Cisco Wide Area Application Services for Software-as-a-Service Application Acceleration

Q. What new Cisco® Wide Area Application Services (WAAS) solution capabilities are being announced?

A. Cisco is announcing new Cisco WAAS optimization capabilities for cloud-based application delivery, or software as a service (SaaS).

Q. What value proposition is Cisco WAAS delivering?

A. Cisco WAAS provides an innovative solution for optimizing cloud-based SaaS applications, such as Cisco WebEx™, Microsoft SharePoint, and Salesforce.com, while preserving security and simplifying IT operations. By simplifying secure optimization of SSL- and HTTPS-based SaaS applications, Cisco WAAS helps IT departments lower the costs of SaaS deployments, reduce the amount of WAN bandwidth required, and improve end-user productivity. IT operational costs for delivering large-scale SaaS deployments are reduced through simplified configuration. WAN bandwidth costs are reduced through the extension of Cisco WAAS optimization technologies to SaaS applications. The security perimeter is preserved through features that help ensure that the server private keys, used for SSL traffic optimization, never leave the data center.

Q. Why are organizations increasingly accessing applications from a SaaS provider?

A. The SaaS model saves organizations the cost of hosting and managing the applications, as well as licensing and acquisitions costs, so the savings from the use of SaaS can be considerable. Among the many types of applications delivered by SaaS, some of the most popular are collaboration applications, such as Cisco WebEx and Microsoft SharePoint and Exchange. These applications increase user productivity, delivering additional financial benefits, and they are designed to be hosted in a SaaS delivery model, in which collaboration occurs across organizations, over private and public networks.

Q. How is the SaaS deployment model different from the typical enterprise model?

A. In a SaaS application delivery model, the application used by the enterprise is hosted by a third-party application provider in the application provider's own data center and delivered over the Internet to the enterprise. Analyst reports state that 60 percent of SaaS applications are accessed from the SaaS hosting center and then backhauled through the corporate data center to the branch office.

Q. How does SaaS affect security policy?

A. Since SaaS applications are accessed remotely, from the hosting data center over the Internet, they must be accessed securely to avoid inappropriate access to data. For this reason, SaaS applications are accessed over a secure HTTPS link in which the data is encrypted with SSL. This scenario presents challenges for many organizations.

Q. How important are security concerns to customers?

A. According to a recent IDC survey, 74 percent of respondents rate cloud security concerns as very significant. The reason is that the public cloud's multi-tenant, dynamic characteristics, puts sensitive or regulated data at risk as activities and data move across open, untrusted networks. To address this concern, security must span internal and external clouds, and encryption and key management must follow sensitive data.

Q. Why would WAN optimization be used with SaaS applications?

A. Today, many organizations are using WAN optimization to extend the reach of their data center–hosted applications to users in remote branch offices. By using WAN optimization, organizations can recover bandwidth that was lost due to redundant data transmission and increase the number of users that a link can support. SaaS applications often are transported over an optimized WAN link to improve application performance and increase the number of user sessions. Analyst reports state that 60 percent of SaaS deployments are backhauled through the corporate data center; thus, IT departments can use WAN optimization and build on the automation benefits that Cisco delivers.

Q. What functions does WAN optimization provide?

A. WAN optimization performs four main functions: it compresses traffic in flight, it eliminates transmission of redundant data through caching, it accelerates TCP flows, and it accelerates application-specific protocols.

Q. What benefits does Cisco WAAS provide to SaaS deployments?

A. Early results have shown up to 80 percent faster performance for redundant Cisco WebEx streams to the branch office. Hosted Microsoft SharePoint delivery is up to 98 percent faster.

Q. How does the introduction of WAN optimization change the security model?

A. When WAN optimization is in place to serve remote branch offices, the backhauled SaaS model introduces challenges in setting up the secure sessions. SSL encryption obscures data repetition so data cannot be compressed, nor can it be cached, although it can be accelerated by the WAN optimization device. Thus, the WAN optimization device must have a trust relationship with the SaaS application so that it can see the data and perform compression and caching before sending it over the WAN link.

Q. How does the SaaS model complicate SSL configuration?

A. A number of factors in the SaaS deployment model can complicate session setup with WAN optimization. A typical SaaS provider has a farm of application servers and multiple SSL servers. The WAN optimization device in the enterprise data center needs to know the IP addresses and hostnames of these servers to complete authentication to optimize user connections. The SaaS provider also may add or remove hostnames or change IP addresses, which complicates the authentication process for the WAN optimization device.

Q. What does Cisco WAAS provide to make SSL configuration effective?

A. An efficient method of configuration for the sessions over the optimized link is needed. Cisco WAAS enables optimization of SaaS deployment models by providing a simple solution that streamlines the process of SSL connection setup and eliminates security problems.

Q. How does SSL configuration work with WAN optimization?

A. The WAN optimization device in the data center splits the original SSL connection from the client to the SSL server into two SSL connections. To the client, the connection appears as the SSL server. To the SSL server, it appears as the SSL client. To act as the SSL server to clients, the data center WAN optimization device needs a certificate for each SSL service it is optimizing. Since the WAN optimization device can optimize multiple SSL services, the data center device potentially has multiple SSL certificates. To supply the correct certificate to the client, the WAN optimization device uses the SSL server IP address and associates each certificate with a specific server IP address. When the WAN optimization device intercepts a TCP connection from the client to the SSL server, it uses the server IP address in the connection to determine which certificate to supply to the client.

Q. How does configuration control in the SaaS model differ from that in the enterprise model?

A. For SSL services hosted in the enterprise data center, the IT administrator knows and controls the SSL server IP address and can provide it to the data center WAN optimization device, but for an SSL-connected service hosted by a third-party SaaS provider, the SSL server IP address is not controlled by the IT administrator, and many server IP addresses may be used even for a single SaaS service. For both enterprise and SaaS deployments, the SSL server IP address may change at any time, and the WAN optimization device will need to be reconfigured with the new IP address.

Q. How has Cisco WAAS simplified the SSL configuration model?

A. Cisco WAAS simplifies the configuration process by allowing IT administrators to specify the Domain Name System (DNS) hostname of the SSL server; Cisco WAAS automatically keeps track of IP address changes and needs no manual intervention by the IT administrator.

Q. Why is this configuration automation important to customers?

A. DNS hostnames work well for enterprise SSL servers and for SAAS applications with very few DNS hostnames. However, for some applications the number of hostnames is very large, and the hostnames can change. For these use cases, Cisco WAAS provides the additional capability of DNS domain recognition. In the Cisco WAAS configuration, the IT administrator specifies the DNS domain suffix--for example *.webex.com--and the associated certificate. Cisco WAAS automatically discovers whether a given SSL connection belongs to this domain (by performing a reverse DNS lookup on the IP address). After Cisco WAAS has identified the domain, it can supply the correct certificate to the client.

Q. How does this automated SSL configuration process benefit customers?

A. With this simplified configuration process, Cisco WAAS provides a transparent one-click solution that reduces IT administrative tasks and delivers proven performance for cloud-based applications, enabling customers to benefit from next-generation deployment models for SaaS-delivered applications such as Cisco WebEx and Microsoft SharePoint.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.

Printed in USA C67-574898-00 01/10