Cisco Solutions for a VMware View 4.0 Environment Design Guide

Last Updated: February 15, 2010

Cisco Validated Design

Building Architectures to Solve Business Problems

About the Author

Shannon McFarland

Shannon McFarland, Solutions Architect, CMO ESE, Cisco Systems

Shannon is a solutions architect for data center technologies and enterprise IPv6 design on Cisco's Enterprise Solutions Engineering team. He is currently focused on data center design validation and optimization with an application/OS focus on Microsoft, VMware and VDI. He has been responsible for his team's enterprise IPv6 design and deployment effort for more than five years. Shannon has authored many technical papers, been a contributor to Cisco Press books, and is a frequent speaker at Cisco Networkers and other industry conferences. Previously he was a Cisco field systems engineer, supporting enterprise customers and partners. Shannon has been in the networking and application industry for more than 16 years. He holds CCIE certification 5245.

CONTENTS

Cisco Solutions for a VMware View 4.0 Environment

Introduction

VMware View 4.0 is a virtual desktop infrastructure (VDI) offering that is used by businesses, educational institutions, government bodies, and many other vertical industries. VMware View 4.0 provides many of the core components that are needed to deploy a scalable, available, and secure VDI implementation. Cisco offers a wide variety of value-add solutions that make VMware View 4.0 more scalable, available, and secure as well as greatly optimize the end-user VDI experience.

Audience

This document is intended for network engineers and architects who support VMware View 4.0 environments and need to understand the design and configuration options for deploying VMware View 4.0 on a Cisco network.

Document Objectives

This document provides design and configuration guidance for deploying and optimizing VMware View 4.0 in a Cisco data center, campus, branch, and for Internet-based users. This document describes VMware View components and various Cisco products and technologies, and explains how combining them increases the availability and performance of the VMware View environment.

An overview of the various VMware View components is provided for the reader who may be focused on the network but needs a basic understanding of the VMware View environment.

The following are prerequisites for deploying the Cisco solution for VMware View:

- Experience with basic networking and troubleshooting
- Working knowledge of the Cisco Internetworking Operating System (IOS) and Nexus OS (NX-OS)
- Working knowledge of the Cisco Nexus 1000V Series switch
- Working knowledge of the Cisco Application Control Engine (ACE)

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- Working knowledge of the Cisco Adaptive Security Appliance (ASA)
- Working knowledge of the Cisco Wide Area Application Services (WAAS) suite of products, including WAAS Mobile
- Experience with Cisco quality-of-service (QoS) fundamentals (classification/marking, queuing, policing, and so on)
- Familiarity with VMware Virtual vSphere 4.0 components (ESX, Virtual Center, and so on)

For additional information that might be useful in understanding and deploying this solution, as well as other applications, see the documents listed in the "Related Documents" section on page 77.

Solution Overview

The Cisco solution for VMware View offers increased application availability, performance, and improved end-user experience by leveraging the following technologies and services:

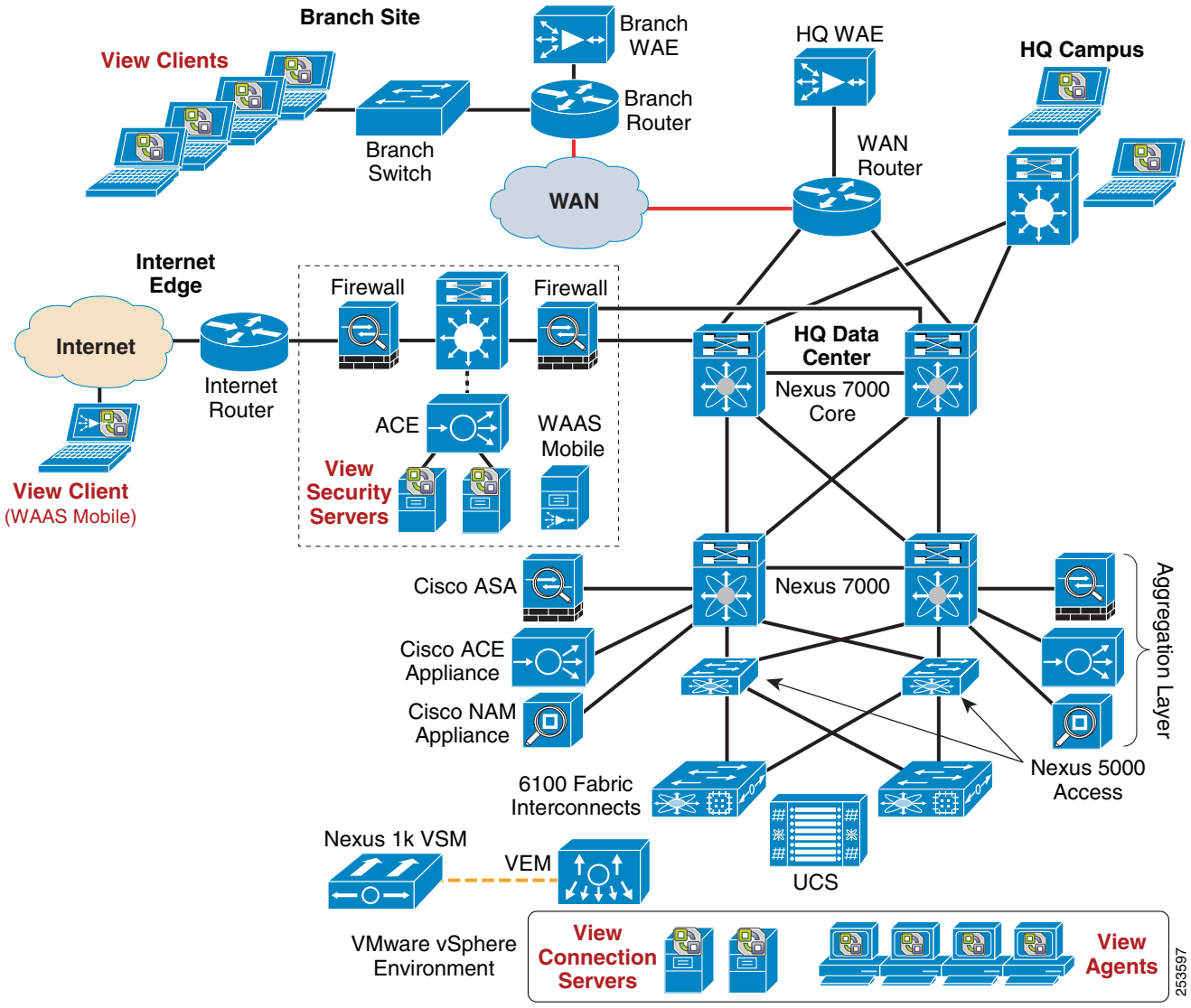
- Cisco ACE—The ACE provides server load balancing, server/application health monitoring, and Secure Socket Layer (SSL) offload for the VMware View Connection Server and Security Server roles (if deployed).
- Cisco WAAS and WAAS Mobile—WAAS offers an improved end-user experience by optimizing the transport protocol used by remote display protocols such as Microsoft Remote Desktop Protocol (RDP), and local data caching and compression of duplicate data sent between the VMware View Client and the VMware View Connection Server, Security Server (if deployed), and/or the View Agent.
- Cisco ASA—The ASA offers perimeter protection for the VMware View Connection Server and Security Server roles by providing firewall services for traffic destined for the View Connection Server and Security Server (if deployed) roles.
- Cisco Nexus 1000V—The Nexus 1000V offers policy-based virtual machine (VM) connectivity as well as mobile VM security by providing VMware View components with consistent network connectivity and policy enforcement between ESX hosts.
- Cisco QoS:
  - Classification and marking—Identifies and classifies/marks VMware View remote display protocol traffic so that it is treated differently than other types of traffic.
  - Policing—Ensures policy conformance to administratively-defined traffic rates for VMware View remote display protocol traffic and takes action such as marking/remarking or dropping packets if these rates are exceeded.
  - Scheduling/queuing—Selectively drops packets as the queues are filling to avoid traffic congestion.
  - Link-specific tools—Shaping, link fragmentation and interleaving, compression and transmit rings offer non-application-specific capabilities to smooth and reduce traffic over slow-speed WAN links.

Solution Components and Topology

VMware View 4.0 can be deployed in a variety of ways that range from a highly consolidated approach focused on small- and medium-sized implementations to highly complex, redundant, and scalable implementations used by large enterprise accounts. A large number of variables and implementation options are available with a VMware View implementation; therefore, it is important to break down the various VMware View roles to their basic elements. This document provides a brief overview of three of the main VMware View roles (View Agent, View Client, and View Connection Server) that were used in the validation of the Cisco solution.

Figure 1 illustrates the high-level view of the design presented in this document. Although not shown in this high-level diagram, the Cisco environment is deployed with redundant devices for each role and layer of the network.

Figure 1 Cisco Solution for VMware View 4.0—High Level Overview



The sections that follow briefly describe the components in each area of the diagram in Figure 1.

WAN/Branch

In the WAN/branch area of Figure 1, several 1 Gb Ethernet attached client computers are running Microsoft Windows XP SP3 with the VMware View Client 4.0 service installed. These client computers are connected to the network via a Cisco Catalyst 3750 Series Switch. The branch switch is connected to a Cisco ISR 3845 Router that has a T1 connection to the WAN. The branch router is connected to a Cisco WAE appliance for WAN optimization. Terminating the branch router connections is another Cisco ISR router that acts as the headend WAN router.

The WAN/branch is connected to the data center through the Cisco Nexus 7000 Series Switch.

Internet Edge

The Internet edge provides access, security, server load balancing (SLB), and SSL offload for the View Security Servers as well as housing the WAAS Mobile server that is used by View Clients located on the Internet. The Internet edge connects to the Internet through redundant Cisco ASR 1004 routers. Behind the ASRs are ASA 5540s that provide firewall services for the View Security Servers and WAAS Mobile Servers. The Cisco ACE 4710 Appliance provides Layers 4 to 7 SLB and Secure Socket Layer (SSL) offload services for the View Security Servers.

Campus

In the campus area of the diagram in Figure 1, several 1 Gb Ethernet attached client computers run Microsoft Windows XP SP3 with the VMware View Client 4.0 service installed. These client computers are connected to the network through an access layer Cisco Catalyst 6500 switch. The Catalyst 6500 is connected to the distribution layer Cisco Catalyst 6500 with Supervisor 720 via 10 Gb Ethernet. The distribution layer Catalyst 6500 is connected to the data center via the core layer Nexus 7000 Series Switch.

Data Center

The data center connectivity is as follows:

- The core layer Nexus 7000 is connected to the Nexus 7000 aggregation layer via 10 Gb Ethernet links.
- The Nexus 7000 aggregation layer is connected to the Nexus 5000 access layer via 10 Gb Ethernet links.
- The Nexus 5000 has direct connections to the Cisco Unified Computing System (UCS) 6100 Fabric Interconnects through 10 Gb links.
- For non-View servers (not shown) that have only 1 Gb Ethernet NICs (physical servers or VMs located on platforms other than Cisco UCS), the Nexus 2000 Fabric Extender connects the server to the Nexus 5000 access layer switch. Additionally, the Cisco UCS is connected to the Cisco MDS 9000 SAN Director for SAN access to the storage array (not shown).
- The Nexus 1000V Virtual Ethernet Module (VEM), which is managed by the Virtual Supervisor Module (VSM), provides network connectivity for the various View components that are running as VMs.
- The VMware ESX hosts have multiple virtual machines running to include the View Connection Server role, Windows XP SP3 View Agents, and Microsoft Active Directory/DNS/DHCP servers.
- The Cisco ASA, Cisco ACE, and Cisco NAM appliances are also located in the data center and connected to the Nexus 7000 in the aggregation layer.

