Cisco Wide Area Application Services SSL Acceleration Technical Overview

What You Will Learn

Secure Socket Layer version 3 (SSLv3), also known as Transport Layer Security version 1 (TLSv1) is one of the most common protocols used to encrypt content transported over IP networks. The significant growth in the use of SSL/TLS-secured applications, including both web-based and non-web-based applications, suggests the need to apply policy-based WAN optimization to the secured traffic. Recently, the use of SSL/TLS to encrypt content within the enterprise has been growing steadily and rapidly. There are also many customers who have not yet deployed SSL in the enterprise but who want to help ensure that when they do implement SSL in the future, they will benefit from a WAN optimization solution.

Cisco® Wide Area Application Services (WAAS) is a comprehensive WAN optimization and application acceleration solution that is a key component of Cisco Borderless Networks and Data Center 3.0 solutions. Cisco WAAS accelerates applications and data over the WAN, optimizes bandwidth, empowers cloud computing, and provides local hosting of branch-office IT services, all with industry-leading network integration. Cisco WAAS allows IT departments to centralize applications and storage while maintaining productivity for branch-office and mobile users.

Cisco WAAS provides SSL optimization capabilities that integrate transparently with existing data center key management and trust models and can be used by both WAN optimization and application acceleration components. Private keys and certificates are stored in a secure vault on the Cisco WAAS Central Manager. The private keys and certificates are distributed in a secure manner to the Cisco WAAS devices in the data center and stored in a secure vault, maintaining the trust boundaries of server private keys. SSL optimization through Cisco WAAS is fully transparent to the end users and servers and requires no changes to the network environment.

Cisco WAAS also provides simplified management and deployment of the SSL optimization throughout the enterprise, as well as an enhanced management experience for a large deployment. The autodiscovery mechanism in Cisco WAAS provides full support for automatic identification, interception, optimization, and acceleration of SSL traffic even in environments in which the clients are configured to use explicit proxies.

Challenge

Among the several cryptographic protocols used for encryption, SSL/TLS is one of the most important. SSL/TLS-secured applications represent a growing percentage of traffic traversing WAN links today. Encrypted secure traffic represents a large and growing class of WAN data. Standard Data Redundancy Elimination (DRE) techniques cannot optimize this WAN data because the encryption process generates an ever-changing stream of data, making even redundant data inherently nonreducible and eliminating the possibly of removing duplicate byte patterns. Without specific SSL optimization, Cisco WAAS can still provide general optimization for such encrypted traffic with Transport Flow Optimization (TFO). Applying TFO to the encrypted secure data can be helpful in many situations in which the network has a high bandwidth delay product (BDP)[1] and is unable to fill the pipe.

Specific SSL optimization requires termination of the SSL session and decryption of the traffic to apply optimizations such as Cisco WAAS DRE and Lempel-Ziv (LZ) compression techniques to the data. Minimally, SSL optimization requires the capability to:

[1] BDP is the maximum amount of data traveling across the WAN link between the two endpoints at any given time. BDP is calculated by multiplying a data link's capacity in bits per second and its end-to-end latency in seconds.

- Decrypt traffic at the near-side Cisco WAAS Wide Area Application Engine (WAE) and apply WAN optimization on the resulting clear-text data
- Reencrypt the optimized traffic to preserve the security of the content for transport across the WAN
- Decrypt the encrypted and optimized traffic on the far-side Cisco WAAS WAE and decode the WAN optimization
- Reencrypt the resulting original traffic and forward it to the destination origin server

The capability to terminate SSL sessions and apply WAN optimization to encrypted data requires access to the server private keys. Further, the clear-text data received as a result of decryption must be stored on the disk for future reference to gain the full benefits of DRE. These requirements pose serious security challenges in an environment in which data security is paramount. Security by itself is the most important and sensitive aspect of any WAN optimization solution that offers SSL acceleration.

