server.

Routers enrolling with the IOS CA will periodically retry enrollment if they are unable to contact the IOS CA. This means that the CA server can be offline periodically for short periods without substantial impact to the network, only new-deployed sites will not be able to establish connectivity. Furthermore, routers that are already enrolled and are attempting re-enrollment should be configured to automatically re-enroll before their existing certificate expires. If their first attempt fails, the router will continue attempting enrollment at a periodic interval until they can contact the CA Server and the enrollment succeeds.

CRL's are more sensitive to unavailability of the CRL Distribution point. If IPsec peers retrieve CRLs from the IOS CA and the IOS CA is unavailable, tunnel negotiation will fail if CRL checking is required. The same issue is true if an external server is used as the CDP. Once tunnels are established, the IOS CA does not need to be available for tunnel maintenance, unless tunnels peers will check CRLs when IPsec or IKE SAs are re-established.

The IOS CA does not presently include any high availability features such as hot standby or failover. However, a similar capability can be accommodated using external equipment to monitor the primary IOS CA and activate a secondary, "warm-standby" device in the event that the primary IOS CA becomes unavailable. The standby device would be configured identically to the primary device, with the public and private keys from the primary device installed in the secondary. Ideally, the database would be stored on an external server, so when the standby device is activated, it would be able to check the serial number file and work with the existing CRL. If the monitor system loses contact with the primary IOS CA, the upstream switch port for the primary would be shut down and the standby's port would be activated. The standby would then continue distributing CRLs and servicing enrollment/re-enrollment requests.

## CONCLUSION

Cisco IOS CA selection depends on a number of conditions that must be considered to properly select the appropriate platform for a network's IOS CA. Fortunately, the key material and certificate database is fairly portable. In the event that a network outgrows the existing CA or a router proves to be inadequate for IOS CA requirements, the router can be replaced with a router offering higher performance.

## FOR MORE INFORMATION

- PKI Deployment Guide: [http://www.cisco.com/en/US/tech/tk1132/technologies\\_white\\_paper09186a00800e79cb.shtml](http://www.cisco.com/en/US/tech/tk1132/technologies_white_paper09186a00800e79cb.shtml)
- Cisco IOS CA Backup and Restore: [http://www.cisco.com/en/US/products/ps6540/products\\_configuration\\_example09186a00807f98ff.shtml](http://www.cisco.com/en/US/products/ps6540/products_configuration_example09186a00807f98ff.shtml)



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, BPX, 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, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, 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. (0701R)