Solution Components—Software Versions

Table 1 lists software components and software versions.

Table 1 Software Components—Software Versions

Device	Version
Cisco ISR 3845	12.4.24T2
Cisco Catalyst 3750	12.2.53-SE
Cisco WAE-512	4.1.3a.32
Cisco WAE-512	4.1.3a.32
Cisco Nexus 7000	4.1(4)
Cisco Nexus 5000	4.1(3)N2(1a)
Cisco Nexus 1000	4.0(4)SV1(2)
Cisco Catalyst 6500 Supervisor 720	12.2.33-SXI3
Cisco WAAS Mobile	3.4.2.1676
Cisco ACE 4710	A3(2.4)
Cisco NAM 2220	4.0(1)
Cisco ASA 5540	8.0(5)
VMware ESX	4.0.0, 208167 (U1)
VMware vCenter/vSphere Client	4.0.0, 208111 (U1)
VMware View	4.0.0, 210939
Microsoft Windows XP	Professional– SP3
Microsoft Windows Server 2003 R2	Enterprise—SP2

Cisco Solution Overview for VMware View 4.0

This section presents a brief introduction to the active Cisco solution components used to optimize the VMware View 4.0 environment.

Cisco Application Control Engine

The Cisco Application Control Engine (Cisco ACE) provides a highly available and scalable data center solution from which the VMware View environment can benefit. The Cisco ACE is available as an appliance or integrated services module in the Cisco Catalyst 6500 platform. The Cisco ACE features and benefits include the following:

- Device partitioning (up to 250 virtual Cisco ACE contexts)
- Load-balancing services (up to 16 Gbps of throughput capacity and 325,000 Layer-4 connections per second)
- Security services through deep-packet inspection, access control lists (ACL), unicast reverse path forwarding (uRPF), Network Address Translation (NAT)/Port Address Translation (PAT) with fix-ups, syslog, and so on

- Centralized, role-based management through Application Network Manager (ANM) GUI or CLI
- SSL offload (up to 15,000 SSL sessions per second through licensing)
- Support for redundant configurations (intra-chassis, inter-chassis, and inter-context)

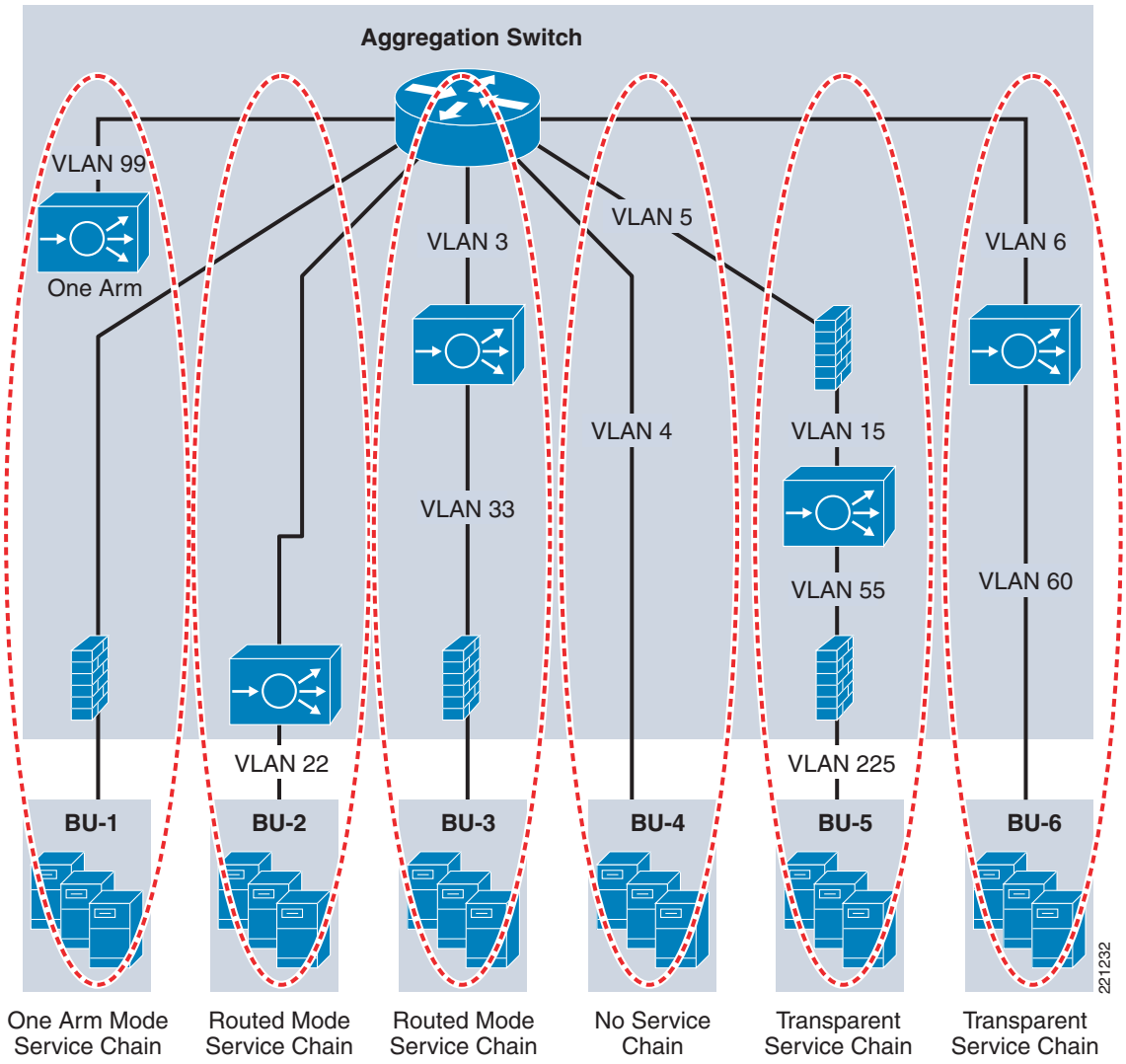
Cisco ACE Virtualization

Virtualization is a prevalent trend in the enterprise today. From virtual application containers to virtual machines, the ability to optimize the use of physical resources and provide logical isolation is gaining momentum. The advancement of virtualization technologies includes the enterprise network and the intelligent services it offers.

The Cisco ACE supports device partitioning where a single physical device might provide multiple logical devices. This virtualization functionality allows system administrators to assign a single virtual Cisco ACE device to a business unit or application to achieve application performance goals or service-level agreements (SLAs). The flexibility of virtualization allows the system administrator to deploy network-based services according to the individual business requirements of the customer and technical requirements of the application. Service isolation is achieved without purchasing another dedicated appliance that consumes more space and power in the data center.

Figure 2 shows the use of virtualized network services afforded through the Cisco ACE and Cisco Firewall Services Module (FWSM).

Figure 2 Service Chaining via Virtualized Network Services



In Figure 2, a Cisco Catalyst 6500 housing a single Cisco ACE and Cisco FWSM supports the business processes of five independent business units. The system administrator determines the application requirements and assigns the appropriate network services as virtual contexts. Each context contains its own set of policies, interfaces, resources, and administrators. The Cisco ACE and Cisco FWSMs allow routed, one-arm, and transparent contexts to coexist on a single physical platform. Alternatively, the Cisco ACE appliance and Cisco ASA can be used to achieve a similar level of virtualization to their module counterparts.

The Cisco ACE can be used to apply a different context and associated policies, interfaces, and resources for one View role and a completely different context for another View role. Each context can be assigned a different administrator, allowing for role-based access control (RBAC) of the services.

SSL Offload

The Cisco ACE is capable of providing secure transport services to a VMware View deployment. The Cisco ACE can offload Transport Layer Security (TLS)/SSL processing from the View Connection Server and View Security Server roles, thereby saving processor cycles. The Cisco ACE implements its own SSL stack and does not rely on any version of Open SSL. The Cisco ACE supports TLS 1.0, SSLv3, and SSLv2/3 hybrid protocols. The following are three SSL-relevant deployment models available to each Cisco ACE virtual context:

- *SSL termination*—Allows for the secure transport of data between the client and Cisco ACE virtual context. The Cisco ACE operates as an SSL proxy. As such, it negotiates and terminates secure connections with a client, and a non-secure or clear-text connection to an application server in the data center. The advantage of this design is the offloading of application server resource requirements from the CPU and memory demands associated with SSL processing, while continuing to provide intelligent load balancing.
- *SSL initiation*—Provides secure transport between the Cisco ACE and the application server. The client initiates a non-secure HTTP connection with the Cisco ACE virtual context, while the Cisco ACE acts as a client proxy that negotiates an SSL session to an SSL server.
- *SSL end-to-end*—Provides a secure transport path for all communications between a client and the SSL application server residing in the data center. The Cisco ACE uses SSL termination and SSL initiation techniques to support the encryption of data between client and server. Two completely separate SSL sessions are negotiated, one between the Cisco ACE context and the client, the other between the Cisco ACE context and the application server. In addition, the Cisco ACE provides intelligent load balancing services in an end-to-end SSL model. The system administrator may choose to modify the level of data encryption to reduce the load on either the frontend client connection or backend application server connection (allowing for the reduction of SSL resource requirements on either entity).

SSL URL Rewrite

The Cisco ACE is capable of inserting or deleting HTTP header information for connections it is sustaining. This capability is highly useful when an application server responds with an HTTP 302 or Moved Temporarily response to a client HTTP GET or HEAD request. The HTTP 302 response usually indicates a new HTTP LOCATION URL for the client to access. Modifying the HTTP LOCATION value for a secure connection is known as *SSL URL Rewrite*. The SSL URL Rewrite feature allows the system administrator to alter the HTTP LOCATION value returned to the client, resulting in granular control of the application's session flow and persistence in the data center.

Session Persistence

Session persistence is the ability to forward client requests to the same server for the duration of a session. One common approach to maintaining session persistence with VMware View is to use Source IP sticky. While Source IP sticky is not ideal, especially for Internet-based clients, it is generally all that can be used with VMware View 3.0 and 4.0. More information regarding VMware View and session persistence is provided later in this document.

In addition, the Cisco ACE supports the replication of sticky information between physical devices and their respective virtual contexts. This provides a highly available solution that maintains the integrity of each client's session.

Allowed Server Connections

Enterprise data centers should perform due diligence on all deployed server and network devices, determining the performance capabilities to create a more deterministic, robust, and scalable application environment. The Cisco ACE allows the system administrator to establish the maximum number of active connections value on a per-server basis and/or globally to the server farm. This functionality protects the end device, whether it is an application server or network application optimization device such as the Cisco WAE.

Route Health Injection

Route Health Injection (RHI) allows the Cisco ACE to advertise host routes associated with any number of virtual IP addresses hosted by the device. The injection of the host route to the remaining network offers Layer-3 availability and convergence capabilities to the application environment.

Health Monitoring

The Cisco ACE device is capable of tracking the state of a server and determining its eligibility for processing connections in the server farm. The Cisco ACE uses a simple pass/fail verdict, but has many recovery and failure configurations, including probe intervals, timeouts, and expected results. Each of these features contributes to an intelligent load-balancing decision by the Cisco ACE context.

The following are the predefined probe types currently available on the Cisco ACE module:

- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Echo (TCP/UDP)
- Finger
- Hypertext Transfer Protocol (HTTP)
- Secure HTTP (HTTPS) SSL Probes
- File Transfer Protocol (FTP)
- Telnet
- Domain Name System (DNS)
- Simple Mail Transfer Protocol (SMTP)
- Internet Message Access Protocol (IMAP)
- Session Initiation Protocol (SIP)
- Post Office Protocol version 3 (POP3)
- Remote Authentication Dial In User Service (RADIUS)
- Real Time Streaming Protocol (RTSP)
- Simple Network Management Protocol (SNMP)
- Scripted–Cisco Tool Command Language (TCL) support

Note The potential probe possibilities available via scripting make the Cisco ACE an even more flexible and powerful application-aware device. In terms of scalability, the Cisco ACE module can support 2500 open probe sockets simultaneously.

For more information on these services, see the Cisco ACE documentation listed in the "Related Documents" section on page 77.

Cisco Wide Area Application Services

To appreciate how the Cisco WAAS provides WAN and application optimization benefits to the enterprise, consider the basic types of centralized application messages that are transmitted between remote branches. For simplicity, three basic types are identified:

- *Bulk transfer applications*—Transfer of files and objects using application protocols such as FTP, HTTP, and IMAP. In these applications, the number of round-trip messages might be few and might have large payloads with each packet. Examples include web-portal or thin-client versions of Oracle, SAP, Microsoft (SharePoint, OWA) applications, E-mail applications (Microsoft Exchange, Lotus Notes), and other popular business applications.
- *Transactional applications*—High numbers of messages transmitted between endpoints. Chatty applications such as SMB/CIFS and MAPI, with many round-trips of application protocol messages that might or might not have small payloads.
- *Multi-media Streaming applications*—Integrated forms of one or several media messages and content (text, graphics, video, animation and audio) which are streamed or transported using streaming channels to the client over the network.

The Cisco WAAS uses the technologies described in the following subsections to provide a number of benefits, including application acceleration such as HTTP(s) acceleration, file caching, print service, and bandwidth optimization.

Advanced Compression Using DRE and LZ Compression

Data Redundancy Elimination (DRE) is an advanced form of network compression that allows the Cisco WAAS to maintain an application-independent history of previously-seen data from TCP byte streams. Lempel-Ziv (LZ) compression uses a standard compression algorithm for lossless storage. The combination of using DRE and LZ eliminates the number of redundant packets that traverse the WAN, thereby conserving WAN bandwidth, improving application transaction performance, and significantly reducing the time for repeated bulk transfers of the same application. In a VMware View implementation using Microsoft RDP, it is important to disable RDP compression and encryption in order to apply DRE and LZ compression. Also, DRE and LZ compression can be used for USB redirection flows, print services (see below), and even PCoIP control and heartbeat flows that are TCP-based (note that PCoIP data flows are UDP).

Transport File Optimizations

Cisco WAAS Transport File Optimizations (TFO) uses a robust TCP proxy to safely optimize TCP at the Cisco WAE device by applying TCP-compliant optimizations to shield the clients and servers from poor TCP behavior because of WAN conditions. Cisco WAAS TFO improves throughput and reliability for clients and servers in WAN environments through techniques like an increase in the TCP window sizing and scaling enhancements, as well as through the implementation of congestion management and recovery techniques, to ensure that the maximum throughput is sustained in the event of packet loss. By default, Cisco WAAS provides only TFO for RDP. If RDP compression and encryption are disabled, full optimization (TFO + DRE/LZ) can be enabled for RDP flows.

Common Internet File System Caching Services

The Common Internet File System (CIFS) used by Microsoft applications is an inherently chatty transactional application protocol; it is not uncommon to find several hundred transactional messages traversing the WAN just to open a remote file. The Cisco WAAS provides a CIFS application accelerator that can inspect and predict to a certain degree which follow-up messages are expected. By doing this, the local Cisco WAE caches these messages and sends them locally, significantly reducing the number of CIFS messages traversing the WAN.

Print Services

Cisco WAAS provides a fully transparent feature called Print Application Optimizer (PAO) to accelerate Microsoft Windows printing. Windows printing uses CIFS/RPC over SMB between client and print server. PAO understands the way Windows printing works at the CIFS/RPC protocol level and is able to optimize the Windows print traffic by removing chattiness of the Microsoft RPC protocol. Moreover, WAAS provides native SMB-based Microsoft print services to be hosted locally as a virtualized Windows service component on the WAAS device.

WAAS PAO provides benefits when the Windows Print server running on Windows 2000 or 2003 Server is centrally located in data center, and employees are using Windows Vista, XP, or Windows 2000 client PCs at a remote office. In this case, when printing documents on printers located at the remote office, the PAO improves both performance and the user experience as it reduces the number of round trip messages needed to go over the WAN between the Print server and the local printer.

Similarly, the new Cisco WAVE appliances, with virtualization capability, allows the Windows Print services to run on the virtual blade as a service of the Windows Server on WAAS solution. Thus, even if WAN connectivity fails at the remote location, employees in the remote office can print on the local printer after being authenticated by the Active Directory running on the same virtual blade.

In a VMware View implementation, the Cisco WAAS can offer optimization of the traffic for printer redirection to locally attached printers (such as USB-connected printers) at the branch client device.

SSL

Secure Sockets 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. Cisco WAAS provides SSL optimization capabilities that integrate seamlessly with existing data center key management and trust models and can be used by both WAN optimization as well as 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 end users and servers and requires no changes to the network environment.

By including powerful SSL encryption to the broad set of WAN optimization technologies, Cisco WAAS can provide a core component to ensure the secure delivery of existing SSL-protected VMware View implementation.

Note For more information on these enhanced services, see the *Cisco Wide Area Application Services (Cisco WAAS) v4.1 Technical Overview* at the following URL: http://www.cisco.com/en/US/products/ps6870/products_white_paper0900aecd8051d5b2.shtml.

Cisco WAAS Mobile

In addition to Cisco WAAS for branch optimization, Cisco offers Cisco WAAS Mobile for telecommuters, mobile users, small branch and home office users who access corporate networks and need accelerated application performance. Cisco WAAS Mobile is purpose-built for the Microsoft Windows operating system.

Advanced Data Transfer Compression

Cisco WAAS Mobile maintains a persistent and bidirectional history of data on both the mobile PC and the Cisco WAAS Mobile server. This history can be used in current and future transfers, across different VPN sessions, or after a reboot, to minimize bandwidth consumption and to improve application performance. In addition, instead of using a single algorithm for all file types, Cisco WAAS Mobile uses a file format-specific compression to provide higher density compression than generic compression for Microsoft Word, Excel, and PowerPoint files; Adobe Shockwave Flash (SWF) files; ZIP files; and JPEG, GIF, and PNG files.

Application-Specific Acceleration

Cisco WAAS Mobile reduces application-specific latency for a broad range of applications, including Microsoft Outlook Messing API (MAPI), Windows file servers or network attached storage using CIFS, web applications using HTTP/S and other TCP-based applications, such as RDP.

Transport Optimization

Cisco WAAS Mobile extends Cisco WAAS technologies to handle the timing variations found in packet switched wireless networks, the significant bandwidth latency problems of broadband satellite links, and noisy Wi-Fi and digital subscriber line (DSL) connections. The result is significantly higher link resiliency.

Note For more information on Cisco WAAS Mobile, see the Cisco Wide Area Application Services (Cisco WAAS) Mobile Configuration Guides at the following URL: http://www.cisco.com/en/US/products/ps9523/products_installation_and_configuration_guides_list.html.

Cisco ASA

The Cisco ASA 5500 Series includes the Cisco ASA 5505, 5510, 5520, 5540, 5550, and 5580—purpose-built, high-performance security solutions that take advantage of Cisco expertise in developing industry-leading, award-winning security and VPN solutions. The Cisco ASA 5500 Series builds on proven technologies from Cisco PIX 500 Series Security Appliances, Cisco IPS 4200 Series Sensors, and Cisco VPN 3000 Series Concentrators. Designed as a key component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting SMB, enterprise, and service provider networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.

Through its unique Modular Policy Framework (MPF), the Cisco ASA 5500 Series brings a new level of security and policy control to applications and networks. MPF allows businesses to adapt and extend the profile of the Cisco ASA 5500 Series through highly customizable, flow-specific security policies tailored to application requirements while providing performance and extensibility through user-installable Security Services Modules (SSMs). This adaptable architecture enables businesses to rapidly deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and content security such as those delivered by the Adaptive Inspection and Prevention (AIP) and Content Security and Control (CSC) SSM. Furthermore, the modular hardware architecture of the Cisco ASA 5500 Series along with flexible MPF enables the integration of future network and security, extending the outstanding investment protection provided by the Cisco ASA 5500 Series, and allowing businesses to adapt their network defenses to new threats as they arise.

For the purpose of validating this solution, the ASA 5540 was used. The Cisco ASA 5540 Adaptive Security Appliance delivers high-performance, high-density security services with active/active high availability and Gigabit Ethernet connectivity for medium-sized and large enterprise and service provider networks, in a reliable, modular appliance. With four Gigabit Ethernet interfaces and support for up to 100 VLANs, businesses can use the Cisco ASA 5540 to segment their network into numerous zones for improved security. The Cisco ASA 5540 Adaptive Security Appliance scales with businesses as their network security requirements grow, delivering exceptional investment protection and services scalability. The advanced network and application-layer security services and content security defenses provided by the Cisco ASA 5540 Adaptive Security Appliance can be extended by deploying the AIP SSM for high-performance intrusion prevention and worm mitigation.

Note For more information on Cisco ASA, see the Cisco ASA 5500 Series documentation at the following URL: http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html.

Cisco Network Analysis Module

The Cisco Catalyst 6500, Cisco 7600 Series Network Analysis Module (NAM), and the Cisco NAM 2200 appliance and branch router series provide performance monitoring, traffic analysis, and advanced troubleshooting capabilities. Cisco NAM offers real-time visibility into applications such as VMware View. The Cisco NAM can monitor, analyze, and report on traffic through Switched Port Analyzer (SPAN) ports, NetFlow, and Cisco WAAS appliances.

Intelligent Application Performance Analytics

The Cisco NAM provides intelligent application performance (IAP) measurements to accurately characterize end-user experience. It analyzes the TCP-based client/server message to provide transaction and session-based statistics. Intelligence derived from integrated application and network visibility helps to isolate application problems to the network, application, or server. The NAM also helps to quickly analyze the root cause and resolve problems to minimize any impact to end users.

Visibility into WAN-Optimized Networks

Cisco NAM 4.0 uses the built-in instrumentation on the Cisco WAE as additional data sources to gather flow data for optimized traffic and provide end-to-end application performance visibility in a Cisco WAAS environment. The NAM 4.0 measures and reports on application response time, transaction time, bandwidth usage and LAN/WAN data throughput, and other metrics. As a result, it can accurately quantify the impact of Cisco WAAS optimization.

