

Cisco Web Network Services For E-Commerce

Implementing Secure and Scalable E-Commerce Network Services

Introduction

E-commerce operations are becoming a fundamental business necessity, and important source of revenue, for both “dot com” and traditional enterprises. Businesses need to improve the performance of fast-growing e-commerce Web sites while ensuring business transaction integrity, positive shopping experiences for customers, and continuous availability of their virtual storefronts.

Web businesses need to deliver rapid transaction response time and manage peak-period volume levels—whether from seasonal increases in traffic or from unexpected surges in customer demand. Customers will return to e-commerce sites that offer consistently high levels of reliability—and they will avoid sites that deliver slow response times, difficult shopping experiences, or failed attempts to make purchases. A key component in ensuring that e-commerce sites remain open for business requires support for persistent, “sticky” network connections between customers and e-commerce servers, so shopping carts are not lost before purchase transactions are completed.

Further, with an increasingly competitive business environment, popular e-commerce sites gain customer loyalty through delivery of differentiated, customer- and content-focused services. On the Web today all customers expect good, reliable performance. But certain customers and content deserve prioritized service because of their strategic value to the business.

Running on Cisco CSS 11000 content series services switches, Cisco Web Network Services (Web NS) software allows e-business companies to build secure, reliable, and scalable e-commerce sites that support high-volume e-commerce transactions, a consistently positive user experience, and prioritized services for important customers and content.

The technical challenges associated with building a competitive e-commerce Web infrastructure are associated with three common traffic scenarios:

- *Authenticated/nonencrypted Hypertext Transfer Protocol (HTTP)-based transactions*—desirable when security requirements are less demanding and the need for site performance is high, as in catalog browsing
- *End-to-end encrypted Secure Sockets Layer (SSL)-based transactions*—desirable for e-commerce applications where security requirements are very high, as in banking or online trading
- *Authenticated/encrypted transactions*—a combination of HTTP connections for browsing and SSL connections for purchase transactions, desirable for high-volume purchasing applications that need to optimize site performance by limiting SSL overhead to connections involving credit-card or other highly personal information

The Nature of E-Commerce Traffic

E-commerce is exploding because of its efficiencies in connecting buyers directly with sellers and reducing the cost of sales. Developing and managing e-commerce infrastructure is a major challenge for both established and emerging companies. A single Web-based transaction can span multiple servers, applications, and databases, and companies must be able to connect users seamlessly to these resources throughout the life of their shopping session. This can be accomplished only by creating “sticky connections” between a customer and a single server—regardless of the type of connection used (HTTP, SSL, or combination HTTP/SSL).

Successful e-commerce sites must overcome several other obstacles. The rapid growth in e-commerce requires the ability to build scalable solutions that can handle dramatic increases in traffic, including the ability to respond to flash crowds for “hot” content as well as the ability to rapidly scale site capacity to accommodate rapid increases in demand.

Companies must deliver consistently high response times so buyers can quickly and easily purchase products or services on line. Just as retail stores with long lines at the checkout counter lose customers unwilling to wait, e-commerce sites need to make sure that long waits and annoying errors do not result in lost customers. High levels of reliability require carrier-class networking equipment that can deliver the 24x7 availability demanded by e-commerce customers.

Security can also be a major obstacle to the successful deployment of e-commerce sites. There is just no room for equipment failure or revenue-reducing downtime resulting from denial-of-service (DoS) attacks. These DoS attacks typically involve the misuse of standard protocols or connection processes with the intent to overload and disable the target Web servers. Companies need the ability to perform per-flow filtering of content requests, without degrading performance, so they can implement policy-based security that considers any combination of source address, destination address, protocol, type, or content Universal Resource Locator (URL).

Protecting personal information is a major security concern as well. Companies need to evaluate the optimum security level for each site and analyze the impact of encryption techniques on both the scalability and performance of the site. Finally, e-commerce businesses must protect mission-critical back-end systems without creating performance bottlenecks associated with traditional firewalls.

The ability to build highly secure e-commerce sites with fast response times that can scale efficiently is a major obstacle to the successful deployment of e-commerce. Those companies able to overcome this obstacle can achieve major successes in this exciting marketplace.