To be considered a total solution ready for enterprise deployment, SSL optimization must meet these security requirements:

- The solution must not compromise the security of private keys. Private key trust boundaries must be honored, and the keys must not be distributed beyond the secure data center. The private keys and certificates should be stored in a secured electronic vault in the data center.
- Data storage encryption of stored information must be provided under all circumstances to prevent unauthorized access due to device theft or hard-drive removal.
- The key for the disk encryption must not be stored on the disk and should be retrieved over a secure link from a secured central management system and then kept only in memory to help ensure data security on the disk in case of a disk loss.

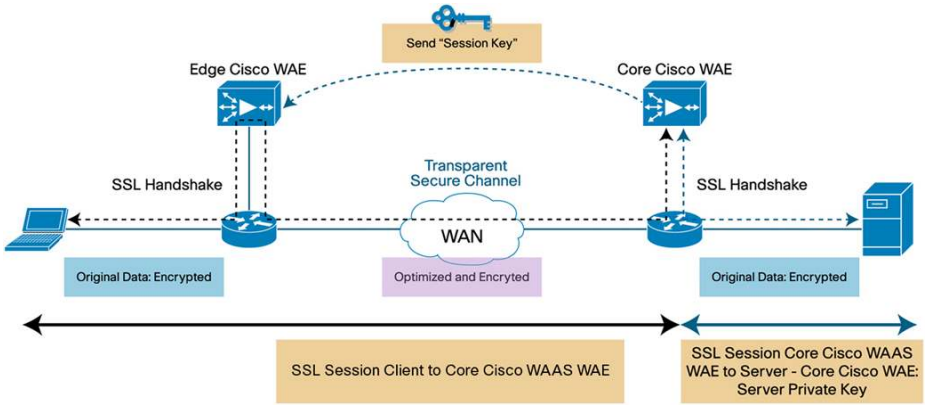
Another key aspect of the solution is transparency. Clients and servers should not be aware of, nor require configuration to operate in a special manner with, the WAN optimization for SSL. Specifically, clients and servers should not be aware of the existence of any WAN optimization devices, and should not be required to change their proxy or other settings. The SSL acceleration should be compatible with all types of client browser proxy settings including autodetection and explicit proxy configuration.

Cisco WAAS SSL Optimization Benefits

Cisco WAAS is an industry-leading, comprehensive WAN optimization and application acceleration solution. Cisco WAAS includes SSL optimization that integrates transparently with the existing Public Key Infrastructure (PKI) trust model in customer deployments and can be easily deployed without compromising the existing data center key management security.

With Cisco WAAS, the SSL trust model is maintained in the data center. Server private keys are stored securely in the data center on the core Cisco WAAS WAEs and Central Managers and are never pushed to the branch office. Temporary SSL session keys are distributed from the secure core Cisco WAEs to edge Cisco WAEs over a secure HTTPS connection between an edge and a core Cisco WAE. The Cisco WAAS SSL Application Optimizer operates in a completely transparent mode that does not require any changes to the client or destination server. Figure 1 shows how Cisco WAAS SSL optimization integrates transparently with existing application key exchanges and preserves the trust boundaries of server private keys.

Figure 1. Cisco WAAS SSL Optimization



- During the initial client SSL handshake, the core Cisco WAE in the data center participates in the conversation. The connection between Cisco WAEs is established securely using the Cisco WAE device certificates and the Cisco WAEs cross-authenticate each other.
- After the client SSL handshake is completed and the data center Cisco WAE has the session key, the Cisco WAE will transmit the session key (which is temporary) over its secure link to the edge Cisco WAE so that it can start decrypting the client transmissions and apply DRE.
- The optimized traffic is then reencrypted using the Cisco WAE peer session key and transmitted, in-band, over the current connection and maintaining full transparency, to the data center Cisco WAE.
- The core Cisco WAE decrypts the optimized traffic, reassembles the original messages, and reencrypts the messages using a separate session key negotiated between the server and the data center Cisco WAE.
- If the back-end SSL server asks the client to submit an SSL certificate, the core Cisco WAE will request one from the client. The core Cisco WAE will authenticate the client by verifying the SSL certificate using a trusted certificate authority (CA) or an Online Certificate Status Protocol (OCSP) responder.

Unlike other solutions that provide SSL support and only partial integration into existing security architectures, the Cisco WAAS SSL Application Optimizer provides significant advantages:

- Simple, easy to deploy architecture: The architecture allows creation of aggregated services with additional support for wildcard certificates and IP addresses.
- Preservation of trust boundary: Cisco WAAS does not distribute private keys beyond the secure data center Cisco WAAS devices.
- Scalable secure storage of keys: All certificates and private keys are stored securely on the Cisco WAAS Central Manager and distributed to the Cisco WAAS devices only in the data center. The private keys are never distributed to the edge Cisco WAAS devices.
- Disk encryption: Encryption can be enabled selectively or globally with disk encryption keys managed by the Cisco WAAS Central Manager. This approach helps ensure that data written to the Cisco WAAS device disks is completely unusable should a Cisco WAAS device be compromised.
- Interoperability with existing proxy infrastructure: Cisco WAAS provides full support for automatic identification, interception, optimization, and acceleration of SSL traffic even in environments in which web proxies have already been deployed or in which clients are configured to use explicit proxies.
- OCSP support: By providing support for OCSP, Cisco WAAS improves security with a real-time security check of certificates.
- Client authentication support: Full support is provided for client certificate-based authentication during initial session establishment.

- Role-based access control (RBAC): The Cisco WAAS Central Manager RBAC framework allows controlled access to SSL configuration and monitoring.

Cisco WAAS SSL Optimization Architecture Solution: Simple, Scalable, and Easy to Deploy

Cisco WAAS offers the industry's most comprehensive yet easy-to-deploy SSL optimization architecture. The Cisco WAAS solution enables highly flexible configuration of SSL accelerated services and offers significant advantages:

- SSL accelerated services configuration supports wildcard certificates and any IP. It also supports use of multiple IP addresses and TCP ports per service. A single SSL accelerated service can be used to aggregate multiple back-end servers.
- Cisco WAAS supports a wide variety of certificate formats including Privacy Enhanced Mail (PEM) and Public-Key Cryptography Standards 12 (PKCS12). Cisco WAAS supports certificate chaining and provides the option of self-signed certificates for a quick proof-of-concept mode. Cisco WAAS also can generate Certificate Signing Requests (CSRs).
- Cisco WAAS provides a default list of root certificate authorities and supports the addition of new certificate authorities.
- The SSL accelerated service supports ciphers ranging from stream ciphers to block ciphers. Cisco WAAS also supports the Diffie-Hellman key exchange method, which is the default option on popular browsers and servers such as Firefox and Apache. The default cipher suite includes all the encryption and MAC methods included in FIPS 140-2.
- The SSL accelerated service supports both SSLv3 and TLS by default. Additionally, the SSL accelerated service offers the capability to customize protocol selection and restrict protocol use.

Preservation of Trust Model in the Data Center

The Cisco WAAS SSL Application Optimizer requires the private keys to be stored only on the Cisco WAAS devices in the data center, and the keys are never required on the Cisco WAAS devices in the remote branch offices. This approach helps ensure the security of the private keys by restricting them from leaving the secure data center.

Secure Storage of Certificates and Keys on Cisco WAE

The Cisco WAAS SSL application optimizer requires that all imported and generated certificates or private keys used for peering and optimization services be stored encrypted in a secure store (PKI store) located on an internal file system and protected by a single encryption key. The secure store is used for all certificates and keys that Cisco WAAS needs for SSL service. The secure store is encrypted using the same passphrase as is used for disk encryption. However, the secure store functions independently from the disk encryption service. The secure store is used whenever SSL services are deployed.

The Cisco WAAS Central Manager provides management of encryption services for all Cisco WAAS devices in the network, including the secure vault for encryption key pairs and keys necessary for Cisco WAAS device disk encryption. All sensitive data used or generated by a Cisco WAAS deployment is stored and transmitted in a secure manner.