Network and Application Usage Analysis

One of the foundational elements of the Cisco NAM is its ability to look inside the live packet to gather information on applications, hosts, and conversations. Application monitoring identifies every application that has consumed bandwidth, reports how much bandwidth has been consumed, and detects which hosts are using which applications. Host-and-conversation pair monitoring provides bandwidth consumption per host and shows which hosts are talking to each other along with the amount of traffic each host is generating. Monitoring applications, hosts, and conversations can help to proactively spot bottlenecks before the network suffers impact to performance and availability. It can also help improve the consistency and quality of both individual and overall network services because these metrics reveal usage patterns for users and for router and switch, interface, server, and application resources. Besides delivering a real-time snapshot of bandwidth usage and consumption, Cisco NAM also delivers a continuous historical view of how the bandwidth was used so the network administrator can quickly decide when and where to make changes in network resources.

Advanced Troubleshooting for Cisco NAM

On detecting degradation in performance, Cisco NAM can automatically trigger a packet capture to help investigate and analyze the root cause. Captures can be performed using a web browser from any desktop and packet decodes can be viewed through the web-based traffic analyzer GUI.

Note For more information on the Cisco NAM family of products, see the following URL: http://www.cisco.com/go/nam.

Cisco Nexus 1000V

The Cisco Nexus 1000V switches are virtual machine access switches that are an intelligent software switch implementation for VMware vSphere environments running the Cisco NX-OS Software operating system. Together with the VMware ESX hypervisor, the Cisco Nexus 1000V supports Cisco VN-Link server virtualization technology, which provides the following:

- Policy-based virtual machine connectivity for VMware View components such as the View Agents, Connection Servers, and Security Servers as well as other non-View related components such as Microsoft Active Directory, DHCP, DNS, and so on.
- Mobile virtual machine security and network policy for VMware View components to include DHCP-Snooping, Dynamic ARP Inspection, IP Source Guard, access control, and many other policy-based features.
- Non-disruptive operation model for server virtualization and networking teams by leveraging VMware High Availability (HA), VMware Distributed Resource Scheduler (DRS), and redundant Cisco Nexus 1000V Virtual Supervisor Modules (VSM).

The Cisco Nexus 1000V switches allow for a single Virtual Ethernet Module (VEM) to span multiple physical VMware ESX hosts. The Cisco Nexus 1000V essentially replaces the default vSwitch that runs on each VMware ESX host and provides a single VEM that allows for mobile security and network polices to span multiple VMware ESX hosts without having to reproduce those policies per host. This is a critical addition to the overall Cisco solution for VMware View 4.0 because it allows for multiple View Agent VMs to move across multiple physical VMware ESX hosts without reproducing VM- or port-specific policies between ESX hosts, thus reducing the chances of security and/or network access issues.

Note For more information on the Cisco Nexus 1000V, see the following URL: http://www.cisco.com/en/US/products/ps9902/index.html.

VMware View 4.0 Solution Overview

The VMware View solution offers many advantages to customers, including remote access to applications and virtual desktops, integrated application delivery, simplified printing, and more. The following new or updated features of VMware View 4.0, along with a well-designed Cisco solution, help to achieve the best possible customer experience while also providing availability, security, and ease of deployment and management:

- VMware View 4.0 runs on vSphere 4.0—vSphere serves as the platform for VMware View 4.0, which allows for the world-class benefits of vSphere to be extended to the VMware View environment. Some advantages of View 4.0 on vSphere are:
  - Dynamic Resource Scheduling (DRS) and High Availability (HA)—Automatic movement of VMware View 4.0 Agents and Connection Servers between clustered ESX hosts for optimal use of the computing resources as well as automated failover of VMs between ESX hosts in the event a host is down.
  - Affinity—The ability to group VMs to specific resources for the sake of isolation, security, and management.
  - Resource reservations—The ability to provide resource prioritization for pools of VMware View Agents, giving some pools access to additional resources such as memory on-demand.
  - Consolidated backup—Centralized backup for VMware View components.

- VMware View Composer—Based on the Linked Clone feature, VMware View Composer allows for rapid provisioning and deployment of VM desktop images. A master image can have patches and upgrades applied without impacting user settings, applications, or data running on the Linked Clones.
- Support for large monitors and multiple monitors.
- VMware View with PCoIP—PCoIP is a remote display protocol that is now available on VMware View 4.0 that allows for a high performance and high quality user experience.
- USB redirection—Allows for USB devices that are physically connected to the VMware View 4.0 Client device to be remotely "redirected" to the VMware View Agent VM.
- Multimedia redirection (MMR)—Provides a greatly enhanced user experience for media such as video streaming.
- ThinApp—Allows administrators to publish encapsulated applications (in EXE or MSI format) that are independent of the operating system, allowing for a faster application deployment time.

VMware View 4.0 Components

This section provides a brief overview of each component that was tested in the VMware View 4.0 architecture. Each component serves a unique purpose within the VMware View architecture and is flexible enough to be deployed in organizations of various sizes with varying requirements.

The VMware View 4.0 components that were tested in this Cisco Validated Design (CVD) include the following:

- View Connection Server (includes the Security Server role)
- View Agent
- View Client
- View Portal

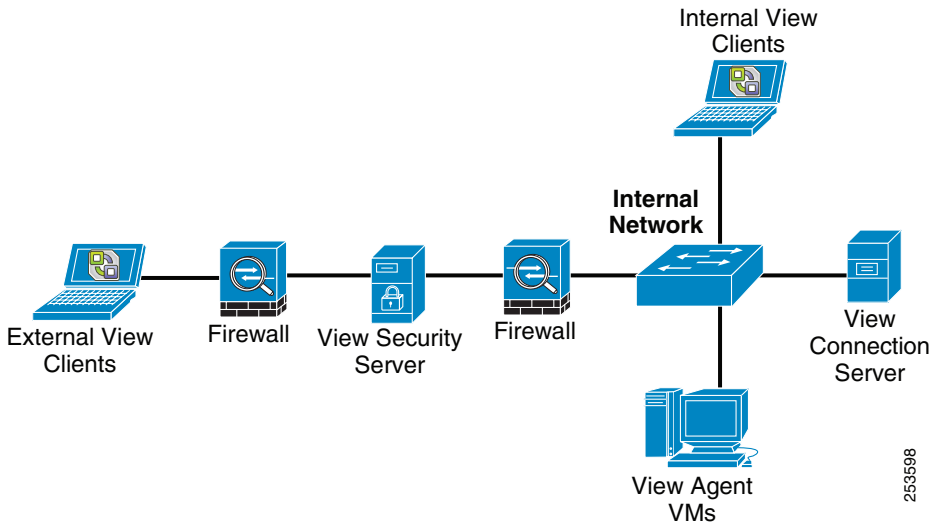
Other required components that support VMware View 4.0 that were used, but are not discussed in detail in this document, include the following:

- Microsoft Active Directory (AD), DNS, DHCP services
- VMware vSphere 4.0 (note that VMware View can run on ESX 3.5 U3 or U4)

Note The sections that follow summarize the four tested VMware View components and are not meant to provide a tutorial on the architecture, design, and operation of each role. Detailed information on the VMware View 4.0 product, architecture, system requirements and design can be found at the following URL: http://www.vmware.com/support/pubs/view_pubs.html.

Figure 3 shows an overview of the common VMware View 4.0 roles and their general locations in the network.

Figure 3 VMware View—High-Level Diagram



View Connection Server/Security Server

The View Connection Server is central to the overall View architecture. The View Connection Server (CS) is home to the View Administrator Console where View desktop sources, user/group entitlement, VM pools, and other policy components are configured. The View CS is installed in one of three modes: Standard, Replica, or Security. The View CS Standard mode is usually used for the first View CS installed, and subsequent View CS installations use the Replica mode. This provides for increased availability of the View CS role as well as load balancing when used with a third-party server load balancer such as the Cisco ACE.

The View CS allows for the following two types of connections between a View Client and a View Agent VM:

- *Direct mode*—A View Client initially establishes an HTTP or HTTPS connection to the View CS for the sake of initial authentication, pool association/entitlement, and View Agent VM association. After this initial connection phase is completed, the View Client establishes a new and "direct" connection to the View Agent VM with which it has been associated. This *second phase* connection, as it is sometimes known, can be over VMware's software implementation of PCoIP, which is the default, or Microsoft RDP.
- *Tunneled mode* (also known as proxy mode)—A View Client establishes an HTTP or HTTPS connection to the View CS, as previously described, with the exception that in this case, the second phase connection is still between the View Client and the View CS. The second phase connection uses an encapsulated RDP-in-HTTP or RDP-in-HTTPS session to the View CS, which then "proxies" the RDP session to the View Agent VM.

The sole purpose of deploying a View Security Server (SS) role is to provide Internet-based View Clients an access method to View Agent VMs over an RDP-in-HTTPS connection. If a remote access VPN solution is available, there is no need to deploy View SS because the user can leverage the remote access VPN solution to gain access to the View Agent VMs via that solution. It is important to note that if PCoIP is the display protocol of choice for View Clients, a remote access VPN solution must be used because the View SS role does not support termination of PCoIP sessions.

View Client

The View Client is used to establish a connection between the View CS, SS and/or View Agent VM (if using direct mode). The View Client software is currently supported only on Microsoft Windows operating systems. VMware partners with Linux-based thin clients to provide support for Linux client variants. VMware View also provides the View Portal implementation, which is a browser-based solution for Linux and Apple Mac OS clients to access the View environment.

View Agent

The View Agent is a software service that runs on each virtual machine that serves View Clients. This View Agent service communicates with the View CS and is managed by the View Administrator Console. The View Agent resides on the guest OS VM running on VMware ESX hosts.

Solution Design and Implementation Details

In addition to the security, application/server availability, and application optimization of VMware View, it is important to also discuss some general deployment considerations for the environment.

General Considerations

VMware provides several options for implementing View to provide users the flexibility to enable/disable functionality based on business and technical requirements. Some of these options include whether to do the following:

- Enable direct mode or tunneled mode for View Client connections
- Use RDP instead of PCoIP
- Enable MMR

It is critical that the reader understands each of these options and performs proof-of-concept testing to assess the impact of any one deployment method. The following section briefly discusses a few of the many considerations related to the above options.

Direct Mode and Tunneled Mode

Direct mode is when a View Client establishes a direct connection over either RDP or PCoIP to the View Agent instead of traversing the View CS for all display protocol activity. Direct mode has many advantages, which include:

- Significantly less load (CPU/memory/network) on the View CS—The View CS responds to the initial first phase connections from View Clients, which is a very low resource-intensive operation. Subsequent data passes directly between the View Client and Agent.
- More granular application visibility for QoS and WAN optimization—Direct mode allows for each protocol in use to be seen and acted upon by network-based policies. These protocols include RDP, PCoIP, MMR, and USB redirection. If tunneled mode is used, all these protocols (excluding PCoIP because it does not support tunneled mode) are encapsulated into HTTP/HTTPS and are no longer visible to the network as independent flows.
- Flexibility to run either RDP or PCoIP.

- Higher availability for in-progress sessions—With direct mode, if a View CS becomes unavailable, the session between the View Client and View Agent does not go down. Only new sessions or sessions that are being re-established fail until the View CS is back online or connections are reestablished via a replica CS.

Direct mode has some disadvantages as well:

- Without comprehensive security policies, it is possible for users to connect directly to the View Agent VM via the standard Microsoft Remote Desktop Connection application over RDP. This connection bypasses the View CS and the associated View policies.
- Direct mode cannot be used with View Security Servers or in an environment where only HTTP or HTTPS is allowed into the data center where the View Agents reside,

Tunneled (proxy) mode is when a View Client establishes a connection to the View CS or SS for all phases of communication including the remote display data sourced from the View Agent VM. Tunneled mode has some advantages, which include the following:

- Tighter access control and policy enforcement—Only a single TCP port needs to be permitted into the data center where the View CS resides. Tunneled mode also deals with the issue of exposing the View Agent VMs subnet(s) to direct access or bypass of View CS policies.
- Allows for an HTTPS connection from any IP-based connection into the View environment using just a single protocol.
- Both HTTP and HTTPS can be optimized by application acceleration solutions such as WAAS/WAAS Mobile.