Building Competitive E-Commerce Sites

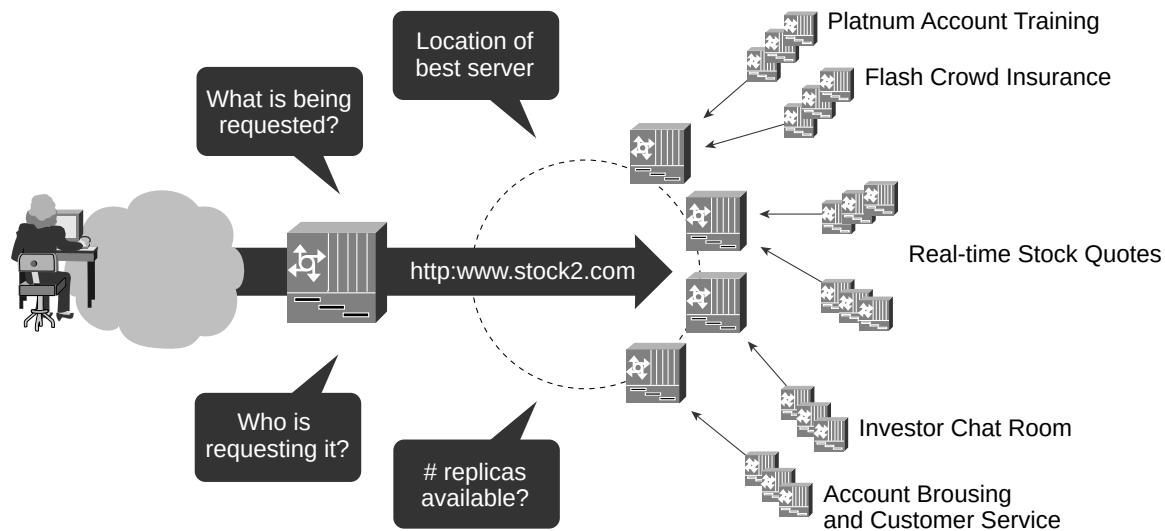
For busy e-commerce sites, traditional Layer 4 switches, and new “content-aware” switches are insufficient for achieving high performance and balancing traffic loads across Web server farm and caching resources. Conventional load balancers and Layer 4 switches were originally designed for address-based switching and differentiate applications based only on the identity of well-known TCP ports and source and destination IP addresses.

However, most e-commerce traffic comprises HTTP requests for content, and conventional load balancers cannot differentiate between multiple HTTP requests for different content URLs or between individual customers based on user “cookies.”

Layer 4 switch architectures with content-aware software upgrades provide limited (40 to 80 contiguous bytes) visibility into HTTP header information, but e-commerce solutions require the increased intelligence of Cisco CSS 11000 series switches.

Cisco Web NS—With the industry’s most comprehensive URL- and cookie-based switching, Cisco Web NS software lets network managers tailor customer or content-specific service agreements, offer premium services for preferred customers, and deploy content-delivery services for streaming audio and video, distance learning, and Internet audio and video broadcasting. Support for sticky connections based on IP address, SSL session ID, and cookies ensures reliability and security for e-commerce transactions. The unique Cisco content-replication technology enables dynamic expansion of site capacity in response to sudden “flash crowds” for “hot” content, or seasonal peaks in traffic that can overwhelm servers.

Figure 1 Cisco Web Network Servers



Running Cisco Web NS software, with patented content switching technology, Cisco CSS 11000 series switches know:

- Who the customer is, based on full visibility to the user cookie located anywhere within the HTTP header
- What information or transaction the customer is requesting
- Where best to service the customer from anywhere within a globally distributed Web infrastructure, based on comprehensive and current information on network, application, and server conditions

With this innovative software, Cisco CSS 11000 series switches can access information deep in the TCP and HTTP headers, including the complete URL and "mobile" cookies that change location within the header between requests. This information is used to enable advanced load balancing, routing of requests, security (DoS and access control), priority access for important customers, and sticky connections. Cisco CSS 11000 series switches were designed for name-based switching, and they are the only switches to use the entire URL and cookie to select the best site and server for the customer's inquiry or purchase at any given moment.

Cisco CSS 11000 series switches allow organizations to improve reliability and response time by examining content requests in detail and directing users to the best site and best server at that moment, avoiding busy or overloaded sites and dynamically replicating hot content across the network. When users are connected to a server, Cisco CSS 11000 series switches ensure that they stay connected to a single server for the duration of their transaction, using the source IP address or address range, TCP port, SSL session ID, and even "cookies" embedded in the users' request. "Content-aware" solutions are incapable of dealing with complex cookie streams, and cannot provide the successful transition between cookie-based policies and SSL-encrypted portions of the transactions.

E-commerce sites can eliminate debilitating DoS attacks by using the FlowWall security' features of the Cisco CSS 11000 series switches, which provides wire-speed, per-flow filtering of content requests with no performance penalty. FlowWall security provides intelligent flow inspection technology to screen for all common DoS attacks and any abnormal or malicious connection attempts. Access rules can be implemented based on any combination of source address, destination address, protocol, type, or content URL.

Ensuring Transaction Security and Reliability

The most common method of securing Web-based transactions is the use of the popular SSL protocol. SSL is an end-to-end encryption mechanism and is the primary means of encrypting Web transactions today.

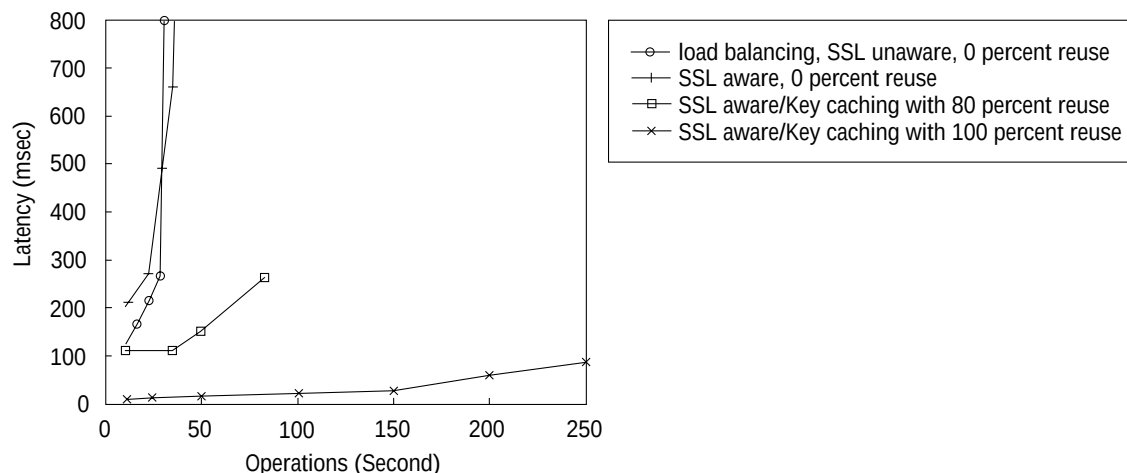
Netscape Communications designed the SSL protocol to enable encrypted and authenticated communications across the Internet. SSL is used primarily to establish secure connections between Web servers and browser clients, and provides privacy, authentication, and message integrity. If a Web address begins with HTTPs, it means that users are entering into a secure, encrypted

connection. In an SSL connection, each side of the link transmits a security certificate or “session key.” The server and the browser both encrypt traffic flows using the other’s certificate so that only the intended recipient can decrypt the information. This ensures that the session came from the intended user and that the flow has not been altered along the way.

Yet SSL imposes significant processing overhead on servers that can slow e-commerce site performance considerably. Data encryption and decryption both increase SSL processing overhead, and several approaches to increasing SSL performance are commonly used. However, the most substantial overhead from SSL is created by the negotiation of session keys (see Figure 2).

- Method 1—A traditional method is to integrate encryption directly into business applications. Although this offers the tightest security—because the traffic flow is encrypted from the client directly to the application—the computing-intensive encryption process will consume significant Web server resources.
- Method 2—Another approach is to use hardware-based encryption accelerators, which can be deployed in the Web server itself to improve SSL performance.
- Method 3—Recently a new approach has emerged that deploys hardware accelerators in dedicated devices that sit in the path to the server farm and process all SSL traffic for all servers in the server farm. Although this offloads processing from Web servers onto dedicated devices, it is complicated to administer, may not scale for busy Web sites, and creates a potential security breach between the hardware accelerator and the Web server—where the traffic is not encrypted. A single dedicated encryption device can handle more SSL requests than one or even several nonaccelerated servers, but using hardware accelerators on a per-server basis provides linear scalability as servers are added.

