Cisco Wide Area Application Services Software Version 5.1 Technical Overview

What You Will Learn

Enterprises face numerous challenges in the delivery of applications and critical business data to the enterprise edge. As the global workforce continues to become more distributed, providing adequate service levels throughout the organization becomes increasingly difficult, causing IT departments to deploy costly and difficult-to-manage infrastructure at each location, including file services, email, video, software distribution, and print services. With continuous pressure from industry and federal regulation, IT departments now face the significant challenge of consolidating this costly infrastructure into the data center or onto scalable, virtualized branch-office application-delivery platforms to improve data protection, security, and availability, while maintaining the service level that the distributed workforce has come to expect.

Furthermore, as applications continue to become more complex and robust, delivering applications and application information to the enterprise edge becomes increasingly challenging and expensive. In today's environment, IT managers face increasing pressure to reduce application-delivery costs over the WAN while helping ensure application availability and agility with the adoption of virtualization and cloud computing. However, poor application response time experienced by users in remote sites is often cited as one of the main inhibitors of cloud adoption. The latency of the WAN or Internet link between the data center and cloud location and the user at the remote site adversely affects the performance of business applications. A solution to the application performance challenge is to make WAN optimization a part of the cloud infrastructure.

As discussed in this document, Cisco® Wide Area Application Services (WAAS) accelerates applications and data over the WAN, optimizes bandwidth, empowers cloud services, 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.

Challenge

IT budgets are not increasing to match the growing expectations that executives have for IT resources. Almost every IT department that manages a distributed infrastructure wants to consolidate costly remote-office infrastructure into the data center or onto scalable, virtual branch-office application-delivery devices to control capital expenditures (CapEx) and operating expenses (OpEx). Furthermore, as applications continue to evolve and become larger and more complex, the network load grows and the performance characteristics of the WAN affect application delivery even more. The challenges of data-retention policies and business-continuance, disaster-recovery, and compliance requirements exacerbate the problem, given a heavily distributed infrastructure and already overburdened WAN environment.

Having a centralized IT infrastructure enables CapEx and OpEx savings while streamlining data-protection processes. Many vendors have attempted to solve such problems with point products that do not effectively allow IT departments to take advantage of existing investment in network intelligence. Furthermore, cloud-based models are likely to change the consumption model for technology, allowing enterprises to increase their business agility and save costs through on-demand provisioning and deprovisioning of infrastructure and services using a utility-based chargeback model.

Cisco WAAS Solution for the WAN

Cisco WAAS delivers a comprehensive, cost-effective, cloud-ready WAN optimization solution. Cisco WAAS accelerates applications, optimizes bandwidth, provides local hosting of branch-office IT services, and enables a smooth evolution to cloud-based services. Cisco WAAS improves end-user productivity by accelerating application delivery and improves IT staff productivity by simplifying service integration, while maintaining a low total cost of ownership (TCO) and increasing business agility with network integration. Cisco WAAS enables organizations to accomplish crucial business objectives such as these:

- Enhance productivity by mitigating the effects of WAN latency. Applications perform better, and data is transferred faster.
- Offer a superior end-user application experience by enabling rich-media applications and live and on-demand video streaming with high performance without affecting the performance of other applications across the WAN.
- Allow migration of business applications to the cloud and deliver high-performance cloud services and software-as-a-service (SaaS) applications without affecting application performance for end users at remote branch offices, campuses, and data centers.
- Reduce bandwidth consumption, delaying or eliminating increased recurring bandwidth costs. Cisco WAAS enables IT consolidation, reducing both CapEx and recurring expenses for branch-office IT infrastructure.
- Lower operating costs by providing on-demand WAN optimization with integration into Cisco Integrated Services Routers Generation 2 (ISR G2) routers through Cisco IOS® Software-based Cisco WAAS Express and Cisco WAAS on Services-Ready Engine (SRE) Modules.

Figure 1 shows a typical customer deployment using Cisco WAAS.

Figure 1.　　Cisco WAAS Deployment Architecture
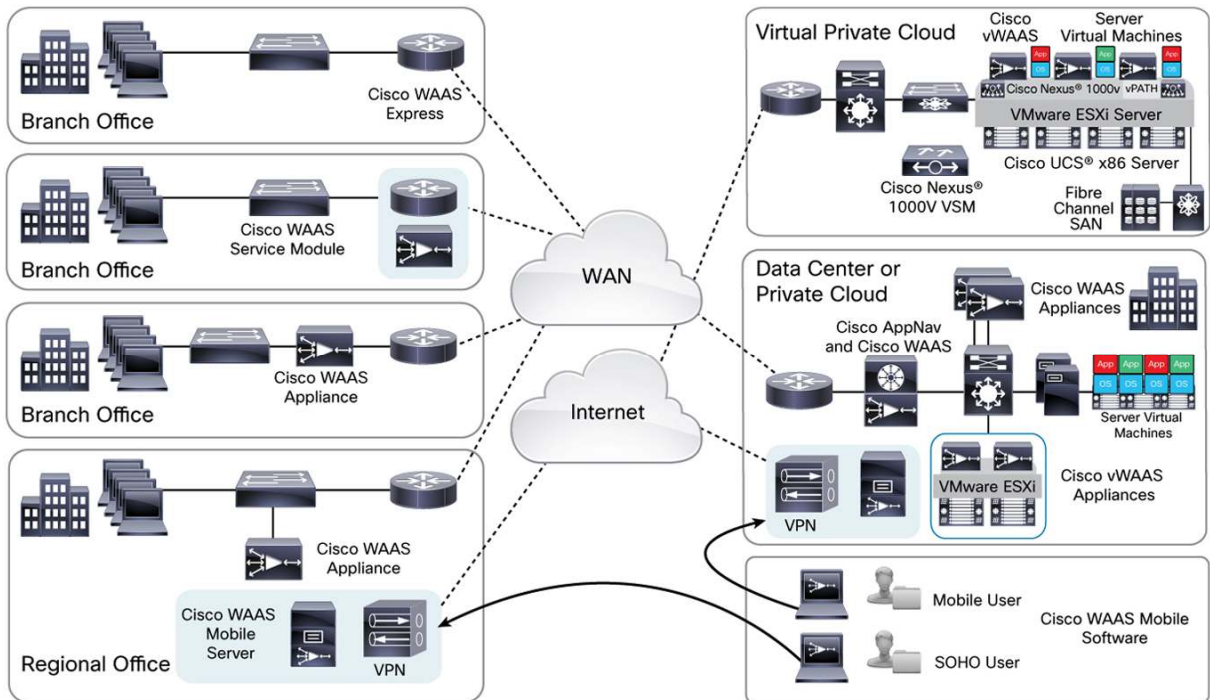
Cisco WAAS is deployed on a physical appliance, virtual appliance, router-integrated services module, or router-integrated Cisco IOS Software on each side of the WAN to provide application-specific acceleration and WAN optimization capabilities. You can deploy Cisco WAAS Appliances out of the data path or physically in-path in the data center or in the remote branch office, and you can deploy Cisco WAAS network modules as well as service modules out-of-path in the branch office. Regardless of the deployment model, Cisco WAAS provides application performance improvements and enables centralization without compromising high availability and scalability by providing intelligent load distribution and fail-through operation.

Figure 2 shows how Cisco WAAS devices, deployed on each end of a WAN link, optimize application traffic by using optimized connections over the WAN.

Figure 2.　　Cisco WAAS Optimizes Connections over the WAN
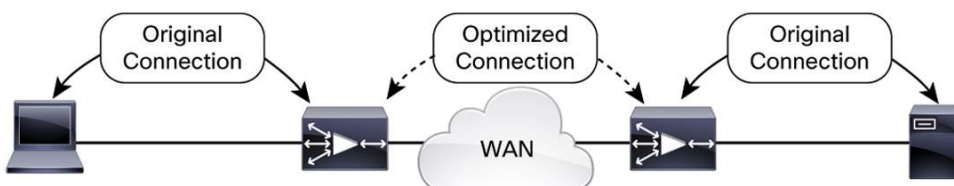
Cisco WAAS allows IT departments to:

- Consolidate and virtualize data centers
- Deliver desktop virtualization
- Deploy new, rich-media applications
- Deliver high-performance cloud services and software-as-a-service (SaaS) applications
- Optimize organization branch-office sites with reduced network and IT infrastructure
- Optimize bandwidth for rich media and telepresence
- Manage bandwidth expenses
- Protect remote data and help ensure business continuity for regulatory compliance

Cisco WAAS facilitates such benefits through a series of optimizations that are not only safe for all applications, but also validated by the application vendors themselves while also being transparent to clients, servers, and the network itself:

- Application-vendor-validated protocol-specific acceleration: Cisco WAAS provides application-specific acceleration features that are validated by application vendors themselves for both encrypted and unencrypted applications. These techniques for improving application performance over the WAN reduce the effects of latency and bandwidth use through protocol acceleration, read-ahead, operation batching, multiplexing, and safe caching. The result is full correctness with the protocol specification, full coherency of data, and a dramatically improved user experience when compared with native WAN access. Applications include Microsoft file services (Common Internet File System [CIFS]) and Microsoft Exchange Messaging API Remote Procedure Call [MAPI-RPC]), plus numerous other application protocols.
- Advanced protocol-agnostic WAN optimization: Cisco WAAS provides powerful WAN optimization capabilities that overcome limitations associated with the movement of data over the WAN. Cisco WAAS can compress data in flight using long-lived compression techniques including standards-based compression and Context-Aware Data Redundancy Elimination (DRE). Coupled with TCP optimizations that enable more intelligent and high-performance use of the network, the result is a significant reduction in network bandwidth consumption, more efficient network use, improved application throughput, and LAN-like performance for remote-office users and inter-data center applications.
- Branch-office consolidation through virtual blades: Cisco WAAS uniquely provides customers with the capability to consolidate application infrastructure on scalable, high-performance Cisco WAAS Appliances for applications that must remain in the branch office. Cisco WAAS provides virtual blade support for Microsoft Windows Server 2008 R2 with its entire suite of applications. Furthermore, Cisco WAAS support for Microsoft Windows Server 2008 R2 adheres to the Microsoft Server Virtualization Validation Program (SVVP).

With Cisco WAAS, almost every TCP-based application can benefit from the network and application-specific acceleration techniques, including Internet and intranet, database, file service, file transfer, email, data protection, virtual desktop infrastructure (VDI), client-server, data protection, video streaming and video on demand (VoD), and Secure Sockets Layer (SSL)-encrypted applications.

Figure 3 shows the Cisco WAAS new-generation Cisco Wide Area Virtualization Engine (WAVE) appliances and high-performance connectivity options.

Figure 3.   Cisco WAAS WAVE Appliances and Connectivity Options
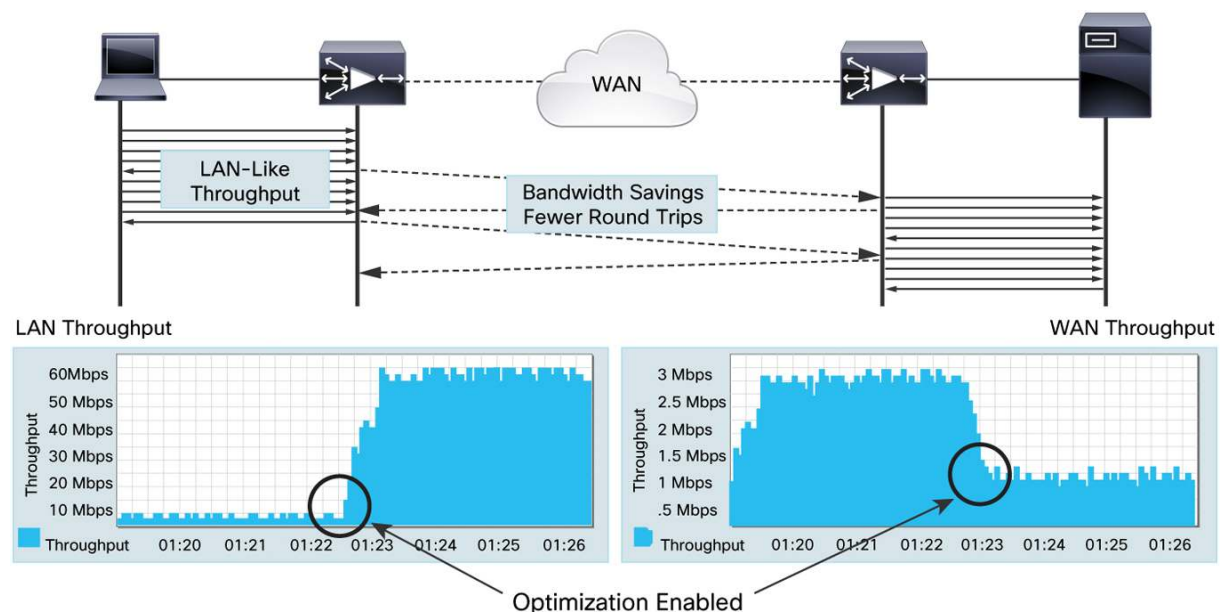

WAN Optimization with Cisco WAAS

Cisco WAAS provides numerous WAN optimization capabilities that help improve application performance and mitigate the need for costly WAN bandwidth upgrades. By employing a series of techniques ranging from TCP optimization to advanced cross-protocol data suppression, all working together, Cisco WAAS helps ensure that application data traverses the WAN more efficiently, thereby improving application performance and user productivity. Additionally, you can apply these capabilities to plain-text or SSL-encrypted traffic, thereby allowing you to improve productivity and performance for critical enterprise applications.

Figure 4 summarizes the WAN optimization capabilities of Cisco WAAS.

Figure 4.   Effects of Cisco WAAS WAN Optimization Features

Transport Flow Optimization

The Cisco WAAS transport flow optimization (TFO) feature provides optimizations that help improve TCP behavior under problematic WAN conditions to meet challenges associated with packet loss, congestion, recovery, and long fan networks (LFNs). With Cisco WAAS TFO, communicating nodes are shielded from WAN conditions, and Cisco WAAS devices manage WAN conditions on behalf of the nodes to help ensure that available capacity can be used advantageously, the effect of packet loss and congestion is mitigated, and throughput is increased. TFO maintains packet-network friendliness and safe coexistence with other network nodes communicating using standard TCP implementations. TFO provides adaptive buffering to help ensure that connections requiring additional memory to achieve higher throughput are automatically given appropriate system resources without compromising fairness among other optimized and nonoptimized connections. Optimizations provided as part of TFO include large initial windows, advanced congestion-avoidance algorithms, and slow-start mitigation.

Figure 5 shows how the Cisco WAAS device acts as a TCP proxy to shield communicating nodes from WAN conditions and employs other optimizations, including the Cisco WAAS DRE and Persistent Lempel-Ziv (PLZ) compression features.
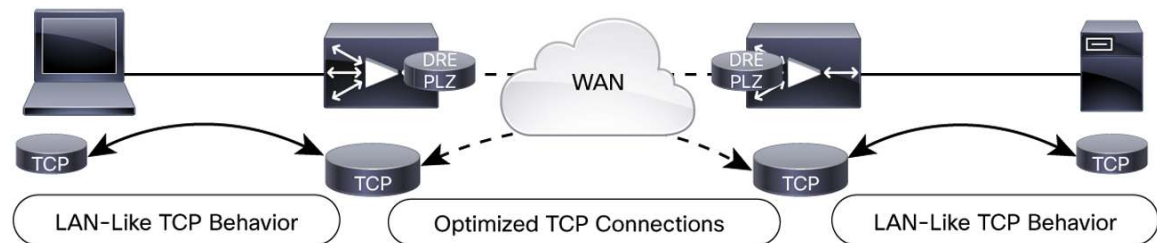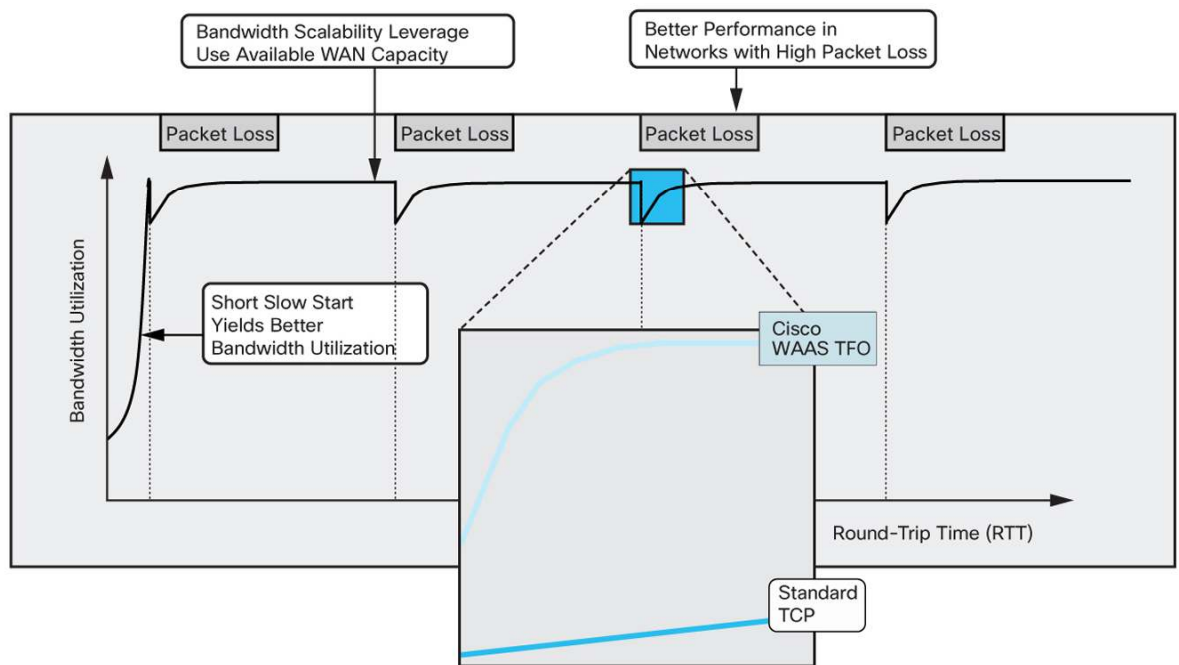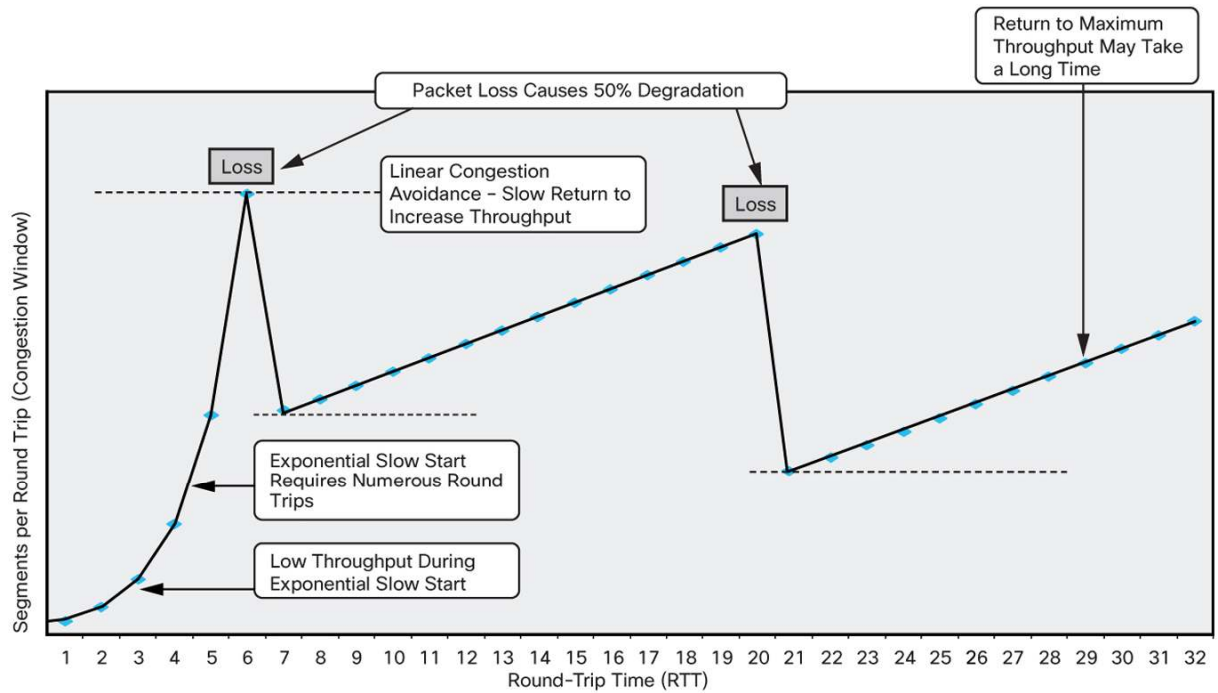
Figure 5.   Cisco WAAS TFO

Figure 6 shows the benefits of Cisco WAAS TFO for TCP behavior and application performance of TCP-based applications.

Figure 6. Cisco WAAS TFO Enables Efficient Usage and Improves Application Performance

Data Redundancy Elimination

Cisco WAAS DRE is a Context-Aware DRE implementation that includes application intelligence and inspects TCP traffic to identify redundant data patterns at the byte level and then quickly replaces them with signatures if they have been previously seen so that the peer Cisco WAAS device can use them to reproduce the original data. There are two types of data traffic:

- Transactional: Transactional traffic moves between the client and the server on the same TCP connection and includes email send and receive traffic and file uploads and downloads. Typically, all traditional client and server application traffic is in this category.
- Directional: Directional traffic tends to travel in only one direction on the same TCP connection. Examples are traffic from VDI screen scrapping, video streams, and cloud-based applications such as backup. This type of traffic flow represents a new trend in applications.

Emerging applications require new approaches to DRE architecture, so Cisco WAAS has introduced three modes of Context-Aware DRE:

- Bidirectional DRE: Data chunks and signatures are written to the disk on both the sender- and receiver-side Cisco Wide Area Application Engines (WAEs) to provide optimal compression.
- Unidirectional DRE: Only signatures are written on the sender-side Cisco WAE, and both signatures and data chunks are written on the disk on the receiver-side Cisco WAE. In addition to providing optimal compression, this mode effectively uses the DRE cache for higher scalability.
- Adaptive DRE: Context-Aware DRE intelligently chooses between the bidirectional and unidirectional DRE caching mechanism, depending on the type of application traffic.

  Context-Aware DRE also stores signatures in the data center (headend) Cisco WAE on a per-branch-office basis, and the actual data chunks are shared across branch offices. The tight synchronization of branch-office signatures combined with shared chunks of data across branch offices helps provide consistent, reliable, and fair DRE performance for all branch offices. Figure 7 shows the architecture of Cisco WAAS Context-Aware adaptive DRE.

**Figure 7.**   Cisco WAAS Context-Aware Adaptive DRE
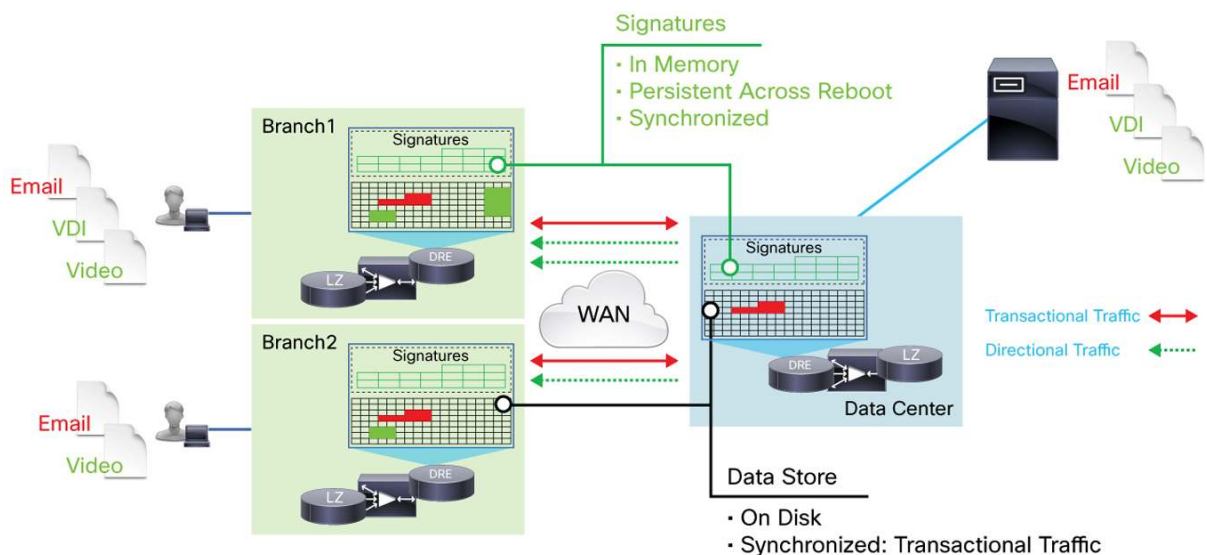
PLZ Compression

Cisco WAAS implements PLZ compression with a connection-oriented compression history to further reduce the amount of bandwidth consumed by a TCP connection. You can use PLZ compression in conjunction with DRE or independently. It provides up to an additional 5:1 compression, depending on the application used and the data transmitted, in addition to any compression that DRE offers.

SSL Optimization

Cisco WAAS provides SSL optimization capabilities that integrate transparently with existing data center key management and trust models that both WAN optimization and application acceleration components can use. Encryption key pairs are stored securely in a secure vault on the Cisco WAAS Central Manager and distributed securely to the Cisco WAAS devices in the data center to be stored in a secure vault.

Figure 8 shows how Cisco WAAS SSL optimization integrates transparently with existing application key exchanges and preserves the trust boundaries of server private keys.

Figure 8.   Cisco WAAS SSL Optimization
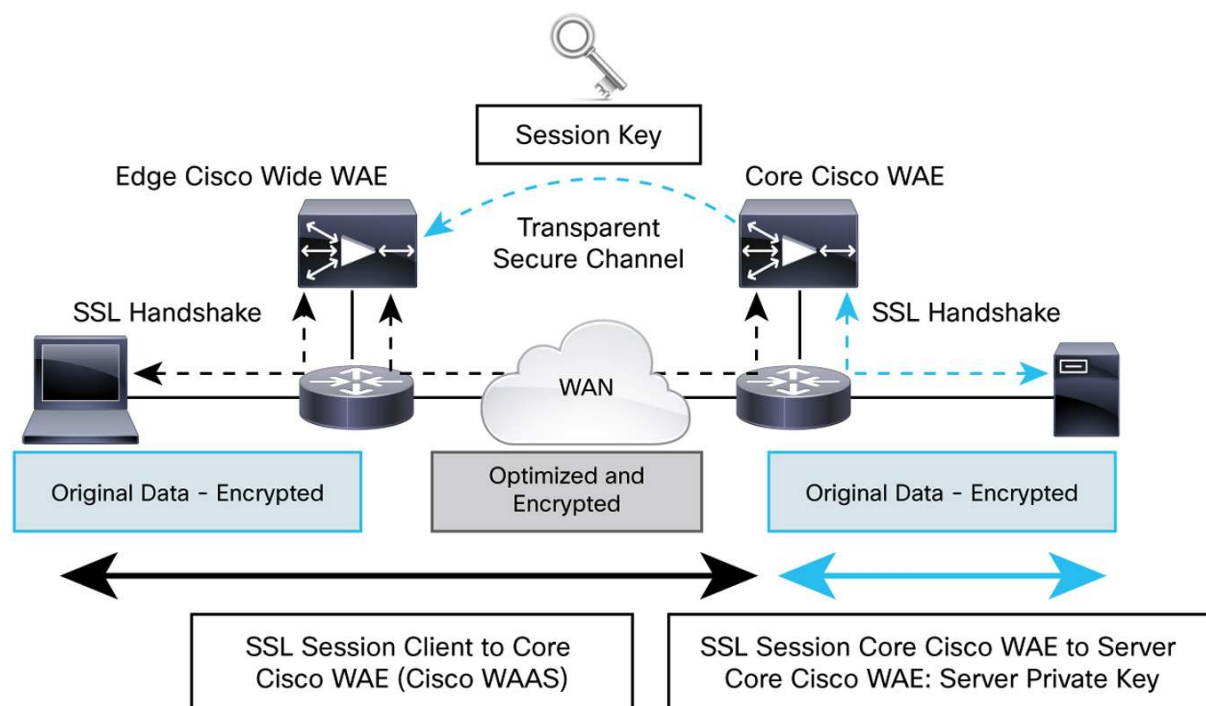
Other solutions provide only partial integration into existing security architectures. Cisco WAAS SSL optimization provides the following advantages over older WAN optimization solutions that provide SSL support:

- Preservation of trust boundary: Cisco WAAS does not distribute private keys beyond the data center Cisco WAAS devices.
- Secure storage of keys: All certificates and private keys are stored securely on the Cisco WAAS Central Manager.
- 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 clients are configured to use explicit proxies.

- Client authentication support: Cisco WAAS provides full support for client certificate-based authentication during initial session establishment.
- Online certificate status protocol support: By providing support for the Online Certificate Status Protocol (OSCP), Cisco WAAS can provide a real-time security check of certificates to improve security.
- SSL services on the SaaS provider cloud: Cisco WAAS can simplify the configuration needed to handle the large numbers of IP addresses and IP address changes required by SSL services hosted through a third-party SaaS provider cloud.
- HTTP optimization techniques: Cisco WAAS SSL optimization uses HTTP optimization techniques such as local HTTP responses through the metadata cache, DRE hints, and server compression offload. Refer to the section "HTTP Acceleration" later in this document for more information.

Citrix XenDesktop and XenApp Optimization

Cisco WAAS is a Citrix Ready certified solution that helps ensure a high-quality user experience for Citrix CenDesktop and XenApp. The solution - which is jointly tested, validated, and supported by Cisco and Citrix - provides optimization transparently, requiring no changes to existing Citrix infrastructure. Figure 9 shows the components of Cisco optimization for Citrix XenDesktop and XenApp solutions:

- Citrix XenDesktop delivers desktops and applications hosted on virtualized infrastructure in the data center.
- Cisco WAAS, deployed on both sides of the WAN, optimizes Citrix HDX traffic between the end users and the data center using a sophisticated combination of TCP optimizations that reduce the effects of the WAN, persistent session-based compression, and sophisticated algorithms to reduce data redundancy in Citrix HDX traffic.
- Cisco WAAS Central Manager is used to manage the Cisco WAAS solution from a central point, reducing operation burdens and costs.

Figure 9.   Cisco Optimization for Citrix XenDesktop and XenApp Solution Components
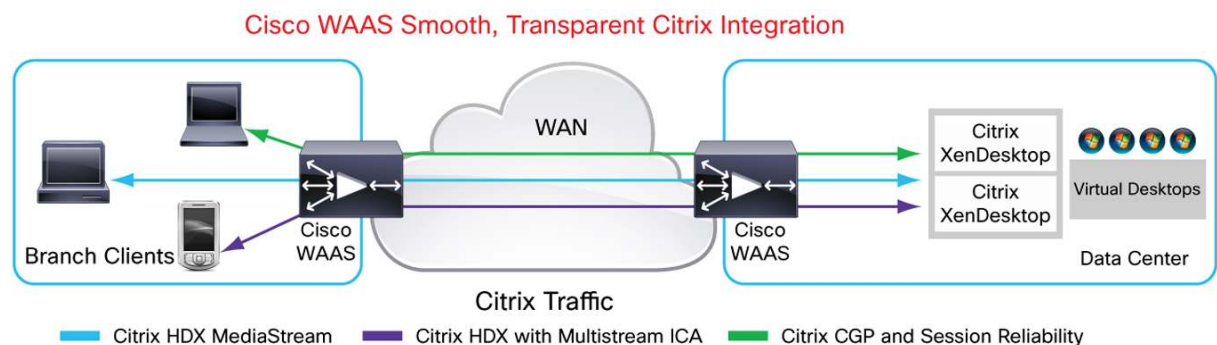
The Cisco WAAS with Citrix XenDesktop and XenApp solution offers the following benefits:

- Full support for Citrix XenDesktop and XenApp: Cisco WAAS optimization techniques are applicable to Citrix XenDesktop and XenApp deployments.
- Transparent to Citrix encryption: You can transparently insert Cisco WAAS into encrypted communications (Basic and RC5) without requiring changes to the Citrix configuration or infrastructure.
- Full compatibility with Citrix MultiStream ICA (MSI) and the ability to apply differentiated-services-code-point (DSCP) tagging of both MSI and non-MSI ICA and Citrix Common Gateway Protocol (CGP) traffic.

- Full compatibility with Citrix Session Reliability (CGP) including enhanced optimization for CGP.

- Full compatibility with Citrix HDX MediaStream: Citrix HDX MediaStream exposes media stream, which enables Cisco WAAS optimization of the streaming media protocol.

- Context-Aware DRE: Directional understanding of data enables best performance as well as increased bandwidth savings as a result of improved compression.

Application Acceleration with Cisco WAAS

Cisco WAAS provides application-specific acceleration capabilities that, unlike competitive solutions, have been approved by the application vendors themselves. Along with reducing the negative effects of latency and bandwidth and providing tremendous improvements in response time and performance, Cisco WAAS application acceleration offers the reassurance that the vendors that produce the applications being optimized fully support the acceleration capabilities of Cisco WAAS. Application-acceleration capabilities provided in Cisco WAAS work in conjunction with WAN optimization features and help mitigate the negative effects of the WAN by providing safe caching, protocol acceleration, message batching, read-ahead, write-behind, stream splitting, and more. Cisco WAAS supports a broad range of applications accelerated through application-specific support, including CIFS, Microsoft Windows Print Services, Network File System (NFS), MAPI, HTTP, Secure HTTP (HTTPS), and enterprise video.

Figure 10 shows how Cisco WAAS application acceleration improves application performance while offloading servers and preserving application semantics.

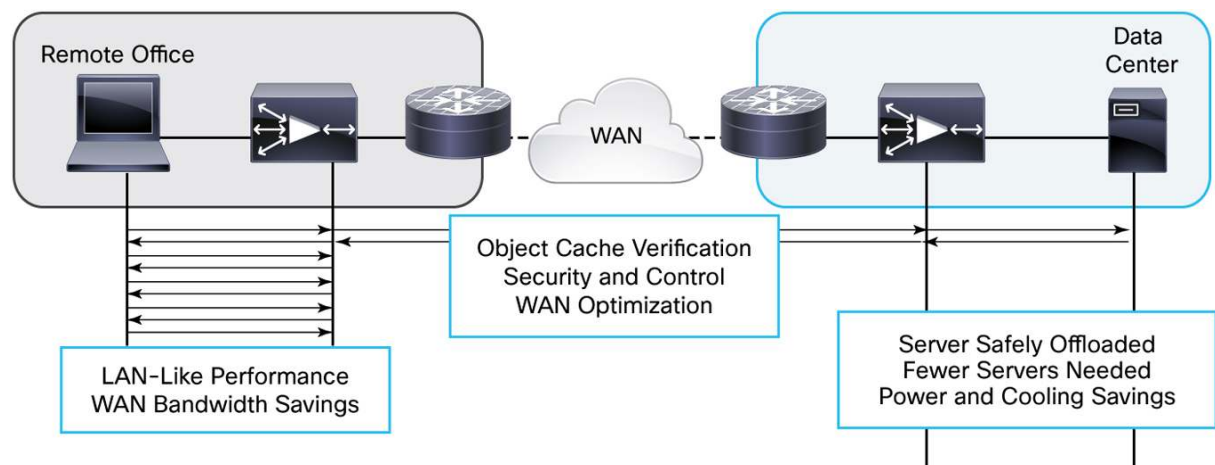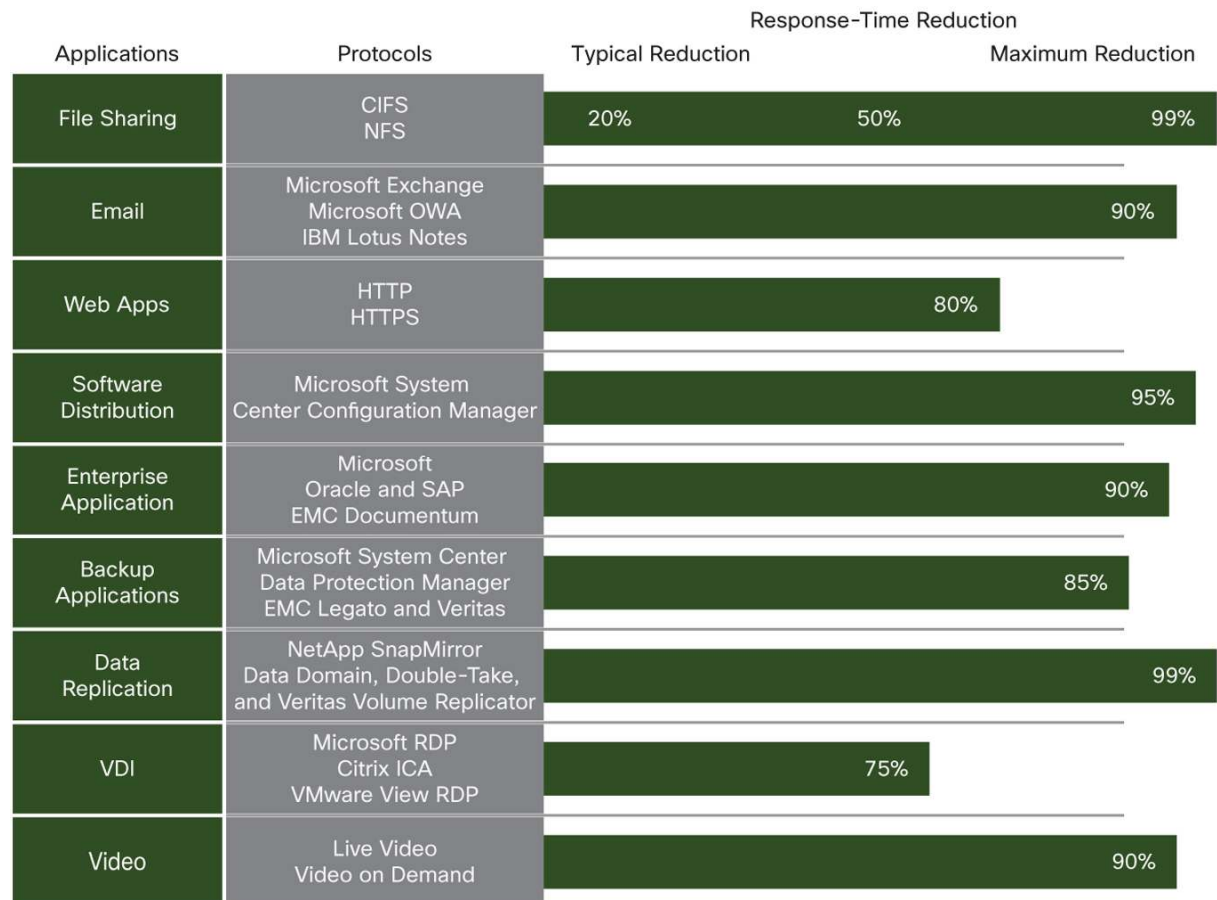**Figure 10.**   Cisco WAAS Application Acceleration

Figure 11 shows the typical and peak performance improvements provided by Cisco WAAS.

Figure 11. Typical and Peak Performance Improvements Provided by Cisco WAAS

CIFS, Microsoft Windows Print, and Server Message Block Acceleration

Building on the industry-leading capabilities provided in Cisco WAAS Software Version 4.0, Cisco WAAS Software Version 4.1 provided enhancements to CIFS acceleration to further improve performance and streamline operations, resulting in simplified deployment of services to enable consolidation of distributed file and print resources in the data center without compromising performance. Cisco WAAS Software Version 5.0 adds acceleration for Server Message Block Version 2 (SMBv2) and signed SMBv2 protocols.

Cisco WAAS can provide the following acceleration capabilities for CIFS:

- Safe data and metadata caching: By caching copies of objects and metadata, Cisco WAAS can reduce the transmission of CIFS data over the WAN, thereby providing tremendous levels of optimization for branch-office users accessing file servers in the data center. All data is validated against the server for coherency to help ensure that a user never receives out-of-date (stale) data.

- Read-ahead: For situations in which objects are not cached or cannot be cached, Cisco WAAS employs read-ahead to bring the data to the user more quickly. Read-ahead reduces the negative effects of latency on CIFS by requesting the data on behalf of the user. This data can then be used, when safe, to respond to the user on behalf of the server.

- Message pipelining: CIFS messages can be pipelined over the WAN to mitigate the effects of send-and-wait behavior of CIFS. This feature allows operations to occur in parallel rather than serially, thus improving performance for the user.

- Prepositioning: File server data and metadata can be copied in a scheduled manner to improve performance for first-user access. This feature is helpful in environments in which large objects must traverse the WAN, including software distribution, video, and desktop-management applications.

- Microsoft Windows printing acceleration: Cisco WAAS can intelligently accelerate CIFS printing traffic over the WAN to allow centralization of print services in the data center. This feature helps reduce the branch-office infrastructure without compromising printing performance and is transparent to the existing printer and queue-management architectures.

- Intelligent file server offloading: Cisco WAAS CIFS acceleration reduces the burden placed on the origin file server through advanced caching techniques that can serve data locally to the requesting user when the user is authenticated and authorized and the cached contents are validated as coherent with the origin file server. Thus, file servers see fewer requests and are required to transfer less data, thereby enabling file server scalability and better economics.

- Invalid File ID: Cisco WAAS can deny requests to access files with invalid file handle values locally instead of sending the requests to the server, thus improving performance for the user.

- Batch close optimization: Cisco WAAS can perform asynchronous file close optimization for file-sharing traffic.

- Signed SMBv2: SMBv2 message signing is supported.

HTTP Acceleration

Oracle, SAP, Microsoft SharePoint, and other applications are central to today's enterprise organization. Cisco WAAS provides acceleration capabilities for enterprise applications that use HTTP, reducing bandwidth consumption and improving WAN efficiency and also mitigating the negative effects of latency in the WAN for these applications. By employing latency mitigation capabilities along with powerful WAN optimization capabilities, organizations can achieve a substantial increase in the responsiveness of enterprise applications accessed over the WAN, greatly enhancing branch-office user productivity.

Cisco WAAS provides the following acceleration capabilities for enterprise applications:

- Fast connection reuse: Connection reuse decreases the load time for complex pages or pages with numerous embedded objects when the client or server cannot use persistent connections. Optimized connections on the WAN remain active for a short time period so that they can be reused if additional data between the client-server pair needs to be exchanged.

