

Certificate Server: Simplifying IPsec VPN Deployment with Digital Certificates

Introduction

IPsec Virtual Private Networks (VPNs) are realizing their potential to offer a high performance, functional alternative to costly dial- and leased-line based WANs. Small VPN deployments are fairly easy to manage in terms of the generation and management of suitable encryption keys and identity information; however, it becomes more difficult to generate and track unique cryptography information as a VPN grows. Larger scale VPNs require a more scalable and secure infrastructure to ease deployment and management burdens. Public Key Infrastructure (PKI) responds to this requirement for scalability and security, but presents its own challenges of complexity and cost. The integrated Certificate Server in Cisco IOS[®] Software addresses such challenges with a simple, scalable, easy-to-manage certification authority, which is built into the same hardware supporting the IPsec VPN.

IPsec and PKI Technology

IPsec networks employ encryption and authentication mechanisms to ensure data confidentiality and integrity. These cryptography mechanisms, such as the DES, 3DES, and AES encryption algorithms and SHA-1 and MD5 hash algorithms for data signing, use key information derived mathematically from information distributed to the devices and users that will be communicating over encrypted channels.

Small deployments can easily employ shared secrets as the key information. Shared secrets are effectively simple passwords configured on both ends of the secured connection. As encrypted networks grow more complex, the task of managing unique shared secrets grows more complex with the addition of every encryption peer, particularly in networks employing “full mesh” cryptographic peering.

PKI reduces the workload necessary to manage key information by automating the distribution of cryptographic material. Unfortunately, a PKI is frequently expensive to purchase and deploy, which can potentially require the addition of support staff. Commercial PKIs frequently offer substantially more capability and functionality than many customers require, making it difficult to justify the high cost of the technology.

Cisco IOS Software Simplifies PKI Deployment

Cisco IOS Software Release 12.3(4)T introduced a Certificate Server that offers functionality for issuing digital certificates for router-based network security. This new feature allows a Cisco IOS Software router to issue and revoke x.509 digital certificates, easily resolving the issue of requiring a costly and difficult-to-administer third-party certification authority. The initial phase of the Certificate Server fulfills the need to issue certificates to other Cisco IOS



Software routers for IPsec VPNs and other encryption and identity services in a single-level hierarchy.

Certificate Server supports the distribution of Certificate Revocation Lists (CRL) via the Cisco IOS Software SCEP server for smaller networks. For larger networks, an external server for CRL distribution is encouraged to reduce load on the Certificate Server router. The Certificate Server can issue a large volume of certificates; the X.509 serial-number field is the only limitation for the maximum, offering the capability to issue millions of certificates. Varying platforms will process different numbers of certificate requests over a given period of time, depending on router load, processor speed, and memory availability. Certificate Validation does not cause additional load on the Certificate Server router besides responding to CRL retrieval requests.

Benefits of Certificate Server

The Certificate Server reduces the cost and simplifies the deployment for IPsec VPNs. Rather than purchasing digital certificates from an online vendor (Verisign), or installing a certification authority (Entrust, Microsoft), Cisco IOS Software offers an integrated solution at no additional cost.

Benefit	Feature
Cost reduction	Certification Authority is integrated in the network infrastructure, so there is no additional hardware or software to purchase
Deployment simplification	Easy to configure and deploy No long-term learning process necessary to understand system architecture
Integrated functionality	Interoperates directly with the VPN and security functions in Cisco IOS Software network devices
Improved security	Secure, scalable management of encryption key information for data communications

The Certificate Server offers a simple deployment procedure to make the server available in a short time. No additional hardware is required beyond the router at a central site in small deployments. Larger deployments may demand a separate router for certificate enrollment, and a web server for certificate revocation distribution.

Security

Digital certificates inherently enhance network encryption security, because they are so difficult to compromise, and their automated, network-based revocation systems, which render a certificate useless in the event the certificate's validity is terminated.

The Certificate Server offers a secure facility for deploying encryption key information through compliance with the x.509v3 standards for digital certificate generation and distribution. Clients may enroll online via the HTTP-based SCEP standard, or offline via manual cut-and-paste or TFTP for greater security where the Certificate Server is not available on the public network. The Certificate Server may be configured to automatically grant all certificate requests, or manual certificate request approval can be configured for greater control over certificate issuing.

The Certificate Server's private keys are protected in the router's private NVRAM, an area that cannot be viewed by any user with access to the device.

Cisco IOS Software Support for Certificate Server

The Certificate Server was first introduced in Cisco IOS Software Release 12.3(4)T. It is offered in all images with IPsec encryption capability on all routers that support Release 12.3(4)T.

Routers	Software
Cisco 800 Series	Cisco IOS Software Release 12.3(4)T
Cisco ubr900 Series	
Cisco 1700 Series	
Cisco 2600XM Series	
Cisco 2691	
Cisco 3600 Series	
Cisco 3700 Series	
Cisco AS5x00 Products	
Cisco 7200 Series	
Cisco 7400 Series	



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe