Data Sheet

Cisco SCA 11000 Series
Secure Content Accelerator

Cisco SCA 11000 Series secure content accelerators are device-based solutions that expand the transaction capacity of any Web site by offloading the processor-intensive tasks related to Secure Sockets Layer (SSL) traffic. Moving the SSL security processing from a Web server to the Cisco SCA 11000 Series liberates capacity of the Web servers to focus on processing "Webified" applications and databases much more efficiently, thereby accelerating the entire site.

As more SSL traffic is introduced in the data center, the ability to perform local load balancing across back-end servers is hindered. In addition, intrusion detection systems (IDSs) are blinded and are unaware of the activity occurring between the remote client and the back-end server. These problems occur because the entire Layer 5 information is encrypted. Using Cisco's SSL products, network administrators and networking engineers can reclaim this control and improve site security by offloading the SSL traffic and de-encrypting it before it gets to the back-end server. The de-encrypted traffic can be switched to an IDS system for monitoring or directly load balanced across several back-end severs.

The Cisco SCA 11000 is a component of Cisco's family of solutions for SSL acceleration, which also includes integrated SSL processing modules for the Cisco CSS 11500 Content Services Switch and the Cisco 6500 Catalyst® Series switches and Cisco 7600 Internet routers. Cisco's SSL product offerings provide Web sites of all sizes the performance they require for optimal SSL processing. The comprehensive set of solutions, and seamless integration with Cisco Data Center products, such as server load balancers, put Cisco and the Cisco SCA 11000 Series in the forefront of SSL technology on the market today. The Cisco SCA 11000 Series was designed from the ground up to enhance any public key infrastructure (PKI) you decide to deploy.

Web designers and networking staff can choose between two distinct models of Cisco SCA 11000 Series, both of which provide linear scalability and fault tolerance and both interoperate with all Cisco server-load-balancing (SLB) products: the Cisco CSS 11000 and 11500 series content services switches; the Cisco Content Switching Module (CSM) for the Cisco Catalyst 6500 Series switches and Cisco 7600 Internet Router; and the Cisco LocalDirector Series. The combination of SSL offloading and intelligent load balancing of SSL traffic forms a perfect union, improving both the performance and availability of any Internet or intranet Web site. Table 1 compares the two versions of SSL offloaders.

Table 1 SSL Offloaders

	SSL appliance SCA	SSL appliance SCA2
Performance		
Rivest, Shamir, Adelman (RSA) operations per second	200	4000 or greater
Connection rates	200	800
Concurrent sessions	5000	30,000
SSL session ID cache	75,000	300,000
No. of proxy servers	255	512
Bulk encryption (rc4-128-md5)	30 Mbps	70 Mbps
Cryptology hardware	Rainbow	BC 5821
RSA hardware	Yes	Yes
Hardware-based bulk encryption	Yes	Yes

Benefits

The Cisco SCA 11000 frees origin Web server capacity by offloading all encryption, decryption, and secure processing for a Web site. It also eliminates the need for SSL server software, and requires no special software on the servers or the Cisco server load balancers.

The Cisco SCA 11000 Series boosts the performance of any secure Web site up to 250 times through dedicated SSL processing hardware. It supports 800 new SSL connections per second, 20,000 concurrent sessions, and 300,000 sustained sessions.

SSL session initiation and aggregation capabilities can be used to secure nonsecure TCP applications, or to offer end-to-end (back-end) encryption to sites with strict security requirements, such as financial, health care, and government institutions.

The Cisco SCA 11000 Series provides advanced client certificate support and Hypertext Transfer Protocol (HTTP) header insertion for integration with Directory Services and Single-Sign-On platforms.

Secure URL Rewrite provides the industry's only secure method of integrating SSL offloading technology with Web-based applications.

The Cisco SCA 11000 Series centralizes and manages the widest range of digital certificates to ensure complete independence from the Web server, and works with any Web server, application server, or TCP-based application platform.

Overview

SSL is the industry standard for secure Web communication, and any Web site delivering e-commerce services or secure personalized information over the Web must efficiently handle SSL traffic. Processor-intensive SSL computations, including site authentication and encryption of data, can quickly bog down Web servers, which are not designed for heavy SSL transaction processing. In fact, up to 95 percent of the processing power of a server can be consumed by SSL processing. When a mission-critical Web server becomes overloaded from processing secure transactions and cannot process other Web transactions, the result is lost customers, lost revenue, and lost productivity.

The Cisco SCA 11000 Series performs all SSL protocol processing for a Web site, supporting up to 800 new connections per second and up to 30,000 concurrent connections. This allows Web, e-commerce, and application servers to function at peak performance levels. The one-rack-unit-high, rack-mountable product offers two 10/100 Ethernet ports and features redundant power supplies for mission-critical networks.

Boost E-Business Performance

The success of an organization's e-business initiatives depends on user experience. When secure transactions are slow to process, it can impact not only revenue and customer satisfaction on public-facing Web sites, but also the productivity of employees who may be using SSL on intranet sites for the transmittal of secure data such as personnel, benefit, or sales forecasts data.

The Cisco SCA 11000 Series uses powerful onboard processors and an embedded real-time operating system to provide all secure transaction functions. By offloading all secure transaction processing, the Cisco SCA 11000 Series lets Web servers do the job they were designed for—serving Web content and processing e-commerce transactions.