- Connection multiplexing: Rather than requiring that multiple connections be established between client-server pairs, connections established between clients and servers are reused. This feature eliminates the latency caused by the process of establishing multiple connections between clients and servers.

- Local response: Use of cached metadata allows Cisco WAAS branch-office devices to respond locally to certain HTTP requests. These local responses are based on cached metadata from previously seen server responses and are continuously updated. This powerful HTTP optimization feature greatly reduces protocol chattiness and helps improve application response times through faster page downloads.

- Enhanced SharePoint: Cisco WAAS SharePoint Optimization provides specific optimization benefits for Microsoft Office documents hosted on a 2010 Microsoft SharePoint Server. The SharePoint feature provides optimization by prefetching objects for Word or Excel and storing them in the Cisco WAAS metadata cache. This optimization saves Round-Trip Time (RTT) for each successful fetch to reduce latency from the client's point of view and improve overall user experience.

- Content-aware optimization: The Cisco WAAS advanced HTTP parser provides intelligent recommendations that make DRE more effective and enable offloading of compression from the server resources.

MAPI Acceleration

Microsoft Exchange email relies on MAPI, used over RPCs, to deliver email, calendaring, contacts, and more to Microsoft Outlook users for collaboration and productivity. As with many applications, the performance of Microsoft Exchange is hampered by the bandwidth limitations and latency found in the WAN. Cisco WAAS provides many acceleration services for Microsoft Exchange to help improve performance. Unlike other solutions that provide acceleration for Microsoft Exchange, Cisco WAAS acceleration is developed in conjunction with Microsoft to help ensure correctness and compatibility with all major versions of the application, without relying on reverse engineering of protocols.
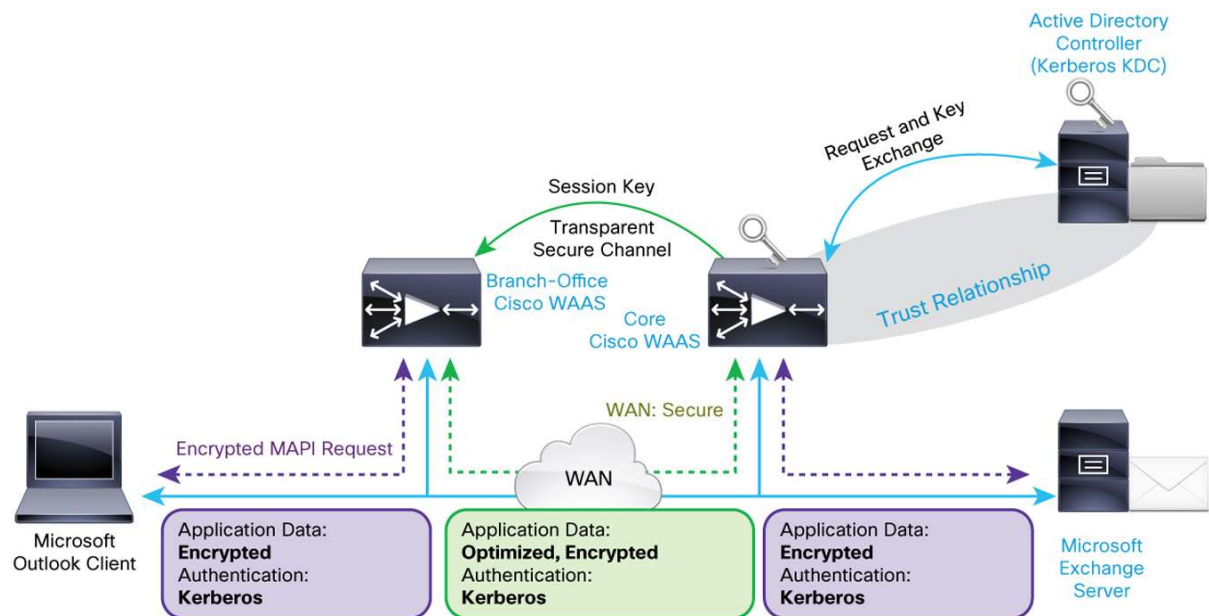
Cisco WAAS provides the following acceleration capabilities for Microsoft Exchange:

- Full application support: Cisco WAAS acceleration for Microsoft Exchange is developed in conjunction with Microsoft to help ensure full compatibility with all major versions, including Microsoft Outlook 2000, 2003, and 2007, and the same versions of Microsoft Exchange.

- Advanced email compression: Cisco WAAS can automatically defer native compression provided by the Microsoft Exchange Server and Microsoft Outlook in favor of Cisco WAAS DRE and PLZ compression. Additionally, Cisco WAAS can natively decode messages encoded by Microsoft Exchange or Outlook to provide additional levels of compression, and full data coherency is preserved end to end.

- Object read-ahead: Objects being fetched from the server, such as email, calendar items, and address books, are fetched at an accelerated rate because Cisco WAAS prefetches objects on behalf of the user. This feature helps mitigate the effects of the send-and-wait behavior of Microsoft Exchange and Outlook.

- Object delivery acceleration: Objects being sent to the server, such as email, folder updates, and calendar entries, are sent at an accelerated rate because of the pipelining and batching capabilities provided by Cisco WAAS.

- Payload aggregation: Cisco WAAS recognizes many Microsoft Exchange messages that are small and can either batch them for optimized delivery or dynamically adjust DRE and PLZ compression to improve compression ratios for these messages.

- Transparent integration: Cisco WAAS acceleration for Microsoft Exchange does not keep user sessions open as in other solutions, a situation that can lead to security vulnerabilities and limit the overall scalability of the Microsoft Exchange Server itself.

Encrypted MAPI Optimization

Cisco WAAS provides Encrypted MAPI (E-MAPI) optimization that integrates transparently with the existing Microsoft Active Directory trust model and allows Layer 7 optimization for encrypted communications using proprietary Microsoft encrypted RPC protocols. Figure 12 shows how Cisco WAAS E-MAPI optimization integrates transparently with the trust model while preserving user-intended boundaries and security goals.

Figure 12.   Cisco WAAS E-MAPI Optimization

Other solutions provide only partial integration with the network security architecture. Cisco WAAS E-MAPI optimization provides a complete and cohesive solution to meet user-defined security objectives and offers the following advantages:

- It maintains trust boundaries and does not distribute the private keys of the data center.
- Keys are dynamically retrieved from Active Directory on demand and are never permanently stored on any Cisco WAAS device.
- E-MAPI acceleration interoperates transparently for all network interception methods and does not require special handling.
- Application transparency allows E-MAPI acceleration without the need to make changes to application clients or application servers.
- Outlook 2007, 2008, 2009, and 2010 are supported (supporting a mix of encrypted and unencrypted traffic).

NFS Acceleration

Cisco WAAS provides robust protocol acceleration for UNIX environments in which the NFS protocol is used for file exchange. In conjunction with the powerful WAN optimization capabilities provided by Cisco WAAS, NFS acceleration helps improve file access performance - both interactive access and access during file transfer - by mitigating the negative effects of latency and bandwidth constraints.

The capabilities for NFS acceleration provided by Cisco WAAS include:

- Metadata optimization: Cisco WAAS pipelines interactive operations such as directory traversal to reduce the amount of time required to traverse directories and view file and directory metadata. Additionally, Cisco WAAS caches metadata when safe to do so, to reduce the number of performance-limiting operations that traverse the WAN.

- Read-ahead optimization: Cisco WAAS performs read-ahead operations on behalf of the requesting node to prefetch data from the file being accessed. This feature makes the data readily available at the edge device for faster read throughput.
- File write optimization: Asynchronous write operations are used to batch write messages and eliminate the send-and-wait behavior of NFS file write operations while working in conjunction with existing NFS protocol semantics to help ensure file data integrity.

Video Delivery Services

One of the most challenging applications to deploy enterprisewide is business video, including streaming video (live video) and VoD. Cisco WAAS provides a series of optimizations that help improve video delivery and meet the challenges normally present when deploying video enterprisewide. Cisco WAAS video-delivery services reduce the burden that video places on the network while providing an architecture that helps ensure high-quality broadcast performance and playback for remote users.

Figure 13 shows the effects of Cisco WAAS video-delivery services on user performance, WAN bandwidth, and server scalability.

Figure 13.   Cisco WAAS Video-Delivery Services
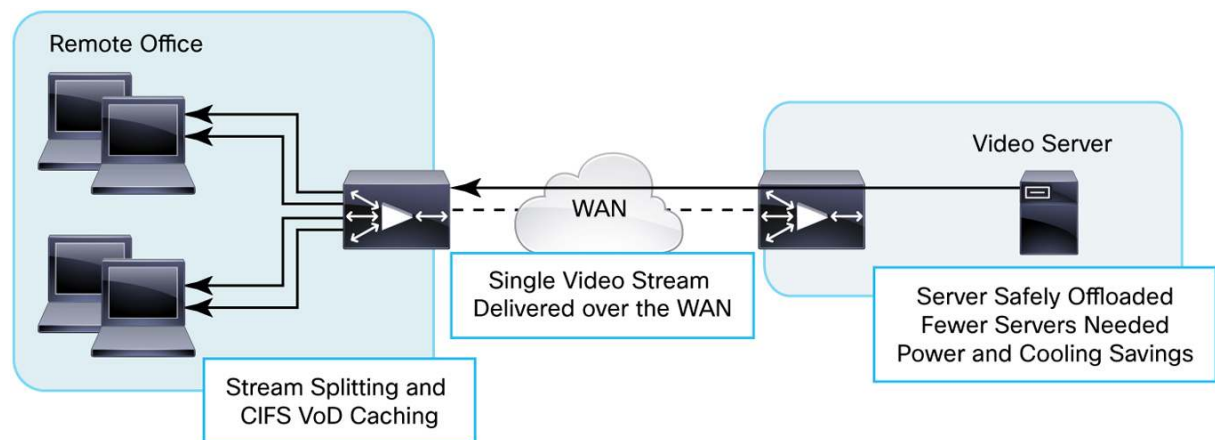
Cisco WAAS provides the following optimizations for video delivery:

- Microsoft Windows Media stream splitting: Cisco WAAS interoperates with Microsoft Windows Media Technologies (WMT) over the Real Time Streaming Protocol (RTSP) to enable one video stream over the WAN to be served to numerous users in the remote branch office, thereby reducing bandwidth consumption of video traffic.
- Data reduction and optimization for non-WMT and non-RTSP video: Cisco WAAS provides WAN optimization and bandwidth reduction for other video formats, including video over HTTP, Adobe Flash, Apple QuickTime, RealVideo, and any other video protocol that uses TCP as a transport.
- VoD caching: You can use Cisco WAAS CIFS acceleration in conjunction with prepositioning to provide a powerful VoD delivery architecture for enterprise e-learning, training, and video message archiving and playback.