Tunneled mode weaknesses are direct mode strengths. The following are some of the disadvantages with tunneled mode:

- Significantly more load (CPU/memory/network) on the View CS—The View CS becomes the choke point for View Clients connecting to View Agents. View Clients with an intensive workload can each generate 10s of Mbps flows. When multiple View Clients generate this much traffic, the network throughput can overwhelm the View CS.

Note VMware has a recommended maximum number of concurrent connections with VMware View CS 4.0 which is 1500.

- It becomes much more difficult to differentiate traffic on the network when it is all HTTP or HTTPS. If View traffic is in HTTP/HTTPS, it becomes more difficult to prioritize it above or below standard browser traffic or any other application leveraging HTTP. This is especially true when a mission-critical application such as a financial application is using HTTP with short-lived flows or small payload sizes and it is competing with View, which may be using very long HTTP flows and very large payloads. With generic QoS configurations, both are classified/marked, queued, and policed based on a single class for HTTP. The mission-critical application will most likely suffer in this situation.
- The use of HTTP proxies may interfere with the View Client connections to the View CS or SS.

Data Center Deployment—Location of VMware View Environment

There are generally two places to deploy a VMware View environment, or any VDI deployment for that matter. The first is to integrate the View environment (vSphere, Composer, CS, Agent VMs, and so on) with the existing data center server farms that may already house a virtualization deployment. Some customers refer to this as a *non-dedicated VDI deployment*, meaning that there is no special or dedicated area of the data center for which View resides. This may sound like a reasonable idea at first because it seems less complicated, but it is in fact not a great solution as compared to the second option.

The second option is to build a dedicated View environment that is either logically or physically separate from the existing data center server farms that house other applications. This is known as a *dedicated VDI deployment*. It is important to remember what is happening with View deployments. The clients that are located in the branch or campus areas of the network, the desktop/PC environment, are now also located in the data center. Take all of the planning, security, and management that were needed for a successful branch and campus desktop environment and do it all again *inside* the data center. A new set of challenges now need to be dealt with in the data center that were limited in scope or not present before the VDI deployment occurred. Some of the considerations that need to be dealt with inside the data center when deploying VMware View are as follows:

- Logical or physical separation—Depending on the scale of the View deployment, it may be necessary to procure and physically deploy new networking products such as switches, firewalls, load balancers, and other devices to be used solely for the View deployment. This is very often the case not only for scale but for budget purposes. The VDI deployment may in fact be the responsibility of the desktop services group instead of the data center or network services group. If this is the case, it is common for the desktop services team to fund a dedicated VDI area within the data center. It is quite easy to logically separate the View deployment from the rest of the data center server farms using network and device virtualization. The Nexus product family as well as other products such as the Cisco ACE, ASA, FWSM, and others support capabilities such as Virtual Device Context (VDC) that allow for the logical isolation or compartmentalization of services and network connectivity while still using the same physical hardware.
- DHCP assignment for VMs—For the most part, DHCP client access currently has limited applicability in the data center. It does happen, but it is a rare occurrence. When VMware View Agent VMs are provisioned, they are done so via DHCP. This means that DHCP server resources must support clients in the campus, branch, and now, the data center. IP helper configurations need to be deployed on interfaces servicing the VMware View Agent subnets, and DHCP-based security features such as DHCP snooping should be supported.
- Network security—Cisco has provided branch and campus desktop deployments a suite of features known as Catalyst Integrated Security Features (CISF). This suite is no longer limited to just Catalyst products (Nexus switches support them), and the features are critical to the security of the View Agent VM and the network itself. The common components that provide protection include the following:
  - DHCP Snooping—This feature acts like a firewall between untrusted hosts (View Agent VMs) and trusted DHCP servers. It helps prevent a View Agent VM user from attempting to configure the VM to act as a DHCP server (prevents a VM from sending a DHCP OFFER).
  - Dynamic ARP Inspection (DAI)—This feature validates ARP request and responses. DAI verifies that a packet has a valid IP-to-MAC address binding before updating the ARP cache or forwarding the packet. DAI uses the DHCP snooping database to check validity. DAI helps prevent an ARP poisoning-based man-in-the-middle (MITM) attack.
  - IP Source Guard (IPSG)—This feature filters traffic on interfaces and permits traffic only where the IP and MAC address matches that in the DHCP snooping database or static IP source entries that are configured. IPSG helps prevent a host from spoofing and using the IP address of another host located on another port.

- Endpoint security—Desktop and security teams go through great effort to properly secure client desktops and PCs. Host-based IPS/IDS, firewalls, Microsoft Active Directory Group Policy, and many other tools are used to lock down and secure the client operating system and applications. These same tools now must be deployed in the View Agent VM environment. Remember that a View user may be browsing, downloading, and receiving (via the browser or e-mail) compromised data that can be used to attack other View Agent VMs that are now located inside the data center that may not have the proper security tools in place to protect from these attacks.

Cisco Nexus 1000V—Network Connectivity for the VMware View Environment

Traditionally, the View components such as the View CS and Agent VMs were connected to the network via vSwitches deployed inside each VMware ESX host, which then had physical connections to the switching environment inside the data center. Having a vSwitch with different VLANs and port configurations per ESX host is highly prone to user error when defining these values, and typos or inconsistent configurations can cause failure of connectivity or vMotion migrations. The Cisco Nexus 1000V deals with these issues by providing an integrated Cisco software switch that is deployed across multiple ESX hosts. In the Cisco solution for VMware View, a Cisco Nexus 1000V deployment was used to support the various View components. Figure 4 illustrates the high-level view of the Cisco Nexus 1000V components used in this solution.

Figure 4 Cisco Nexus 1000V—High-level View

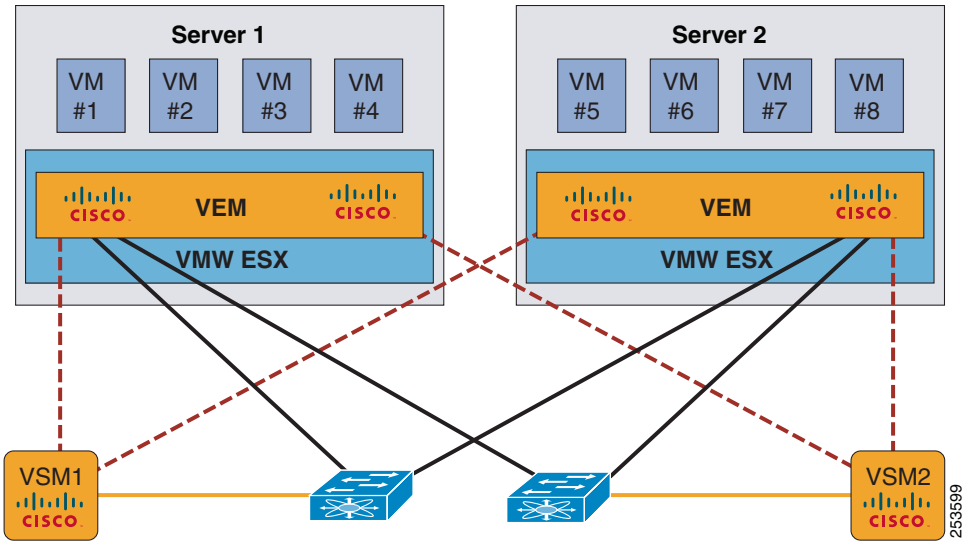


Figure 4 shows that there are two VMware ESX hosts with the Cisco Nexus 1000V VEM installed. The ESX hosts have physical connections outside of the server hardware to a pair of Nexus switches. Two Cisco Nexus 1000V VSMs (primary and standby) manage the VEMs. Many View Agent VMs connect to the VEMs located in each ESX host.

Figure 5 shows the vSphere networking view of the Cisco Nexus 1000V VEM connection.

Figure 5 VMware vSphere Network View—Cisco Nexus 1000V VEM

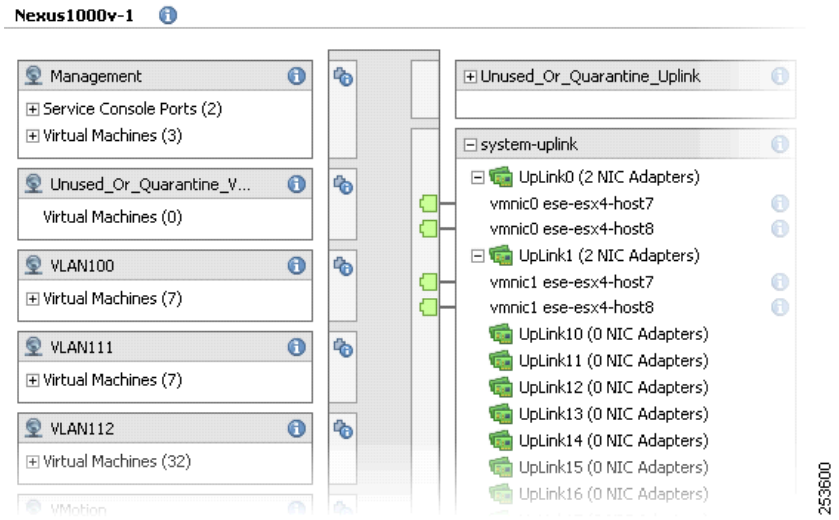


Figure 5 shows *VLAN112* has 32 VMs connected to the VEM (VLANs 112 to 120 are used as View Agent VM VLANs in this document). The VEM has a "system-uplink" definition for both ESX hosts.

To protect the View Agent VMs, network resources, and other services on the network such as DHCP, the Cisco Nexus 1000V needs to be configured to support DHCP snooping, DAI, and IPSG.

DHCP Snooping

DHCP snooping is disabled on the Nexus 1000V by default. When the DHCP snooping feature is enabled on the Nexus 1000V, by default it does not trust vEthernet ports (View Agents VMs and other VMs are attached to these ports), and the Ethernet ports such as uplinks and port channels are trusted. If the DHCP server being used for View Agent VMs is attached to the VEM. The following entry needs to be configured on the vEthernet interface to which the DHCP server is connected:

```
Nexus1000v-1(config-if)# ip dhcp snooping trust
```

For this document, the DHCP server was located in another part of the data center and no special trust command was needed because the DHCP server was located outside of the VEM and automatically "trusted" via an uplink.