Figure 2 Impact of SSL Session Key Caching on Latency and Performance Source: IBM; Cisco Communications



Cisco uniquely optimizes SSL transaction performance in two ways:

1. It uses front-ending SSL accelerator devices to provide application load balancing.
2. Cisco switches cache and reuse SSL sessions, thus offloading from servers the most processing-intensive aspect of SSL—negotiating the SSL handshake.

E-commerce sites need the flexibility to balance the needs for both security and site performance based on their unique business requirements. The ability to maintain sticky connections requires the need to support all three of the following e-commerce security scenarios:

- Authenticated transactions based on HTTP connections
- Transactions encrypted end to end with SSL connections
- Hybrid transactions that combine both of the above types of connections



Cisco provides the flexibility to allow companies to implement the appropriate high-performance solution for their specific security requirements. Organizations can evaluate the three basic means of securing e-commerce and select the most appropriate option-safe in the knowledge that the solution can scale effectively to support more customers and new business initiatives in the future.

E-Commerce Scenario Number 1: Authenticated Transactions

Many sites authenticate users without encrypting each customer's connection. This scenario minimizes SSL processing overhead and supports high levels of scalability for environments where encrypted data transmission is not required.

For example, a market research site that allows its customers access to its proprietary research on line will find this the optimal security approach. After the customer enters his or her name and password, the system conducts a database lookup that will authenticate that the user has paid for access to the site and will then grant access to the secure area.

Preventing an authenticated subscriber from losing the continuity of the session is essential to customer satisfaction. Customers will not tolerate continuous disconnects each time the session is passed to a different server, and many will not bother to reauthenticate to regain access. The e-commerce provider must ensure that the authenticated user maintains session integrity and has a pleasant e-commerce experience.

Because HTTP does not carry any state information for these applications, it is important that the browser maps to the same server for each HTTP request until the transaction is complete. This ensures that the user is not load balanced in midsession to a different server and forced to log in again. Cisco allows you to efficiently deliver authenticated transactions by balancing requests across multiple servers, managing server load, and creating sticky connections.

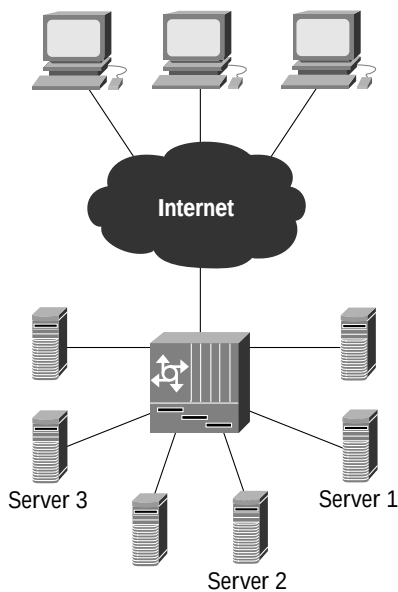
Traditional load balancers can provide sticky connections using IP source address and TCP port, a scenario that is dependent on the client's maintaining a consistent source IP address throughout the life of the session. This becomes an issue if the user is coming through a mega-proxy server-such as an America Online host-because traditional load-balancing products will not have enough information to reliably connect the user to the same server throughout the life of the transaction.

The source IP address is not good enough to identify the client because-in the case of an outbound client proxy-the same source IP address can be used by any number of clients. The source IP address can unexpectedly change if the proxy server dies and a backup server is used, or if a route-change event has forced the use of a new proxy server. Thus, the IP header itself is not a reliable means of identifying an individual customer.

The only reliable way to maintain sticky connections is to use cookies to identify individual customers. Cisco CSS 11000 series switches can read the entire cookie, a server-specific string in the header of the HTTP traffic flow, to identify the user and route him or her to the correct server, as shown in Figure 3. The Web-server application can write a server-specific string in the HTTP header (that is, server 1). The Web switch is then configured to find this string within a specified byte range after the [cookie:] in the HTTP request. The Web switch associates the cookie with a specific service, and directs the request to that service. This is transparent to the user, but the session to the front-end HTTP server is maintained as the transaction crosses multiple back-end servers and databases, ensuring that the user enjoys continuity and optimal response time over the life of the transaction.

Traditional routers and load balancers and content-aware switches are insufficient for this critical task, because dynamic higher-layer information is needed to find and process the cookie. Cisco CSS 11000 series switches support sticky connections based not only on source IP address, address range, TCP port, and SSL session ID, but also on the cookie embedded in the user's HTTP header. This feature is key to enabling sophisticated e-commerce applications by providing sticky client/server connections based on the unique information embedded in the cookie.