- Intelligent video server offloading: Cisco WAAS video-delivery services reduce the burden on the origin video server by intelligently multiplexing remote-user requests over a single connection per location. Thus, video servers see fewer connections and are required to serve less data, thereby enabling video server scalability.

Cisco Virtual WAAS: The First Cloud-Ready WAN Optimization Solution

Cisco Virtual WAAS (vWAAS) is the industry's first cloud-ready WAN optimization solution. Cisco vWAAS is a virtual appliance that accelerates business applications delivered from private and virtual private cloud infrastructures, helping ensure an optimal user experience. Cisco vWAAS runs on the VMware ESXi hypervisor and Cisco Unified Computing System™ (Cisco UCS®) x86 servers, providing an agile, elastic, and multitenant deployment.

Cisco vWAAS is the only WAN optimization solution that is deployed in an application-specific, virtualization-aware, and on-demand manner. Using policy-based configuration in the Cisco Nexus® 1000V Switch, Cisco vWAAS service is associated with application server virtual machines as they are instantiated or moved. This approach enables cloud providers to offer rapid delivery of WAN optimization services with little network configuration or disruption in cloud-based environments.

Cisco IOS Software WAN Optimization Solution on Cisco ISR G2 Routers with Cisco WAAS Express

Cisco WAAS Express extends the Cisco WAAS product portfolio with a small-footprint, cost-effective solution based on Cisco IOS Software and integrated into Cisco Integrated Services Routers Generation 2 (ISR G2) routers to offer bandwidth optimization and application-acceleration capabilities. Cisco WAAS Express increases remote-user productivity, reduces WAN bandwidth costs, and offers investment protection by interoperating with existing Cisco WAAS infrastructure. Cisco WAAS Express is unique in providing network transparency, improving deployment flexibility with on-demand service enablement, and integrating with native Cisco IOS Software services such as security, NetFlow, and quality of service (QoS). Furthermore, there is no need for configuration of inline or Web Cache Communication Protocol (WCCP) interception mechanisms. As soon as the feature is enabled for specific interfaces, the default optimization policy will apply to traffic entering and leaving the interface. Cisco WAAS Express uses a combination of TFO, LZ compression, and DRE caching to optimize the traffic, and it provides select application support for file, web, and SSL traffic.

Branch-Office Consolidation with Cisco WAAS

In addition to providing powerful WAN optimization and application acceleration services, which enable infrastructure consolidation and performance improvements, Cisco WAAS is also a branch-office infrastructure consolidation platform that allows you to migrate critical branch-office services to the extensible Cisco WAAS Appliance platform using virtualization through virtual blades. Some Cisco WAAS Appliances have an embedded hypervisor and services for resource provisioning that allow enterprises to deploy Microsoft Windows on Cisco WAAS safely, securely, efficiently, and transparently along with other operating systems and platforms. This feature allows customers to retain certain crucial services in the branch office, including Microsoft Active Directory, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), print services, and other vendor-validated applications and services, while using far less infrastructure hardware than was previously thought possible.

Resources for the virtual blades are provisioned centrally on the Cisco WAAS Central Manager for unified and centralized management, allowing enterprises to specify the number of CPUs, the amount of memory, and the amount of disk capacity to allocate to each virtual blade on each Cisco WAAS device. You can then transfer a virtual blade boot image to the remote Cisco WAAS device in an optimized or unoptimized manner, and then mount and initialize the image. You can delegate administration, ownership, and ongoing management of the virtual blade to the appropriate IT business stakeholder to help ensure transparent integration into the existing business process. Furthermore, virtual blade computing and network performance, as well as overall usability, is greatly enhanced by support for multiple CPUs, I/O paravirtualization, and remote network boot installation (preexecution environment [PXE]).

Virtual blades on Cisco WAAS provide the following business benefits:

- Lower TCO: Fewer infrastructure devices are required at the branch office, thereby reducing power, cooling, and rack-space requirements, along with ongoing operating expenses (OpEx) and capital expenditures (CapEx).
- Transparent integration: Integration into existing Microsoft management technologies, including Microsoft Management Console (MMC) and network services such as Active Directory, is transparent, and Cisco WAAS can fully optimize and accelerate access to the virtual blade.
- Platform and service isolation: Dedicated resources (CPU, memory, and disk) are allocated to the virtual blade, thereby isolating resources from interference from other virtual blades or from the underlying WAN optimization and application acceleration services.
- IT agility: You can deploy infrastructure services and applications throughout the network in a way that provides outstanding flexibility.

Today, the Cisco WAAS virtual blade solution supports the Cisco Application and Content Networking System (ACNS) Virtual Blade, and Cisco Network Analysis Module (NAM) Virtual Blade. The Cisco ACNS Virtual Blade allows Cisco ACNS Software to run on a Cisco WAAS virtual blade and be managed from the Cisco Content Distribution Manager (CDM). The primary Cisco ACNS personality supported and intended for the Cisco ACNS Virtual Blade is the Content Delivery Engine (CDE). You can also use the Cisco ACNS Virtual Blade as a Content Distribution Manager (CDM). The Cisco NAM Virtual Blade integrates a Cisco NAM with a Cisco WAAS virtual blade to help identify applications and services that would benefit from optimization, quantify the effects of WAN optimization, and perform throughput analysis of LAN and WAN bandwidth.

## Simple, Scalable, Secure Network Integration with Cisco WAAS

Cisco WAAS offers the industry's most complete set of network integration capabilities that preserve investment in existing networking architectures without compromising scalability or network stability. You can deploy Cisco WAAS devices as router-integrated network modules, providing the industry's lowest TCO for the branch office. With their impressive scalability for the data center, Cisco WAAS devices offer industry-leading density and lower power, cooling, and rack-space costs when compared to alternative solutions.

Transparency

Cisco WAAS provides network transparency for both the LAN and the WAN to help ensure investment protection for network services that have already been deployed, are under consideration for deployment, or may be deployed in the future. By preserving packet header information, including IP addresses (source and destination) and port numbers (source and destination), value-added network services can continue operation even in the presence of the optimization and acceleration capabilities that Cisco WAAS provides.

Figure 14 shows how Cisco WAAS transparency preserves packet header information.

Figure 14. Cisco WAAS Transparency Preserves Packet Header Information
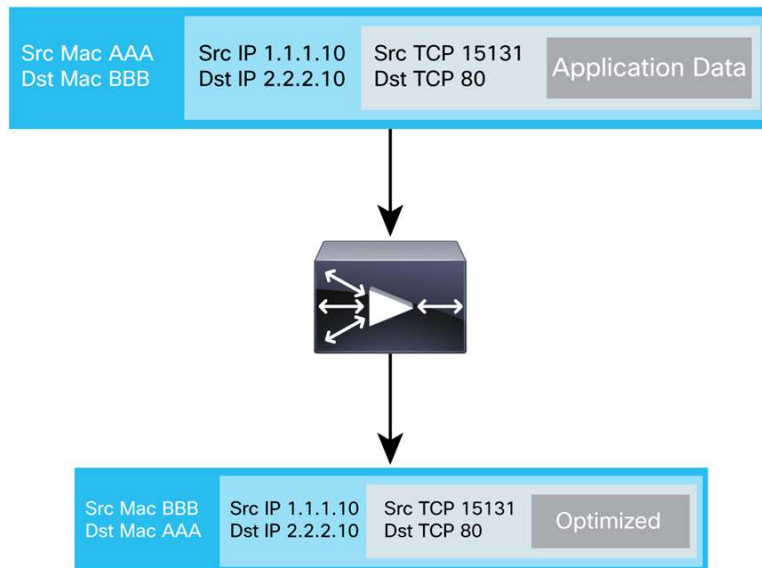

Cisco WAAS transparency helps ensure compatibility with services including the following:

* Network QoS: Cisco WAAS preserves DSCP markings, or alternatively can apply DSCP markings through application QoS, working together with classification, policing, and shaping in the network. Network classification is preserved because the header information is not manipulated, thereby enabling Cisco WAAS to interoperate with network-based classification techniques for QoS.

Figure 15 shows how you can deploy Cisco WAAS in conjunction with network QoS.

Figure 15. Cisco WAAS Complements Network QoS
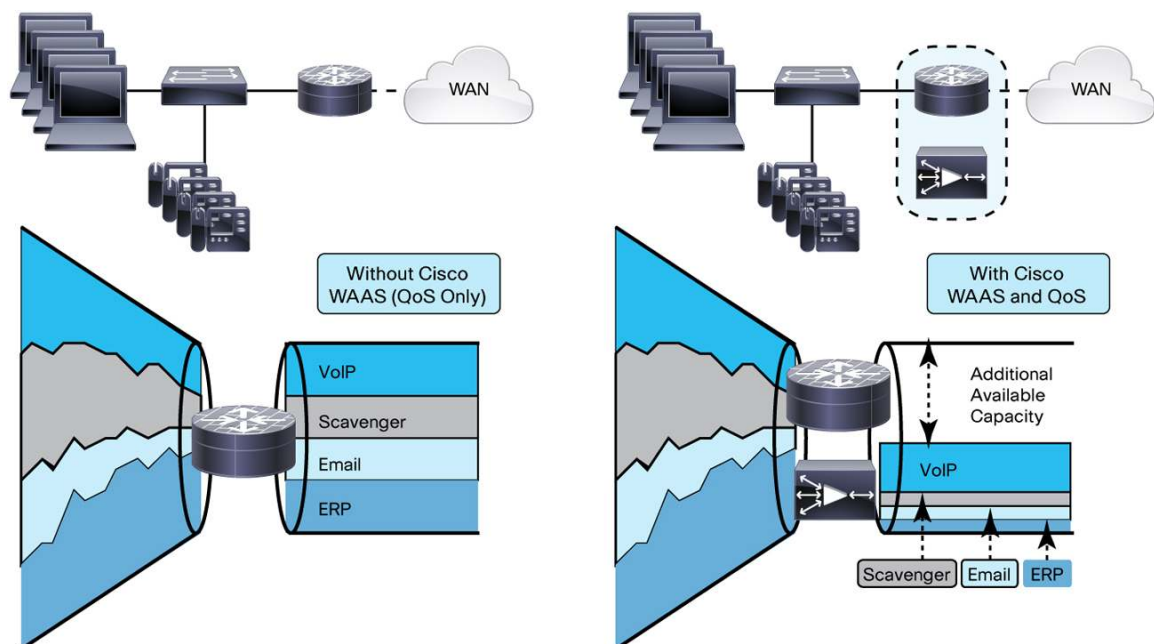
- Dynamic routing: Cisco WAAS interoperates transparently with dynamic routing technologies such as Performance Routing (PfR), Optimized Edge Routing (OER), and Policy-Based Routing (PBR).
- Access control: Cisco WAAS interoperates transparently with access control lists (ACLs) and Cisco firewall policies to block certain types of traffic from traversing network devices.
- NetFlow and performance monitoring tools: Cisco WAAS interoperates transparently with NetFlow and other performance tools to help ensure full visibility into the traffic encountered on the network.

