Deliver Proven Application Performance for Software-as-a-Service Deployments

What You Will Learn

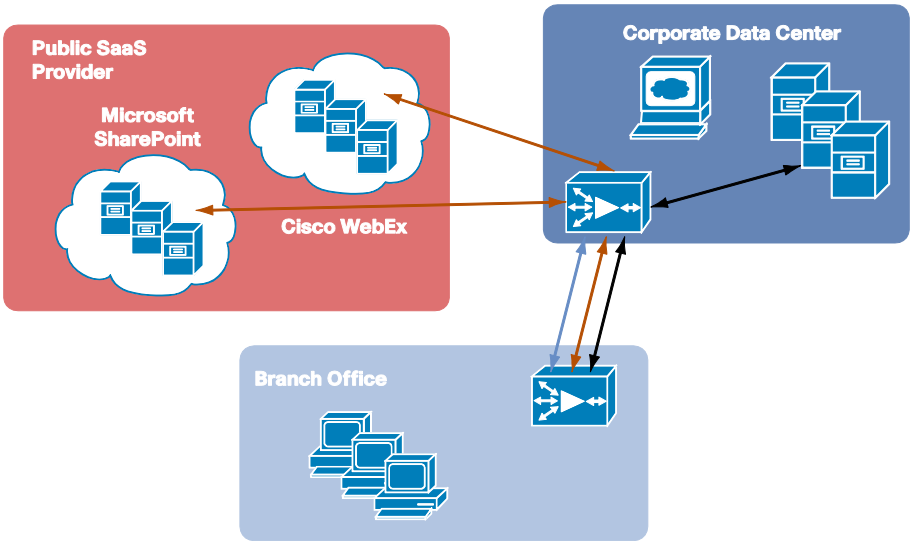
Cisco® Wide Area Application Services (WAAS) provides an innovative solution for optimizing cloud-based, software-as-a-service (SaaS) applications, such as Cisco WebEx™, Microsoft SharePoint, and Salesforce.com, while preserving security and simplifying IT operations. This document describes the benefits of SaaS and how those benefits can be enhanced with Cisco WAAS optimization.

The SaaS Model

Organizations are increasingly adopting SaaS applications delivered from application providers and private and public clouds. The SaaS model enables implementation of per-use and per-user cost structures, allowing customers to avoid capital expenditures (CapEx), replacing CapEx with predictable operating expenses (OpEx), and reducing total cost of ownership (TCO) by eliminating the need to host and manage the application infrastructure. SaaS thus provides both economic and infrastructure benefits. SaaS application delivery is adopted mainly for enterprise collaboration applications, such as Salesforce.com, 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.

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. A recent report from IDC states 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 (Figure 1). Since SaaS applications are accessed remotely, from the hosting data center over the Internet, they must be accessed securely to avoid security problems such as 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 security concern presents challenges for many organizations.

Figure 1. SaaS Sessions Backhauled Through the Corporate Data Center and Then Optimized by Cisco WAAS to the Branch Office



SaaS and Security

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.

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 greatly 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. 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.

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. The authentication and configuration process is relatively straightforward when the application sits in the primary data center; however, additional complexity is introduced when the application is remotely hosted with a SaaS provider.

"People worry that SSL encryption will be too complicated, and ... when they plan their WAN optimization strategy, end-to-end encryption is something they have to consider," said Eric Siegel, a senior analyst with the Burton Group, "and I would worry about it."

SaaS Setup and Configuration

Session setup in a WAN optimized environment is complicated. 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 the authentication process for user connections. The SaaS provider may add or remove hostnames or change IP addresses, creating a management challenge. As a result, an efficient method of configuration for the SSL sessions over the optimized link is needed. Cisco WAAS enables optimization of SaaS deployment models by providing a simple solution to streamline SSL connection setup and eliminate security problems.

Benefits of Cisco WAAS Optimization

To understand how Cisco WAAS benefits SaaS deployment, consider the way that SSL connections are optimized. When a connection is requested, 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, and to the SSL server it appears as the SSL client. To act as the SSL server, the data center WAN optimization device needs an authentication certificate for each SSL service it is optimizing. When the WAN optimization device intercepts a connection request from a client, it uses the SSL server IP address to associate the certificate with the client. Since the device typically optimizes multiple SSL services, it can have many SSL certificates to manage.

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 at an SaaS provider, the SSL server IP address is not controlled by the IT administrator, and many servers may be used for a single SaaS service. Additionally, the SSL server IP address may change at any time, requiring the WAN optimization device to be reconfigured.

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 the IP address changes. Using DNS hostnames works well for SAAS applications with few servers; however, for larger deployments, where hostnames often change, additional automation is needed. For these use cases, Cisco WAAS provides the capability of DNS domain recognition, in which the IT administrator specifies the DNS domain suffix - for example, *.webex.com - and the associated certificate. With this information, Cisco WAAS can automatically associate SSL connections with domains and supply the correct certificate to the client.

Conclusion

By simplifying optimization of SSL- and HTTPS-secured SaaS applications, Cisco WAAS helps IT departments lower the cost of SaaS deployments, reduce the amount of WAN bandwidth needed, and improve end-user productivity. IT operating costs to deliver large-scale SaaS deployments are reduced through the use of simplified configurations. 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. As a result, Cisco WAAS provides a 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 productivity applications such as Salesforce.com, Cisco WebEx, and Microsoft SharePoint.

For More Information

http://www.cisco.com/go/waas

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 C11-574893-00 01/10