The following CLI output shows the default Nexus 1000V DHCP snooping status:

```
Nexus1000v-1# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is disabled
DHCP snooping is configured on the following VLANs:
none
DHCP snooping is operational on the following VLANs:
none
Insertion of Option 82 is disabled
Verification of MAC address is enabled
```

In the following configuration, DHCP snooping has been globally enabled and the VLAN 112 (View Agent VM VLAN) has been configured for monitoring:

```
Nexus1000v-1# conf t
Nexus1000v-1(config)# ip dhcp snooping
Nexus1000v-1(config)# ip dhcp snooping vlan 112
```

The following configuration output shows the updated Nexus 1000V DHCP snooping status:

```
Nexus1000v-1# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
112
DHCP snooping is operational on the following VLANs:
112
Insertion of Option 82 is disabled
Verification of MAC address is enabled
```

The following CLI output shows the DHCP database binding status. These bindings are built when new DHCP exchanges are completed after DHCP snooping has been enabled. Existing DHCP leases that existed prior to DHCP snooping being enabled are not tracked in the binding database.

```
Nexus1000v-1# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type         VLAN  Interface
------------------  ---------------  --------  -----------  ----  -------------
00:50:56:ba:16:0e  10.5.112.12      357509    dhcp-snoop  112   Vethernet23
00:50:56:ba:1d:0e  10.5.112.24      357590    dhcp-snoop  112   Vethernet31
00:50:56:ba:23:64  10.5.112.15      357554    dhcp-snoop  112   Vethernet28
00:50:56:ba:37:d9  10.5.112.11      357675    dhcp-snoop  112   Vethernet21
```

Dynamic ARP Inspection

By default, DAI is disabled on the Nexus 1000V. DAI is enabled by defining a VLAN to inspect:

```
Nexus1000v-1(config)# ip arp inspection vlan 112
Nexus1000v-1(config)# show ip arp inspection vlan 112

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan : 112
-----------
Configuration    : Enabled
Operation State  : Active
```

The following CLI output shows the DAI statistics. Remember that DAI uses the DHCP snooping binding database as a source for inspection. If a host does not have a DHCP binding entry, it fails DAI inspection. It is quite common to see drops when DHCP snooping and DAI have been enabled after a deployment of View Agents with DHCP assigned addresses has already occurred. After those VMs renew DHCP leases or obtain new leases, the DHCP snooping binding table is built, which allows for successful inspection:

```
Nexus1000v-1# show ip arp inspection statistics

Vlan : 112
-----------
ARP Req Forwarded  = 22970
ARP Res Forwarded  = 8221
ARP Req Dropped    = 37061
ARP Res Dropped    = 326
DHCP Drops         = 37387
DHCP Permits       = 8462
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

IP Source Guard

By default, IPSG is disabled on the Nexus 1000V. IPSG is enabled on a per-interface basis and in a View environment, it is configured on each vEthernet interface that connects to or could potentially connect to a View Agent VM (or any other un-trusted VM):

```
Nexus1000v-1# conf t
Nexus1000v-1(config)# interface vethernet 21
Nexus1000v-1(config-if)# ip verify source dhcp-snooping-vlan
```

The following CLI output shows the IPSG status for a vEthernet interface. Again, the IPSG feature leverages the DHCP snooping binding table just like DAI. Entries must be in the binding table before IPSG can inspect properly.

```
Nexus1000v-1(config-if)# show ip verify source interface vethernet 21
Interface         Filter-mode             IP-address     Mac-address       Vlan
------------      -----------             ----------     --------------    ----
Vethernet21       active                  10.5.112.11    00:50:56:ba:37:d9  112
```

Note For more information on the Cisco Nexus 1000V, DHCP snooping, DAI and IPSG, see the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_2/security/configuration/guide/n1000v_security.html.

Optimizing the VMware View Environment

The following subsections describe the design and implementation of VMware View when used with Cisco ASA, Cisco ACE, Cisco NAM, and Cisco WAAS/Cisco WAAS Mobile products.

Table 2 provides a brief overview of which methods of SLB, network optimization, and SSL offload are supported by the View roles.

Table 2 VMware View Roles and LB/Optimization/Offload Methods Supported

View Role	Server Load-Balancing	SSL Offload	Network Optimization
View Security Server	Cisco ACE	Cisco ACE	Cisco WAAS Mobile for View Client access
View Connection Server	Cisco ACE	Cisco ACE	Cisco WAAS/WAAS Mobile for View Client access
View Client	N/A	N/A	Cisco WAAS or Cisco WAAS Mobile

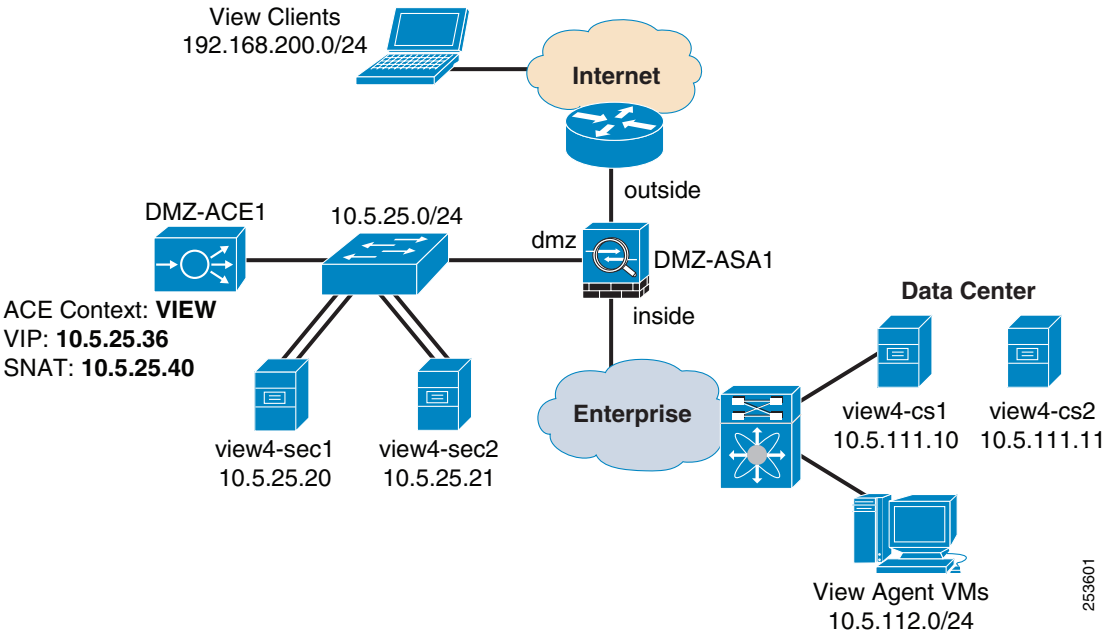
Deploying VMware View Security Servers

The VMware View Security Server (SS) role is a specific type of Connection Server (CS) that acts as an HTTP proxy for incoming View Client or View Portal connections. It is an optional role in the environment and can be excluded if the customer already has or plans to deploy some sort of remote access VPN solution such as the Cisco VPN Client or Cisco AnyConnect Client. If an existing VPN deployment is used, there is little justification for deploying the View SS role.

This section assumes that there is justification for deploying Security Servers and describes the deployment of Cisco ACE for SLB and SSL offload as well as Cisco ASA for perimeter firewall protection of the SS. Note that the Cisco ACE is performing SSL offload (discussed later) for the View SS, so only HTTP is used between the Cisco ACE and the View SS.

Figure 6 illustrates the various components, names, and IP addressing used in the deployment of Cisco ACE for the VMware View Security Server role.

Figure 6 Diagram for Cisco ACE, Cisco ASA, and VMware View SS Role



VMware View Clients are connected to the Internet that use either the VMware View Client or View Portal to connect to the VMware View Agent VMs. The site is connected to the Internet and has a redundant pair of Cisco ASA firewalls for perimeter protection. The Cisco ASA has an interface defined as *dmz* where the Cisco ACE and VMware View SS reside. In this design, the Cisco ACE is operating in one-arm mode but transparent and routed modes are fully supported. The Cisco ASA has an "inside" interface that connects to the rest of the enterprise. There are two VMware View Connection Servers in the data center as well as multiple VMware View Agent VMs.

Note Each Cisco component shown in this design is redundantly configured to remove any single point of failure.

Cisco ASA Configuration for VMware View Security Servers

The VMware View 4.0 Architecture Planning document (http://www.vmware.com/pdf/view40_architecture_planning.pdf) is a must-read document because it does an excellent job of illustrating the actual port breakdown and flow of the various components within the VMware View architecture. The section on the deployment of VMware View Security Servers is the basis for the Cisco ASA configurations that follow.

Table 3 is a summary of Cisco ASA firewall rules that are used for the outside interface. It alters the source and destination information found in the VMware View documentation based on the presence of the Cisco ACE.

Table 3 Cisco ASA Outside Interface Rules

Source	Protocol	Port	Destination
Any	HTTPS	443	Cisco ACE VIP

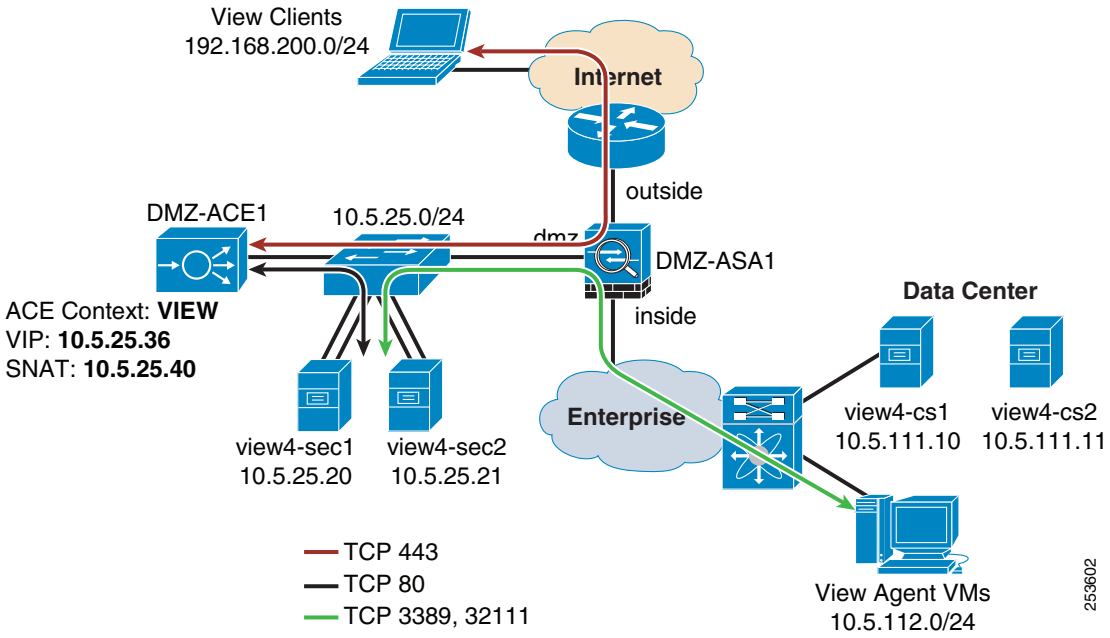
Table 4 provides a summary of the Cisco ASA firewall rules that are used for the DMZ interface.

Table 4 Cisco ASA DMZ Interface Rules

Source	Protocol	Port	Destination
Security Servers	AJP13	8009	Connection Servers
Security Servers	JMS	4001	Connection Servers
Security Servers	USB Redirection	32111	View Agent VMs
Security Servers	RDP	3389	View Agent VMs

Figure 7 illustrates the basic TCP flow between a View Client and the View Agent when connecting from the Internet and using the View Security Servers. Note that the flows between the View SS and View CS are not shown for the sake of clarity.

Figure 7 Traffic Flow—Internet-to-View Agent



In Figure 7, an Internet-based View Client has an HTTPS connection to DMZ-ACE1. DMZ-ACE1 has an HTTP connection to both View Security Servers (for probes as well as data connections). The View Security Servers have connections to the appropriate View Agent VMs over the configured View protocols (RDP, MMR, and USB).

Network Address Translation (NAT) and Port Address Translation (PAT) are commonly used on the perimeter firewall to mask the inside or DMZ addressing from the Internet. In this document, NAT/PAT are not used simply to keep the configuration and diagrams free from confusion related to addressing and flows. All that is needed to make NAT/PAT applicable in a VMware View SS configuration is to have the firewall (or some other device) perform translation on the Cisco ACE virtual IP (VIP) address (10.5.25.36) to the site's IPv4 routable address space, as well as to ensure that the proper Internet DNS entries are defined for that address.

The follow configuration is for the Cisco ASA "DMZ-ASA1". Only relevant configurations for the VMware View deployment are shown.

The following define the three Cisco ASA interfaces "outside," "inside," and "dmz":

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.5.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.5.31.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.5.25.1 255.255.255.0
```