Additionally, Cisco WAAS integrates transparently with application performance monitoring solutions such as Cisco NAM, CA NetQoS SuperAgent, Visual Networks Visual Performance Manager (VPM), InfoVista 5View Service Data Manager (SDM), OPNET AppResponse Xpert, and Compuware Vantage. Other WAN optimization and application acceleration solutions mask the actual performance that clients and servers encounter because of the local acknowledgment of TCP segments. Cisco WAAS also provides such a TCP proxy, but you can configure it to inform both Cisco NAM and NetQoS SuperAgent of otherwise masked connection details to allow you to retain full view of the exact performance that users and servers encounter. Cisco NAM can export the performance information to third-party performance management tools. Additionally, with the introduction of Cisco Performance Agent in Cisco IOS Software Release 15.1(4)M, a Cisco ISR G2 router can report the same application performance and optimization metrics and export the data through flexible NetFlow to Cisco NAM and third-party monitoring systems. As a result, customers gain comprehensive application performance and WAN optimization visibility, independent of the Cisco WAAS form factor.

Cisco WAAS Central Manager includes integrated performance monitoring capabilities that integrate the Cisco NAM reports that are most relevant to Cisco WAAS deployment. This feature simplifies the configuration and monitoring processes, expands reporting capabilities beyond Cisco WAAS visibility to the entire network, and provides end-to-end application performance analytics and optimization statistics.

Security

Cisco WAAS provides the industry's only secure WAN optimization solution in that it allows transparent interoperability with existing security technologies and devices. Whereas other solutions that are either nontransparent or nonintegrated require security posture changes to support optimization, only Cisco WAAS helps ensure full compatibility and preservation of your security posture.

Figure 16 shows the components of Cisco WAAS and secure WAN optimization.

Figure 16. Cisco WAAS and Secure WAN Optimization
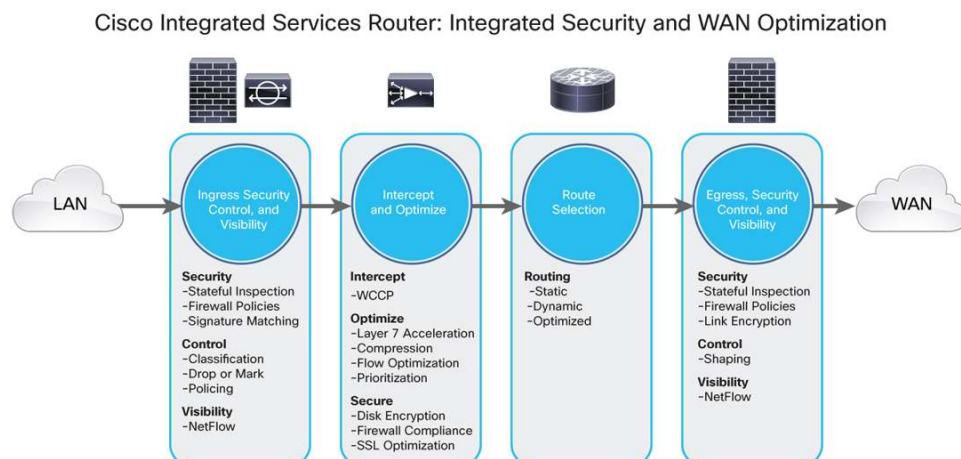
Following are a few capabilities of the Cisco WAAS secure WAN optimization solution:

- Full integration with Cisco firewalls: Cisco firewall devices and software, including Cisco IOS Firewall, the Cisco Catalyst® 6500 Series Firewall Services Module (FWSM), Cisco PIX® Firewall Software, and Cisco ASA 5500 Series Adaptive Security Appliances Enterprise Firewall Edition, are all Cisco WAAS aware and can identify flows that are optimized by Cisco WAAS. This behavior helps ensure that new service ports do not need to be open and that stateful inspection is not compromised.

- Full integration with Cisco Intrusion Detection System (IDS) and Intrusion Prevention System (IPS): Cisco IDS and IPS devices recognize flows optimized by Cisco WAAS and eliminate the false positives that plague competitive WAN optimization and application acceleration solutions deployed in networks with signature- or anomaly-based IDS and IPS.

- Full integration with VPN infrastructure: Cisco WAAS automatically adjusts parameters on optimized connections to help ensure transparent transport through the VPN infrastructure.

- Disk encryption: You can enable disk encryption selectively or globally, with the Cisco WAAS Central Manager managing disk encryption keys, to help ensure that data written to the Cisco WAAS device disks is completely unusable if a system is compromised. This behavior helps ensure compliance with Payment Card Industry (PCI) regulations along with other federal and industry-related compliance initiatives, as shown in Figure 17.

Figure 17.   Cisco WAAS Disk Encryption
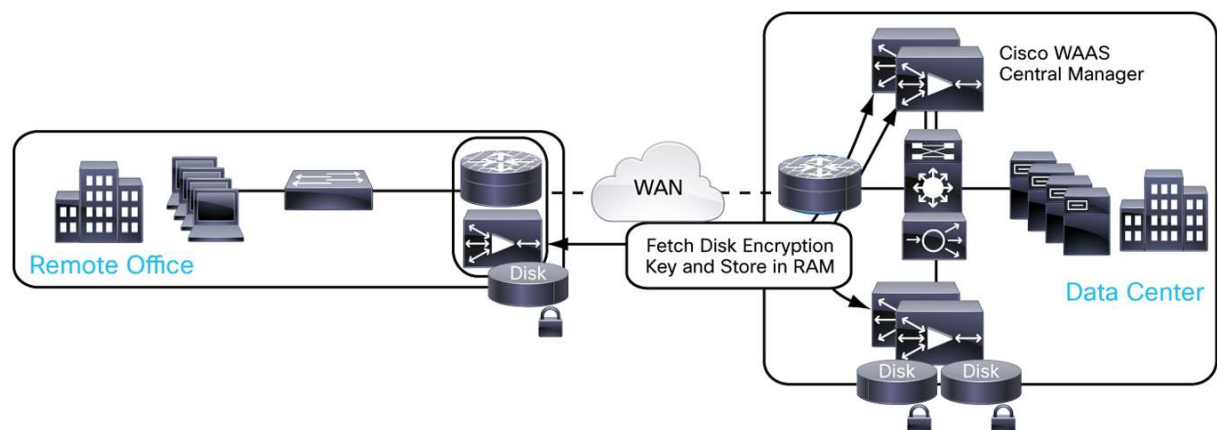
Cisco AppNav WAN Optimization Virtualization

The Cisco AppNav is a comprehensive and network-integrated WAN optimization solution available with virtualization technology that drastically reduces operation complexity in enterprisewide WAN optimization deployments. The Cisco AppNav solution enables customers to virtualize WAN optimization resources in the data center by pooling them into one elastic resource in a manner that is policy based and on demand with the best available scalability and performance. It integrates transparently with Cisco WAAS physical and virtual network infrastructure, providing significant investment protection for existing network design objectives as well as the capability to expand the WAN optimization service to meet future demands. The Cisco AppNav capability to pool elastic resources also lays the foundation for migration to cloud services.

The Cisco AppNav solution provides the following benefits:

- Efficient and cost-effective expansion of WAN optimization services within a company: The Cisco AppNav solution provides an on-demand pool of Cisco WAAS devices (appliances or virtual appliances or a mixture of both) that can be used in all data center deployment models.
- Flexibility in WAN optimization deployment to address various business needs: The Cisco AppNav solution allows flexible policy definitions that dynamically bind business logical constructs to a set of Cisco WAAS pools, and it makes intelligent load-distribution decisions based on the state of the nodes currently providing services.
- Improved business continuity with highly available Cisco WAAS services: The Cisco AppNav clustering mechanism enables redundancy in the pool of Cisco WAAS devices and Cisco AppNav services.
- The Cisco AppNav elastic provisioning and deployment of WAN optimization services along with the upcoming integration of Cisco AppNav technology into the Cisco Cloud Services Router (CSR) provides a transparent, optimized connection from the branch office to the cloud.
- Capability to address challenges posed by today's data center infrastructure: Cisco AppNav native solutions address directional asymmetry in the multipath environment of the data center while preserving the user-intended network path (network path affinity).

Network Interception

Cisco WAAS provides the industry's most flexible and functionally complete set of network interception and redirection techniques. Each technique provides efficient integration and interaction with adjacent network devices to provide stability, scalability, and performance.

- Physical inline deployment: Using the Cisco inline interception card, you can easily deploy Cisco WAAS Appliances by simply inserting the Cisco WAAS Appliance in line between the router (or firewall) and the adjacent switch. With the use of fail-to-wire capabilities, if the Cisco WAAS Appliance experiences a hardware or software failure, within seconds the appliance will transparently become a bridge and remove itself from operation. When deploying them in line, you can deploy Cisco WAAS Appliances in a serial cluster if you want high availability of optimization services. You can deploy serial inline clusters in the data center as well as in the branch office.
- WCCP Version 2 (WCCPv2): Cisco WAAS provides full support for WCCPv2, allowing deployment of up to 32 Cisco WAAS devices in a single device group with load balancing, failover, and nondisruptive Cisco WAAS device insertion and removal. Unlike solutions that implement only a portion of the WCCPv2 specification, Cisco WAAS provides full WCCPv2 compatibility for efficient integration into both the branch office and data center without compromising performance, scalability, or existing infrastructure.
- PBR: You can deploy Cisco WAAS in the network using PBR, which defines the Cisco WAAS device as a next-hop router. PBR allows you to configure multiple Cisco WAAS devices as next-hop routers; you also can use PBR in conjunction with IP service-level agreements (SLAs) for high-availability failover configurations.
- The Cisco ACE Application Control Engine Module or Cisco Content Switching Module (CSM): You can deploy Cisco WAAS Appliances in the data center using the Cisco ACE Module or Cisco CSM for the Cisco Catalyst 6500 Series for tremendous scalability. You can manage up to 4 million connections per Cisco ACE Module, with redirection to a farm of Cisco WAAS Appliances and supporting data rates of up to 16 Gbps. You can deploy up to four Cisco ACE Modules in a Cisco Catalyst 6500 Series chassis, enabling scalability to up to 64 Gbps and 16 million TCP connections.