Figure 3 Sticky Connections



This is the only way to ensure sticky connections for authenticated applications when thousands of users are coming into a site via a mega proxy-such as an AOL server-or whenever multiple incoming clients share a common source IP address. This also eliminates server crashes that result when mega-proxy clients are all connected to the same server, and enhances site performance, reliability, and revenue generation.

E-Commerce Scenario Number 2: Transactions Encrypted End to End with SSL

Many e-commerce sites require the highest levels of security to enable business transactions over the Web. For these companies, authentication alone is not sufficient. It is not enough to know that buyers are who they say they are; it is also critical to protect highly sensitive information used during transactions, such as credit-card numbers and other personal information.

For example, banks and brokerages that allow customers to access highly personal information require encrypted, end-to-end transactions. These companies extend their sales and support channels via the Web, and for them the increased security offered by encryption is mandatory.

Cisco CSS 11000 series switches maintain sticky connections for SSL transactions by using the SSL session ID. This is critical, because cookies are located in the HTTP header that is encrypted for SSL transactions and, therefore, cannot be read by the Web switch to maintain sticky connections.

The initial SSL hello message between the browser and the server contains either an empty session ID field (if a new SSL session is to be established) or the last SSL session used by that client. But this is not the session ID that will be used for the impending e-commerce session. In response to the client hello message, the server picks a new session ID, and then sends its own hello back to the client with that session ID. The Cisco CSS 11000 series switches detect this new SSL session ID in the server hello, and routes the request to the best server at that point in time. All subsequent requests with that SSL session ID will then be routed to the same server.

The Cisco CSS 11000 series switches also resolve the SSL timeout issue. To optimize resources, a Web server is programmed to end a session after a defined period of inactivity. After several minutes with no activity, the server will time out and the session ID will be released. When the user sends a new request, the server thinks it is a new user and begins a new SSL session. If the user was filling out a long form, such as a mortgage application or credit profile, all the information already filled in will be lost and the user will have to start over.



The Web switch resolves this issue by detecting the client's SSL session ID when it attempts to reconnect, and uses it to route the user to the same server to which he or she was last connected. The server will create a new SSL session ID, which the switch learns, and then uses to keep the user connected to the same server.

Content Smart Web switching not only improves efficiency and customer satisfaction by creating sticky connections for encrypted sessions, it can also significantly reduce the strain on application servers. Because the SSL handshake that establishes a session involves the exchange of public keys, it creates the largest single drain on computing resources. By intercepting session IDs and transparently reestablishing failed sessions, a Content Smart Web switch eliminates the processing-intensive task of negotiating a new session after each link failure.

Cisco allows e-commerce sites to deliver encrypted connections while minimizing associated processing overhead. Content Smart Web switches simplify the transaction for the customer and maintain consistent, secure transactions that deliver the performance and reliability required by successful e-commerce sites.

E-Commerce Scenario Number 3: Hybrid Transactions Using HTTP and SSL

The most common security scenario comprises a hybrid of authenticated (HTTP) and encrypted (SSL) connections. This allows e-commerce sites to deploy the optimum level of security for each stage of the transaction while minimizing processor overhead. In this combination approach, part of the transaction may be nonsecure and available to the general public; other parts may be authenticated but not encrypted; and still other flows may be authenticated and encrypted.

For example, a retail site may have product information available to the general public, have authenticated services with additional information available for repeat customers, and offer the ability to purchase goods on line. By implementing a combination of security technologies, this site can efficiently deliver a scalable security solution.

The general product information can be nonsecure and available to all browsers, but established customers can input their passwords to enter a special area of the site that contains additional product information, such as pricing and availability. During these phases of the transaction, the Cisco Web switch can use source IP address or address range, or the cookie to maintain sticky connections. This permits the Web switches to track content requests and to maintain sticky connections while the user fills up the shopping cart and finalizes the purchase.

At checkout time, when the customer clicks the “Buy Me” button to purchase the selected merchandise in his or her “shopping cart,” a new TCP connection is set up between the browser and the server to create an SSL session, which will encrypt this phase of the transaction. At this point, the transaction is encrypted and the Web switch can now use SSL session IDs to maintain sticky connections. When the browser has the same source IP address for both phases of the transaction, the Cisco CSS service switch has a sufficient level of detail to maintain consistent sticky connections between both parts of the transaction. However, when the client is coming to the site from a mega-proxy server, it is likely to use multiple source IP addresses over the life of the transaction.