The following define the access control list (ACL) for traffic entering from the Internet to the Cisco ACE VIP IP address (10.5.25.36):

```
access-list VIEW-DMZ-HTTPS extended permit tcp any host 10.5.25.36 eq https
```

The following define the ACL for traffic leaving the "dmz" to the "inside". Allow access from each SS to each CS as well as the View Agent VM subnet(s):

```
access-list VIEW-DMZ-INSIDE extended permit tcp host 10.5.25.20 host 10.5.111.10 eq 8009
access-list VIEW-DMZ-INSIDE extended permit tcp host 10.5.25.20 host 10.5.111.10 eq 4001
access-list VIEW-DMZ-INSIDE extended permit tcp host 10.5.25.20 10.5.112.0 255.255.255.0
eq 32111
access-list VIEW-DMZ-INSIDE extended permit tcp host 10.5.25.20 10.5.112.0 255.255.255.0
eq 3389
access-list VIEW-DMZ-INSIDE extended permit tcp host 10.5.25.21 host 10.5.111.11 eq 8009
access-list VIEW-DMZ-INSIDE extended permit tcp host 10.5.25.21 host 10.5.111.11 eq 4001
access-list VIEW-DMZ-INSIDE extended permit tcp host 10.5.25.21 10.5.112.0 255.255.255.0
eq 32111
access-list VIEW-DMZ-INSIDE extended permit tcp host 10.5.25.21 10.5.112.0 255.255.255.0
eq 3389
```

The following apply the above ACLs to the appropriate interfaces:

```
access-group VIEW-DMZ-HTTPS in interface outside
access-group VIEW-DMZ-INSIDE in interface dmz
```

Use the **show conn** command on the Cisco ASA to show the connections flowing through the firewall:

```
DC1-ASA1# sh conn
. . .
TCP outside 192.168.200.10:1346 dmz 10.5.25.36:443, idle 0:00:04, bytes 2814, flags UIOB
TCP outside 192.168.200.10:1345 dmz 10.5.25.36:443, idle 0:00:00, bytes 136835, flags UIOB
TCP outside 192.168.200.10:1344 dmz 10.5.25.36:443, idle 0:00:07, bytes 7118, flags UIOB
TCP dmz 10.5.25.20:4550 inside 10.5.112.13:32111, idle 0:00:00, bytes 5915, flags UIOB
TCP dmz 10.5.25.20:4549 inside 10.5.112.13:3389, idle 0:00:00, bytes 82557, flags UIOB
TCP dmz 10.5.25.21:1210 inside 10.5.111.10:4001, idle 0:00:03, bytes 2594, flags UIOB
```

```
TCP dmz 10.5.25.20:4545 inside 10.5.111.11:4001, idle 0:00:03, bytes 3445, flags UIOB
TCP dmz 10.5.25.20:4544 inside 10.5.111.11:4001, idle 0:00:03, bytes 3324, flags UIOB
TCP dmz 10.5.25.21:1209 inside 10.5.111.11:4001, idle 0:00:16, bytes 758, flags UIOB
TCP dmz 10.5.25.20:4540 inside 10.5.111.11:8009, idle 0:00:00, bytes 1037469, flags UIOB
TCP dmz 10.5.25.21:1207 inside 10.5.111.11:8009, idle 0:00:00, bytes 1150478, flags UIOB
```

Cisco ACE Considerations for VMware View Security Servers

The following subsections describe the basics of load balancing and SSL offload, and how the Cisco ACE participates with the VMware View Security Servers.

Load Balancing Overview

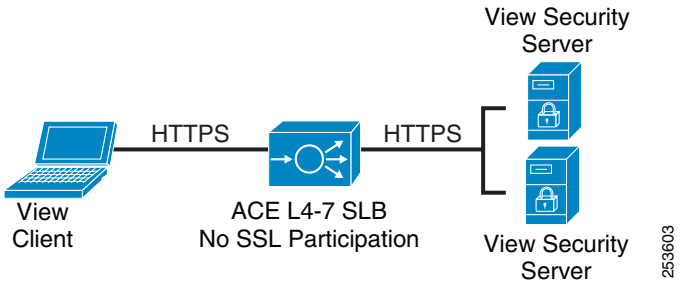
In this design, the Cisco ACE is performing Layers 4to 7 SLB services as well as SSL offload (also known as SSL termination) for the VMware View Security Servers. The following steps illustrate the basic flow of SLB for View SS:

1. The client uses either the VMware View Client or the View Portal to connect to the Cisco ACE and is routed to the most appropriate View SS (based on the Cisco ACE SLB policy). The Cisco ACE VIP is in DNS and is used as the name/IP address in the View Client or Portal.
2. The SS that received the RDP-in-HTTPS tunneled connection from the Cisco ACE contacts the View CS for initial authentication and setup (this is sometimes known as “phase 1”). Based on the information exchange between the SS and CS, a new connection is established (this is sometimes known as “phase 2” or the “tunnel phase”).
3. The SS creates a connection directly to the View Agent VM that is associated with the pool, policy, and entitlement for the authenticated user.
4. The View Client now has an authenticated active connection through the Cisco ACE, through the SS, and to the View Agent VM.

SSL Offload Overview

Several options are available for using the Cisco ACE with SSL offload in conjunction with the VMware View Security Servers. The first option (see Figure 8) shows the Cisco ACE performing basic load balancing for two Security Servers. The Cisco ACE uses its SLB policy to monitor the health (via a probe) of both Security Servers and pass SSL connections to the most appropriate SS based on the SLB policy. The Cisco ACE performs no SSL functions.

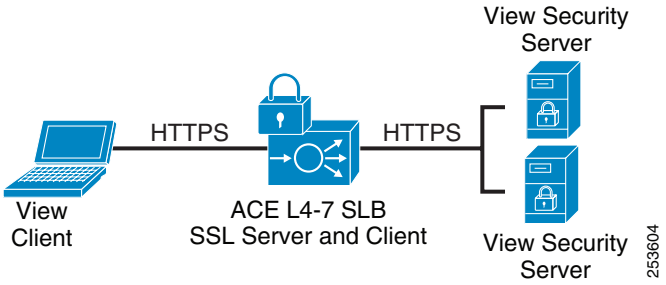
Figure 8 Cisco ACE + Security Servers—Basic Layer 4 SLB



The second option (see Figure 9) shows the Cisco ACE performing load balancing along with SSL offload between the client and the Cisco ACE with SSL reestablishment from the Cisco ACE to the SS. This combined SSL termination and SSL initiation is called *SSL end-to-end*. One advantage of SSL end-to-end is that it offers the capability of maintaining a level of encryption between the Cisco ACE

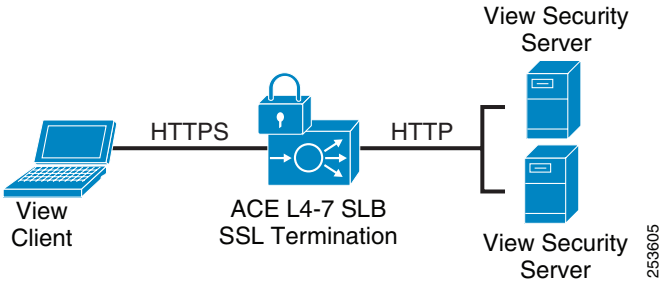
and server, but allows for the use of a lower cipher than the client-to-Cisco ACE connection, which can lessen the SSL load on the SS. Figure 9 shows the Cisco ACE serving the role of SSL server (to the client) and also SSL client (to the SS).

Figure 9 Cisco ACE + Security Servers—SSL End-to-End



The third option (see Figure 10) incorporates the Cisco ACE performing load balancing and SSL termination, the SSL connection terminating on the Cisco ACE, and the Cisco ACE communicating with the SS over HTTP. This approach allows for the offloading of resource-intensive SSL operations to the Cisco ACE, which provides hardware-based SSL offload. This document focuses on the third option.

Figure 10 Cisco ACE +Security Servers—SSL Termination



VMware View 4.0 Security Server Configuration Summary

This subsection provides a brief overview of the required configurations on the VMware View 4.0 Security Servers to include the CS-specific configurations.

These configurations are not meant to be a replacement for the instructions found in the VMware View 4.0 documentation but are shown to add context to the overall design.

The following are summary steps to enable VMware View 4.0 Security Servers for Cisco ACE SLB and SSL offload are as follows:

Step 1 Ensure the VMware View Connection Server(s) are properly deployed.

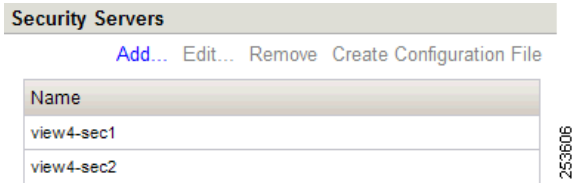
Step 2 Install the VMware View Security Server role on the appropriate servers or VM in the DMZ.

Step 3 Use the VMware View Administrator GUI to identify the View Security Servers.

Step 4 Use either the **Create Configuration File** option in the View Administrator console and/or the **locked.properties** method to fully define the port and protocol usage for the client and security server connections.

Figure 11 shows the View Administrator console with both View Security Servers defined.

Figure 11 Security Servers List in the View Administrators Console



In addition to defining the View Security Servers in the View Administrator console, the Security Servers need to be configured to allow SSL offload to work by configuring the **External URL** to be the DNS name of the Cisco ACE VIP used to terminate the HTTPS sessions from the View Clients on the Internet. In the configuration used in this document, the fields shown in Table 5 were populated for each SS in the View Administrator console.

Table 5 Populated Fields

Security Server	Server Name Field	External URL Field
View4-sec1	view4-sec1	https://view-ext.ese.com:443
View4-sec2	view4-sec2	https://view-ext.ese.com:443

After the View Security Servers are defined in the View Administrator console, a file needs to be created on each SS (or copied if using the "Create Configuration File" method). The "locked.properties" file needs to be created or copied to the **C:\Program Files (x86)\VMware\VMware View\Server\sslgateway\conf** directory on each SS.

The contents of the file should reflect the following:

```
clientProtocol=https
clientHost=view-ext.ese.com
clientPort=443
serverPort=80
serverProtocol=http
```

Note The definition of each option can be found in the Appendix section of the View Manager Administration Guide located at the following URL: http://www.vmware.com/pdf/view40_admin_guide.pdf.