- Cisco Nexus vPath Interception: The Cisco Nexus 1000V provides virtualization-aware network services to all application server virtual machines. Central to this capability are port profiles, which are a collection of interface configuration commands that you can dynamically apply at either physical or virtual interfaces. Any changes to a given port profile are propagated immediately to all ports that have been associated with it. Port profiles are visible as VMware port groups in the VMware vCenter management console. The Cisco Nexus 1000V provides a mechanism for attaching Cisco vWAAS to the port profiles of servers that need to be optimized. vPath will intercept all traffic to and from these servers and forward it to the Cisco vWAAS virtual machine for optimization. vPath interception uses Cisco Nexus 1000V port-profile attributes (vn-service) to redirect traffic to Cisco vWAAS. Administrators need to identify the port profiles of servers to be optimized by Cisco vWAAS. After the port profile is identified, Cisco vWAAS needs to attach to one or multiple port profiles to optimize the traffic. Cisco WAAS autodiscovery helps ensure that a particular TCP connection will be optimized only by the endpoint devices (Cisco WAE or Cisco vWAAS).

- Integrated router (Cisco ISR G2) forwarding: With Cisco WAAS Express on Cisco ISR G2 routers, the default optimization policy will apply to traffic entering and leaving the interface as soon as the feature is enabled for those specific interfaces. In this case, there is no need to configure inline or WCCP interception mechanisms.

Automatic Discovery

Cisco WAAS automatically discovers all Cisco WAAS devices in the path between a source and destination pair. As each TCP connection is established, Cisco WAAS nonintrusively applies markings to the connection request packets to identify each Cisco WAAS device in the path between the communicating nodes as well as the optimizations being requested based on the configured policy. As marked packets are received by the distant Cisco WAAS device, the topology is learned, and optimization capabilities can then be negotiated.

In addition, Cisco WAAS devices can automatically detect the Cisco WAAS Central Manager through DNS and preform an automatic deployment of Cisco WAAS devices at branch offices without any user intervention or specific configuration. This capability significantly reduces time and OpEx spent at remote sites and enables rapid deployment of WAN optimization systems.

Cisco WAAS automatic discovery provides the following benefits:

- No manual topology definition: No tunnel or overlay network definition is required, because Cisco WAAS devices do not use tunnels, and they automatically determine what devices are in the path, negotiating optimization levels automatically without the need for administrative configuration.

- Automatic bypass of intermediary Cisco WAAS devices: Optimization is applied only between the outermost Cisco WAAS devices to help ensure efficient use of resources and optimal optimization of connections.

Secure, Scalable Centralized Management with Cisco WAAS

Cisco WAAS deployments are managed through the secure, scalable Cisco WAAS Central Manager. You can manage up to 2000 Cisco WAAS devices with a single Cisco WAAS Central Manager, which you can also deploy in a highly available failover configuration. All communications between Cisco WAAS devices and the Cisco WAAS Central Manager are encrypted using SSL to help ensure data privacy.

Figure 18 shows the Cisco WAAS Central Manager dashboard.

Figure 18.   Cisco WAAS Central Manager Dashboard
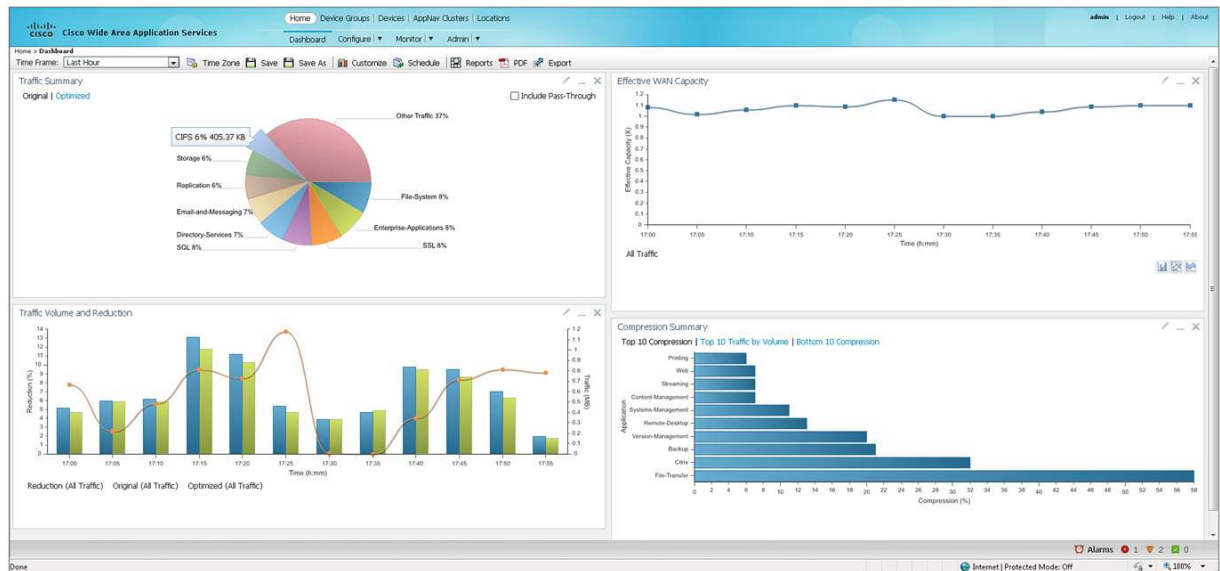
The new Cisco WAAS 5.0 Central Manager with HTML 5 user-friendly interfaces and improved navigation provides deeper visibility into application performance and pass-through traffic and better control and monitoring capabilities. The Cisco WAAS Central Manager offers the following capabilities for managing and monitoring your Cisco WAAS deployment:

- Highly available, secure platform: All communications among Cisco WAAS devices and the Cisco WAAS Central Manager are encrypted, and you can deploy the central manager itself in a high-availability configuration with automatic failover.

- Scalability: You can deploy multiple Cisco WAAS Central Managers to scale to any number of deployed Cisco WAAS devices.

- Configuration simplicity through device groups: Multiple Cisco WAAS devices can belong to a single device group, and you can apply configuration changes to the device group and then automatically apply them to the group's members. The use of device groups reduces the number of clicks necessary to make broad-reaching changes to the Cisco WAAS deployment.

- Customizable, schedulable reports: You can view powerful reporting statistics covering device and system health, WAN optimization performance, application acceleration performance, and traffic by device, by device group, and systemwide. You can schedule all reports for automatic delivery using email, and real-time connection statistics are available. Additionally, a monitoring API that uses XML is available to enable integration into existing monitoring and reporting architectures. Figure 19 shows some of the many powerful reports that the Cisco WAAS Central Manager provides.

Figure 19. Sample HTTP Acceleration and Optimization Reports Provided by Cisco WAAS Central Manager


- Centralized policy management: You can centrally manage the optimization and acceleration capabilities of Cisco WAAS devices through the Application Traffic Policy (ATP) Manager on the Cisco WAAS Central Manager, providing an intuitive policy builder you can use to define the applications to be optimized and the levels of optimization to be applied. More than 150 policies are configured by default, supporting today's most commonly used applications and protocols.

- Full role-based access control (RBAC): The Cisco WAAS Central Manager provides full RBAC capabilities to define the users who can interact with the management and monitoring components on specific devices and whether read or write permissions are allowed. Additionally, you can integrate identity with Microsoft Active Directory, TACACS, or RADIUS to allow a centralized provider to manage authentication based on user or group definition.

- Encryption services: 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 the keys necessary for Cisco WAAS device disk encryption. All sensitive data used or generated by a Cisco WAAS deployment is stored and transmitted securely.

- Integrated application performance monitoring (APM): The Cisco WAAS Central Manager includes integrated performance monitoring capabilities that integrate the Cisco NAM reports that are most relevant to Cisco WAAS deployment. This feature simplifies the configuration and monitoring processes, expands reporting capabilities beyond Cisco WAAS visibility to the entire network, and provides end-to-end application performance analytics and optimization statistics. Figure 20 shows some of the ways in which the Cisco WAAS Central Manager provides application performance visibility.

Figure 20.   Cisco WAAS Central Manager Network and Application Performance Analyses

- Integrated Cisco AppNav configuration and monitoring: The Cisco WAAS Central manager includes an integrated Cisco AppNav configuration and monitoring capability. This feature provides a comprehensive, cohesive, and simple interface for configuring, monitoring, and troubleshooting the entire Cisco AppNav cluster. Figure 21 provides examples of the wizard-guided configuration and comprehensive cluster and device views that the Cisco WAAS Central Manager AppNav interface provides.

Figure 21.   Cisco WAAS Central Manager AppNav Cluster Configuration Wizard and Health Statistics Through 360° Network View
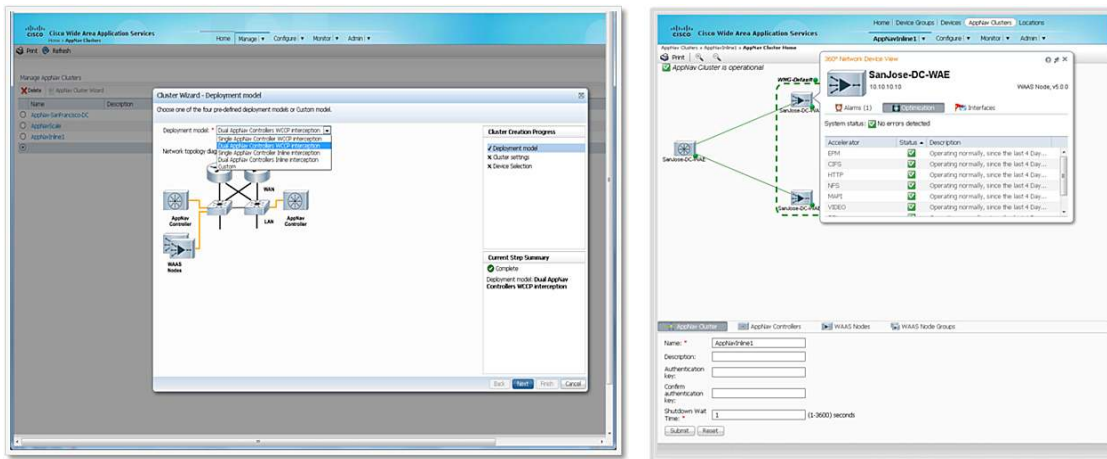
Conclusion

IT departments face significant pressure to do more with less: achieve greater application and data availability and higher levels of performance and throughput, with fewer people and devices and in less time. Application delivery technologies help IT departments consolidate application infrastructure from distributed sites in the data center while providing the optimizations necessary to improve application and data-access performance over the WAN. Along with providing the capabilities necessary to consolidate infrastructure in the data center, Cisco WAAS provides the capabilities necessary to consolidate infrastructure within the branch office itself for applications that are deemed necessary. By providing the industry's most complete set of WAN optimization capabilities, application acceleration services, and virtualization capabilities, Cisco WAAS helps IT departments meet the challenges of consolidating costly infrastructure and improving application performance to enable distributed business initiatives.

For More Information

For more information, please visit http://www.cisco.com/go/waas.

Printed in USA

C11-723231-00   01/13