It is precisely the transition between non-SSL and SSL that virtually guarantees that a new source IP address is used, causing a potential buyer to be load balanced away from the original server in the middle of a purchase. If the client is incorrectly sent to a different Web server in the middle of the shopping experience, the new server may have no record of what is in the shopping basket, and the user is frustrated—at the very point he or she is prepared to complete the sale.

Cisco CSS 11000 series switches avoid this problem by maintaining a sticky connection throughout the completion of the purchase. In the first phase, the Web switch uses the cookie to keep the user connected to a specific server. When the transaction moves into the SSL phase, the page containing the “Buy Me” button must have a link that resolves the transaction to the same server. This is accomplished by the Web-server application, which embeds an absolute HREF1 in the page for the “Buy Me” link. The href points to an explicit virtual IP (VIP2) address, which can be the same one that it was connected to for the first part of the transaction, and a unique TCP port that is associated with that server. When the Web switch sees the SSL hello coming from the browser with that VIP and TCP port, it will route the request to the server associated with the TCP port. The Cisco Web switch can proceed to connect the connection to the server based on the session ID for the duration of the transaction.

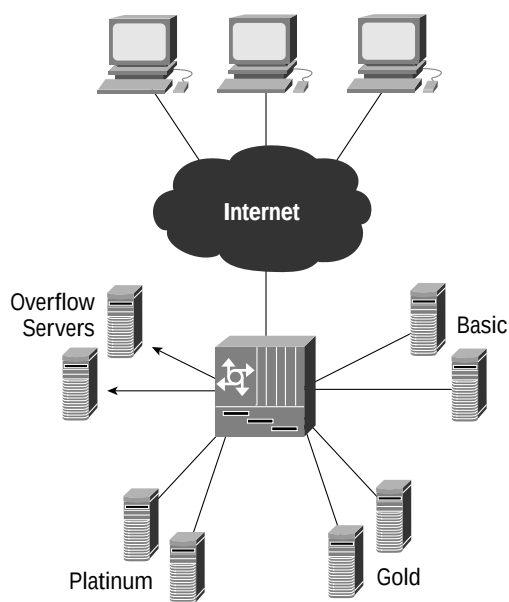
This scenario requires the ability of the switch to maintain complex “content rules” that can maintain the association between the cookie-based policy and the SSL sticky connections that come into the server on a different connection. This level of granularity and the required number of content rules are not supported in content-light implementations.

Using Cookies to Provide Priority Services for Premium Customers

When used for sticky connections, the cookie is associated with a specific service, or virtual Web server. When the switch receives a request with a cookie, the switch routes the request to the service associated with that cookie. When using cookies for premium services, the main difference is that the cookie is now associated with a “content rule,” which is in turn associated with a group of services. In this case, when the switch receives a request with a cookie, the switch routes the request to the best server in the “premium” group of servers associated with that content rule and cookie, as shown in Figure 4.

The servers in the premium group can be configured with a limited number of transactions, or a maximum load limit, ensuring that they will always have enough capacity to provide the best possible service. If the premium servers become oversubscribed, additional overflow services may be configured using a demand-based content-replication capability in the Cisco CSS 11000 series switch. This capability allows thresholds to be set for specific content, and if the threshold is reached, the switch will replicate the hot content to overflow servers or caches.

Figure 4 Premium Services



The scenario for premium services follows:

1. The user comes to the site for the first time. The Cisco CSS 11000 series switch, having not detected any cookie, routes the request to the registration server.
2. The user is authenticated and the application determines the user's priority, based on potential business or some other criteria. The application then writes a cookie, that is, silver, gold, or platinum.
3. The next request that comes in with a silver, gold, or platinum cookie is routed to the group of servers that is associated with that cookie.

Conclusion

Featuring patented content-switching technology, Cisco CSS 11000 series switches give businesses maximum control in allocating e-commerce site resources and building services for optimal return on investment (ROI). By implementing Cisco CSS 11000 series Network Services for e-commerce, companies-and their hosting partners-can provide reliable, secure, high-performance e-commerce sites that are continuously “open for business.”

**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 Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

**Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the
Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • 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 • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States •