Central Manager Backup and Recovery

The Cisco WAAS Central Manager is designed for enterprise scalability and can be deployed in highly available and redundant configurations. In high-availability mode, one Cisco WAE acts as the primary Cisco WAAS Central Manager, and one or more other WAEs serves as a backup Cisco WAAS Central Manager. The Cisco WAAS Central Manager provides an enterprise class key-backup and key-recovery solution that mitigates many of the risks involved in manual backup and recovery options. The Cisco WAAS Central Manager allows backup of the encrypted store files from the secure vault with the Central Management System (CMS) backup option. The certificates and

private key entries are encrypted using the encrypted store password. In high-availability mode, the primary Cisco WAAS Central Manager distributes the secure vault contents to the standby backup Cisco WAAS Central Manager to be stored in its secure vault.

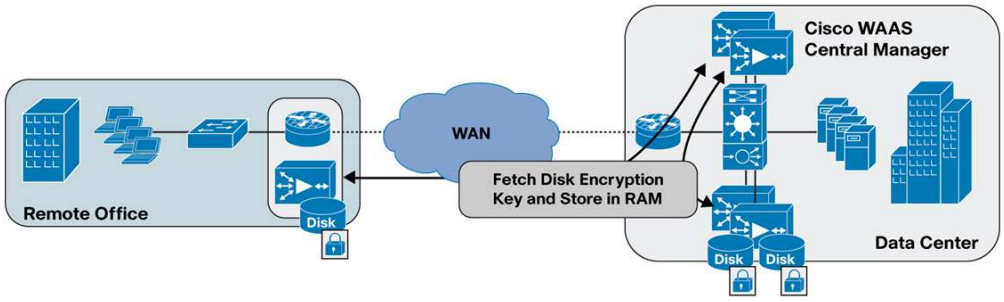
Disk Encryption and Key Management

To achieve the full benefits of DRE caching and compression, the Cisco WAAS SSL Application Optimizer decrypts the SSL-encrypted data and stores the byte patterns on the disk in a low-level format in clear text. This confidential data stored on a physical disk drive needs to be protected against theft just as the SSL-encrypted data traversing the WAN is protected. Typically it is easy to physically secure the Cisco WAAS devices in the data center, but in the remote branch offices this is not always the case. To secure and protect sensitive data in a potentially unsecure remote location, it is strongly recommended as a best practice that disk encryption be implemented to safeguard the stored data on the disk.

Cisco WAAS disk encryption mitigates the risk of data leakage should a device or drive be physically compromised or stolen. Disk encryption uses Advanced Encryption Standard (AES) 256-bit encryption, the strongest commercially available encryption, to encrypt data stored on the disk.

Disk encryption can be enabled selectively or globally with disk encryption keys managed by the Cisco WAAS Central Manager, helping ensure that data written to Cisco WAAS device disks is completely unusable should a system be compromised in any way. This security helps ensure compliance with Payment Card Industry (PCI) regulation and other initiatives such as federal and industry-related compliance rules (Figure 2).

Figure 2. Cisco WAAS Disk Encryption



Key management for disk encryption is performed using Cisco WAAS Central Manager and agent component software on the Cisco WAAS WAE device. The Cisco WAAS Central Manager provides a secure store that serves as a central repository for the disk encryption keys for all the Cisco WAE appliances. The agent software that runs on the Cisco WAE device is responsible for retrieving the disk encryption key from the Cisco WAAS Central Manager upon a Cisco WAE reboot. This approach to key management provides:

- **Highly scalable disk encryption solution:** Encryption keys are never stored on the Cisco WAE appliance itself, preserving data security in case the Cisco WAE appliance or hard disk is lost or stolen.
- **Reduced complexity:** There is no need to manage separate encryption keys for each Cisco WAE.
- **Automatic recovery:** In the event of a Cisco WAE reboot, the Cisco WAE will automatically retrieve the disk encryption key from the Cisco WAAS Central Manager.