SSL Initiation and Aggregation (back-end SSL)

In addition to terminating inbound SSL sessions, the Cisco SCA 11000 Series can also initiate outbound SSL sessions. This enables numerous security functions, including the retrieval of secure information from remote sites for applications such as Web services.

The Cisco SCA 11000 Series aggregates multiple SSL sessions and provides a single SSL session to back-end servers. Cisco SLB can evenly distribute these back-end SSL sessions, increasing server capacity and improving return on investment (ROI). SSL aggregation can even be used in conjunction with cookie persistence.

Client Certificate Support with HTTP Header Insertion

Client certificates are becoming increasingly popular among sites looking to offer the strongest security possible. Unlike other security products that offer extremely limited support, or no client certificate support at all, the Cisco SCA 11000 Series supports configurable client certificate handling, and can also extract client certificate information for presentation to back-end servers using HTTP headers. The Cisco SCA 11000 Series provides the flexibility to integrate existing security infrastructures, such as directory services, PKIs, or Single-Sign-On platforms, with leading-edge SSL technology.

Secure URL Rewrite

The Cisco SCA 11000 Series can be seamlessly inserted into your environment without the need to rewrite existing Web applications or compromise your existing level of security.

In an offloaded environment, the back-end servers generally "talk" HTTP rather than HTTP Secure (HTTPS). Therefore, dynamically rendered pages will often generate links referring to HTTP resources rather than HTTPS resources. In first-generation SSL offloaders, this was handled in an inefficient and nonsecure fashion by sending the client a redirect back to the correct HTTPS resource. With the exclusive Secure URL-Rewrite feature, the Cisco SCA 11000 Series can prevent such risky inefficiencies by recognizing any inconsistency and correcting it before an error is sent to the client. This saves unnecessary redirects, prevents secure data from being transmitted in the clear, and also averts the need to have application developers rewrite applications to support an offloaded environment.

Centralize and Manage Certificates

The Cisco SCA 11000 Series supports up to 255 key pairs (keys and certificates) and has the ability to handle both global and chained certificates. The Cisco SCA 11000 Series also eliminates the need to install and manage special acceleration cards and SSL certificates on every Web server. Private and public keys are stored on the Cisco SCA 11000 to ensure complete independence from the Web server and to eliminate the hassles of setting up the secure processing properties of host applications.

Scales for High Availability

The Cisco SCA 11000 Series works seamlessly with all Cisco SLBs to enable load balancing of multiple Cisco SCAs in an SSL farm. This "one-armed" configuration allows Cisco SCA 11000s to connect to the Cisco CSS 11000s and 11500s) via a single 100-MB Ethernet port, instead of the two ports—one ingress, one egress—required by alternative solutions. The key benefit is adding SSL capacity without impacting Web site and network availability, eliminating site downtime.

Works with Any Servers

SSL transactions slow server processing time considerably—no matter what type of Web server is used, Linux, Solaris, or Windows NT. In fact, according to Networkshop, SSL processing can cause a Web server to deliver up to 50 times fewer connections per second (Networkshop: Scaling Security in E-Commerce Applications). With the Cisco SCA 11000 Series, Web servers are freed from the burden of SSL transaction processing to allow them to perform Web content delivery more efficiently.

Ordering Information

Product Part Numbers

CSS-SCA-2FE-K9

CSS-SCA2-2FE-K9

Table 2 shows product specifications for both the Cisco SCA 11000 Series Secure Content Accelerator models.

Table 2 Specifications

Specifications	
Number of ports	**Port description**
Two 10/100 transmission ports	Network ports: Two 10/100BASE-TX Console port: DB9 serial port Failover port: DB9 serial port Reset switch: Push to reset hardware; configuration data maintained
Network cabling	Data transfer rates
Cable type: UTP Category 5 (100m) **Connector type: RJ-45**	20 Mbps (full duplex) Fast Ethernet 100 Mbps (half duplex) 200 Mbps (full duplex)
Configuration software OS support	Memory
Windows NT 4.0; Red Hat Linux 5.0, 6.0, 6.1, 6.2	64-MB RAM; 16-MB Flash ROM
Standards	Regulatory compliance
IEEE 802.3 10BASE-T EthernetIEEE **802.3u 100BASE-TX Fast Ethernet**	FCC Class A; CISPR-22-A; VCCI-A; CSA and CE Compliant to: EN55022 Class A, EN55024, EN50082-1, EN60950
Protocols	Public key cryptography algorithms
Carrier sense multiple access collision detect (CSMA/CD) Ethernet	RSA-512 RSA-024 RSA-2048
Encryption algorithms	Hash algorithms
Data Encryption Standard (DES) **ARC4** **ARC2**	Secure hash algorithm 1 (SHA1) Message digest algorithm 5 (MD5)
Physical and environmental specifications	
Dimensions	Weight
(L x W x D): 8.875 x 19 x 1.75 (one rack unit)	6 lb (2.7 kg)
Environmental operating range	Power requirements
Temperature: 32° to 104°F (0° to 40°C) **Humidity: 10 to 85% non condensing** **Altitude: Up to 3048 meters (10,000 ft)**	Operating voltage: 100–240V; 50–60 Hz 1.0A Consumption: 20W Power supply: Internal redundant power supplies

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 Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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: 65 317 7777
Fax: 65 317 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