The main threat this feature addresses is unauthorized access to a customer's sensitive data stored on a Cisco WAE that has been stolen and is no longer connected to the customer's network. Encrypting the data storage of the Cisco WAE is one aspect of the feature; another is the secure key management for this storage. A Cisco WAE may be stolen, but the decryption key does not reside in the stolen device, rendering the disk's content useless. In normal operation with a secure connection to the Cisco WAAS Central Manager, the key will be automatically retrieved upon a Cisco WAE reboot and allow normal functioning of the device.

Since sensitive information regularly flows through deployed Cisco WAAS systems and is occasionally stored in Cisco WAAS persistent storage, all such Cisco WAAS devices should be securely protected with disk encryption.

Certificate Revocation Check (OCSP)

Certificates may be revoked by a certification authority for various reasons. For example, if a certificate and its associated key are compromised or need to be retired for any reason, the certification authority may revoke the existing certificate. Certificate authorities keep a list of certificates they have issued and, for revocation purposes, maintain a Certificate Revocation List (CRL). Entities that need to perform certificate revocation checks must periodically download these CRLs. An alternative process is through the use of OCSP. Certification authorities can provide an online service called an OCSP responder, which can be used to check the revocation status of a certificate issued by the certification authority. Anyone can contact the OCSP responder, supply information about the certificate, and learn the certificate's revocation status.

Cisco WAAS supports OCSP for the real-time revocation status of a certificate in compliance with the U.S. Department of Defense (DoD) Class 3 PKI definition. This feature is especially useful in highly secure environments, where OCSP can provide the real-time status of a certificate. OCSP is also useful in cases in which client certificates are used in the SSL handshake for client authentication.

Client Authentication Using Client Certificates

When running in an SSL-protected session, the server and client can authenticate one another and negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. Client certificates provide an additional way to authenticate a client to a server using SSL.

Cisco WAAS supports client authentication and can verify the client before allowing the SSL session with the server to proceed. Client certificate authentication is commonly deployed in highly secure environments, in which message-layer authentication mechanisms using user IDs and passwords, or tokens, are not considered sufficient from a security standpoint.

SSL Tunneling Using HTTP Proxy

Many customer environments have web browsers either configured to use explicit web proxies with URL filtering or configured for automatic proxy detection and configuration. When the web browser is set for HTTP or HTTPS and the user requests a connection using https://<sitename>, the HTTP protocol uses its CONNECT method to establish an SSL tunnel. The client first establishes a TCP connection with the proxy and then sends an HTTP CONNECT method request to the proxy, instructing the proxy to establish a TCP connection with the requested server on port 443. Cisco WAAS can detect these SSL connection requests going through a web proxy, apply SSL optimization to these connections, and enable automatic support of SSL optimization in environments regardless of whether a web proxy is deployed.

Simplified Deployment Model for Cloud-Based Services

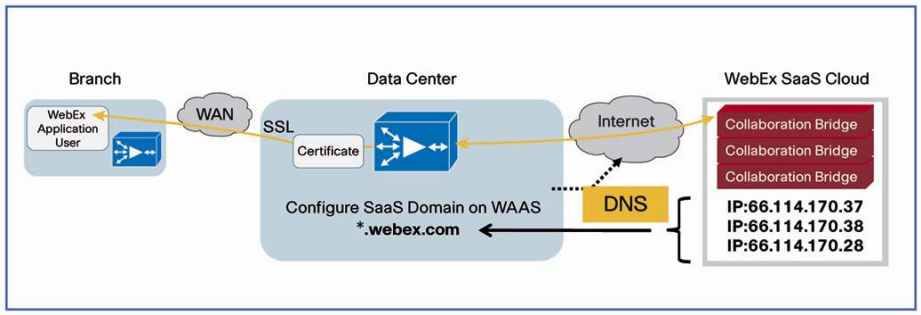
Cloud-based software-as-a-service (SaaS) providers such as WebEx.com and Salesforce.com primarily use HTTPS to securely deliver services to their clients. Using Cisco WAAS SSL Application Optimizer, Cisco WAAS can optimize delivery of these services to the remote branch-office users who connect to these services through a backhaul connection to the data center.

However, the solution poses some unique challenges related to simplifying the implementation and deployment model. Typically, SaaS providers have multiple SSL server farms with multiple hosts spanning several data centers. When a client initiates an SSL connection request to a server located in the SaaS server farm, the Cisco WAAS SSL Application Optimizer needs to map the destination IP address in the incoming SSL request to an SSL accelerated service to present the right SSL certificate to the client to perform an SSL handshake.

For SSL services that are 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 Cisco WAAS. But for an SSL service hosted at a third-party SaaS provider cloud, the SSL server IP address is not controlled by the IT administrator. Also, there may be not just one but multiple server IP addresses even for a single SaaS service, and these may be subject to change.

To simplify the deployment model for SaaS optimization, Cisco WAAS provides support for domain names in the SSL accelerated service configuration. This model can be applied to any cloud-based SaaS applications such as Salesforce.com and WebEx.com. For example, when an SSL accelerated service is configured in the data center Cisco WAE with a wildcard domain name (for instance, *.webex.com) option, the Cisco WAAS SSL Application Optimizer performs a reverse Domain Name System (DNS) lookup on the destination server IP upon receiving an SSL connection request from the client, and if the IP address resolves to a host that matches the configured wildcard domain name (for instance, *.webex.com), then the appropriate SSL accelerated service policy is applied to this connection (Figure 3).

Figure 3. Simplified Deployment for SaaS Optimization



Cisco WAAS provides flexible options to choose from when selecting the SSL server certificate to associate with the SaaS services to be accelerated and optimized. Cisco WAAS can support the original SSL server certificate and private key if that is available from the service provider; otherwise, a self-signed wildcard domain certificate or an enterprise certificate authority signed wildcard domain certificate can be used in place of the original SSL server certificate.

RBAC for Managing Cisco WAAS SSL Application Optimizer

The Cisco WAAS Central Manager allows the Cisco WAAS system to be provisioned so that the various administrative groups requiring control have access to only those portions of the Cisco WAAS topology that they need. Using RBAC, a Cisco WAAS administrator can define administrative users, roles, and domains to specify the areas of the Cisco WAAS Central Manager that users can view and control. The Cisco WAAS Central Manager provides a RBAC framework to enable controlled access to Cisco WAAS SSL Application Optimizer configuration and data. The Cisco WAAS Central Manager provides RBAC SSL-specific rights to the users, including:

- Access to SSL configuration and certificate authorities (read-only or read-write),
- Access to capability to change and export SSL service certificates and private keys (import-export)
- Access to capability to change device certificates and private keys (import-export)
- Access to SSL statistics for each device (read)

Performance Improvements with SSL Acceleration

Cisco WAAS SSL acceleration can provide significant improvement for applications encrypted through SSL and operating over the WAN. The SSL acceleration capabilities of Cisco WAAS provide the full benefits of WAN optimization by applying DRE data reduction, persistent LZ compression, and TCP optimization to the SSL data, which results in lower bandwidth utilization, better utilization of WAN capacity, and faster application performance.

For example, Cisco WAAS provides substantial performance improvement for Microsoft SharePoint Portal as shown in Figures 4 and 5. In this example, Cisco WAAS was deployed with SSL acceleration in an environment with T1 WAN bandwidth, 120 milliseconds (ms) of round-trip latency, and 0.5 percent packet loss.

Figure 4. Cisco WAAS Optimizes Data Transfer from Microsoft SharePoint Portal

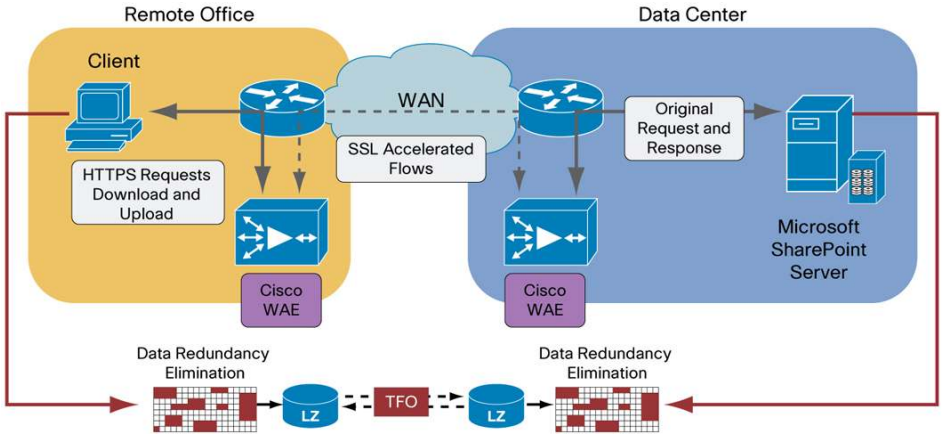
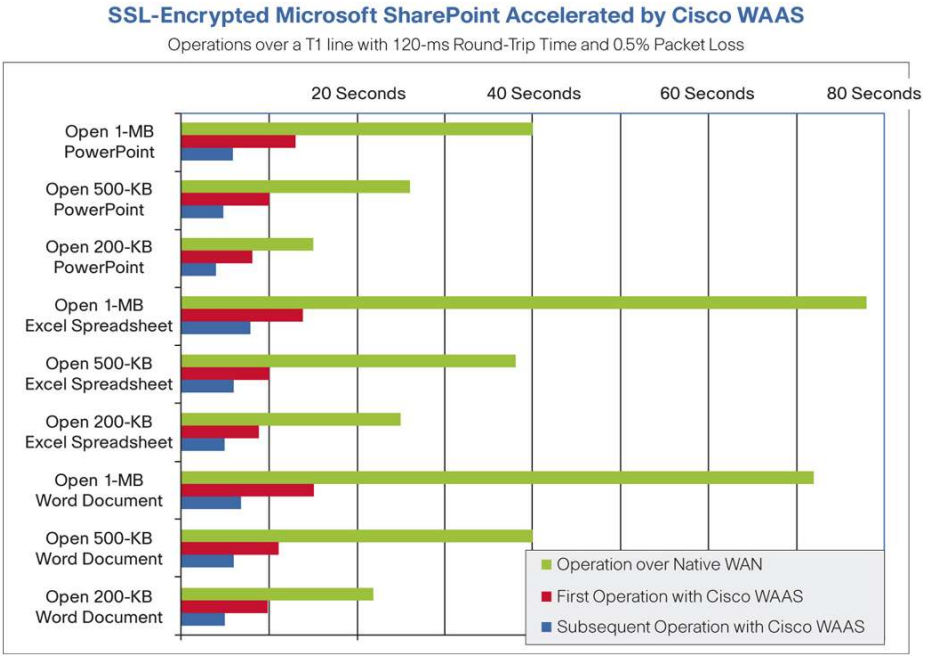


Figure 5. Cisco WAAS Optimizes SSL-Encrypted Data Transfer from Microsoft SharePoint Portal



Conclusion

The growing use of SSL/TLS-secured applications suggests the need to apply policy-based WAN optimization to secured traffic. Cisco WAAS provides the industry's most comprehensive set of SSL acceleration and WAN optimization capabilities that preserve the existing security architecture and provide a scalable key management secure vault. Cisco WAAS SSL optimization is easy to configure and maintain, requiring no changes to the existing client and server environments and working transparently with Internet-facing proxy servers. Cisco WAAS SSL optimization also supports OCSP and client authentication using digital certificates. Cisco WAAS SSL optimization can now help IT departments consolidate their SSL/TLS-secured application infrastructure from distributed sites into the secure data center while providing the optimizations necessary to improve application and data access performance over the WAN.

For More Information

For more information please visit 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 C22-532534-01 06/10