In the design discussed in this document, the following options apply:

- **clientProtocol=https**—Indicates that the client will use HTTPS to connect to the Cisco ACE.
- **clientHost=view-ext.ese.com**—Indicates that the client will connect on the tunnel phase (second phase) to the DNS name that resolves to the Cisco ACE VIP (view-ext.ese.com resolves to 10.5.25.36).
- **clientPort=443**—Indicates the port the client will use to connect. This entry seems redundant because the *clientProtocol* field is already there, but the VMware documentation states that if this entry is not defined, the client will use whatever is defined in the *serverProtocol* field, which will be 80.
- **serverPort=80**—Indicates the port that the Cisco ACE will use to connect to the SS. Remember that SSL offload is being used, so the connection between the Cisco ACE and View SS is HTTP.

- **serverProtocol=http**—This entry is not needed because HTTP is the default, but is included here for clarity.

Cisco ACE Configuration for the View Security Server

The Cisco ACE 4710 Appliance is used in this document. The following configuration gives the basics on setting up the Cisco ACE for network access.

Note Only the basic configuration items that are directly relevant to the design in this document are discussed.

The following configuration steps are performed on the console in the Admin context:

Step 1 Configure the Cisco ACE interfaces. The ACE can be configured with port channels (recommended) or on a per-interface basis:

```
interface port-channel 1
 switchport trunk native vlan 10
 switchport trunk allowed vlan 10,25,43
 port-channel load-balance src-dst-port
 no shutdown
!
interface gigabitEthernet 1/4
 channel-group 1
```

Step 2 Configure IPv4 addresses on the interface and configure static route (management interface not shown):

```
interface vlan 25
  ip address 10.5.25.30 255.255.255.0
  no shutdown
!
ip route 0.0.0.0 0.0.0.0 10.5.25.1
```

Define the Cisco ACE Context for View

The context must be defined and associated with the appropriate one-arm VLAN. The following configuration is applied in the Admin Cisco ACE context:

```
context VIEW
  description Context for VIEW SS
  allocate-interface vlan 25
```

Remote Management Access

To access the Cisco ACE remotely using Telnet, SSH, SNMP, HTTP, or HTTPS; or to allow ICMP access to the Cisco ACE, a service policy must be defined and applied to the interface(s) through which access is to be permitted. The following configuration steps are required:

Step 1 Configure a **class-map** of type management:

```
class-map type management match-any MGMT
  2 match protocol xml-https any
  4 match protocol icmp any
  5 match protocol telnet any
  6 match protocol ssh any
  7 match protocol http any
  8 match protocol https any
  9 match protocol snmp any
```

Step 2 Configure a **policy-map** of type management:

```
policy-map type management first-match MGMT
  class MGMT
    permit
```

Step 3 Apply a **policy-map** to the VLAN interfaces:

```
interface vlan 25
  service-policy input MGMT
```

IP Access through the Cisco ACE

Interface VLANs must be configured for Layer-3 connectivity through the Cisco ACE. Service policies for load balancing, security, and management access to Cisco ACE are also applied at the interface VLAN level.

Basic interface configuration includes the following:

Step 1 Configure an ACL to permit/deny traffic through the Cisco ACE:

```
access-list EVERYONE line 8 extended permit icmp any any
access-list EVERYONE line 16 extended permit ip any any
```

Step 2 Apply an ACL to the interface:

```
interface vlan 25
  access-group input EVERYONE
  no shutdown
```

Resource Class—Preparing for Sticky

Later in this document, an SLB sticky configuration is used to ensure Internet clients connect to the same SS between phase 1 and phase 2 connections. To successfully configure sticky, a resource class must be defined in the Admin context. Note that the minimum requirement for the resource class is to define the "limit-resource sticky" values.

Step 1 Define a resource class to be used by sticky Cisco ACE:

```
resource-class STICKY
 limit-resource all minimum 15.00 maximum unlimited
 limit-resource sticky minimum 15.00 maximum equal-to-min
```

Step 2 Apply resource class to the VIEW context:

```
context VIEW
  member STICKY
```

Configure Connectivity for the VIEW Context

To configure connectivity for the VIEW context:

```
access-list EVERYONE line 10 extended permit icmp any any
access-list EVERYONE line 20 extended permit ip any any
!
class-map type management match-any MGMT
  2 match protocol xml-https any
  4 match protocol icmp any
  5 match protocol telnet any
  6 match protocol ssh any
  7 match protocol http any
```

```
    8 match protocol https any
    9 match protocol snmp any
  !
  policy-map type management first-match MGMT
    class MGMT
      permit
  !
  interface vlan 25
   ip address 10.5.25.35 255.255.255.0
   access-group input EVERYONE
   service-policy input MGMT
   no shutdown
  !
  ip route 0.0.0.0 0.0.0.0 10.5.25.1
  !
```

Probes

Cisco ACE uses probes to verify the availability of a real server. Probes are configured by defining their type and name.

Various types of probes can be configured on Cisco ACE. The following output example lists these probes:

```
DMZ-ACE1/VIEW(config)# probe ?
  dns       Configure dns probe
  echo      Configure echo probe
  finger    Configure finger probe
  ftp       Configure ftp probe
  http      Configure http probe
  https     Configure https probe
  icmp      Configure icmp probe
  imap      Configure imap probe
  pop       Configure pop probe
  radius    Configure radius probe
  rtsp      Configure rtsp probe
  scripted  Configure script probe
  sip       Configure sip probe
  smtp      Configure smtp probe
  snmp      Configure snmp probe
  tcp       Configure tcp probe
  telnet    Configure telnet probe
  udp       Configure udp probe
```

Some key timers and parameters must be tuned when probes are configured. These parameters influence how rapidly Cisco ACE (or any load balancer) takes a server out of rotation and brings it back into service.

The following parameters can be tuned for probes of any type (ICMP, UDP, TCP, HTTP, HTTPS, or scripted):

- *faildetect*—Refers to the number of consecutive failed probes that qualify a server to be declared failed. The faildetect parameter is configured as a counter value. The default value is 3.
- *interval*—Refers to the frequency with which the Cisco ACE sends probes to a server. The interval is configured in seconds. The default value is 120 seconds.
- *passdetect*—Determines how the Cisco ACE reprobes the server after the server has been declared failed. The passdetect variable has two attributes:

  - *passdetect count*—Refers to the number of consecutive successful responses that a Cisco ACE must see before declaring a server as operational. The default value is 3. This value can be tuned according to the requirements.
  - *passdetect interval*—Refers to the number of seconds that a Cisco ACE waits to probe a server after the server has been declared failed. The default value is 300 seconds.

These additional parameters can be configured for TCP, HTTP, and HTTPS probes:

- *Open*—Refers to the duration (in seconds) that Cisco ACE waits to establish a TCP connection with the server. The default value is 10 seconds. Generally, if adjusted this value is configured lower to more aggressively fail the probe which cannot open TCP connections to a server quickly, as this indicates that the server is having difficulty accepting new connections.
- *Receive*—After a TCP SYN (for a probe) is sent to a server, the value for the receive parameter determines the amount of time that a Cisco ACE waits to receive a reply from the server. This value is configured in seconds and the default value is 10 seconds. This parameter must be configured as equal-to-or-less-than the value interval.
- *Connection*—This parameter determines how the Cisco ACE closes the connection after it has successfully sent a probe. By default, the Cisco ACE closes the connection by sending a TCP FIN to close the connection (referred to as a *graceful* connection termination). Optionally, the Cisco ACE can be configured to close the connection with a TCP RESET by configuring connection parameter as *forced*.
- *Port*—TCP/UDP port number on which this probe is sent. The default values for various probes are as follows:
  - TCP—Port 80
  - UDP—Port 53
  - HTTP—Port 80
  - HTTPS—Port 443
- *Request*—Used to configure the HTTP Request method (HEAD or GET) and URL for the probe. The default method is GET and default URL is /. Generally, method and URL are configured according to specific applications.

  This parameter is only applicable to HTTP/HTTPS probes.
- *Expect*—Allows Cisco ACE to detect two values from the server:
  - *expect status*—The HTTP status code (or range) to expect from the server. There is no default HTTP return code expected; it must be explicitly configured.
  - *expect regex*—A regex can be configured to parse a specific field in the response data.

  This parameter is only applicable to HTTP/HTTPS probes.
- *SSL*—Configured to define the cipher and SSL version that the Cisco ACE should use when sending an HTTPS probe. Ciphers and SSL versions supported on Cisco ACE are as follows:

```
ssl cipher:
  RSA_EXPORT1024_WITH_DES_CBC_SHA  EXP1024-DES-CBC-SHA Cipher
  RSA_EXPORT1024_WITH_RC4_56_MD5   EXP1024-RC4-MD5 Cipher
  RSA_EXPORT1024_WITH_RC4_56_SHA   EXP1024-RC4-SHA Cipher
  RSA_EXPORT_WITH_DES40_CBC_SHA    EXP-DES-CBC-SHA Cipher
  RSA_EXPORT_WITH_RC4_40_MD5       EXP-RC4-MD5 Cipher
  RSA_WITH_3DES_EDE_CBC_SHA        3DES-EDE-CBC-SHA Cipher
  RSA_WITH_AES_128_CBC_SHA         AES-128-CBC-SHA Cipher
  RSA_WITH_AES_256_CBC_SHA         AES-256-CBC-SHA Cipher
  RSA_WITH_DES_CBC_SHA             DES-CBC-SHA Cipher
  RSA_WITH_RC4_128_MD5             RC4-MD5 Cipher
```

```
    RSA_WITH_RC4_128_SHA              RC4-SHA Cipher

  ssl versions:
    SSLv2  SSL Version 2.0
    SSLv3  SSL Version 3.0
    TLSv1  TLS Version 1.0
```

This parameter is only applicable to HTTPS probes.

To ensure that the View Security Servers are online and ready to accept connections, the Cisco ACE is configured to perform a health check to determine whether the server is up and running and available via HTTP. There are two layers to availability with View SS. The first is monitoring the health of each SS, but there is also the requirement to ensure that the health of the CS with which each SS is associated is also monitored. There is no point in connecting a client request to an SS that has no way of communicating with its associated CS if the CS is down. Remember that when the SS is first installed, the user is prompted with the name of the CS with which the SS will communicate. SS to CS communication is 1:1 and VMware does not support having one SS communicate with multiple CS's simultaneously. The following Cisco ACE health probe probes the SS using a specific GET URL. When the Cisco ACE probes the SS, the SS immediately performs a check against the CS for which it is configured. This check between the SS and CS happens over the AJP13 (TCP 8009) connection.

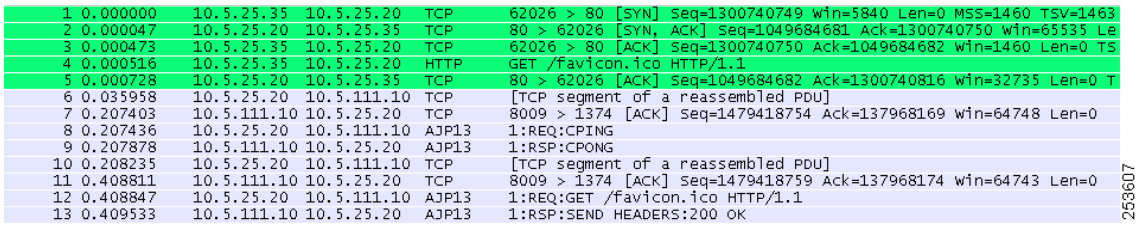
The following is a configuration example for HTTP:

```
probe http VIEW_SS_HTTP
  interval 5
  passdetect interval 5
  request method get url /favicon.ico
  expect status 200 200
  open 1

DMZ-ACE1/VIEW# show probe

 probe       : VIEW_SS_HTTP
 type        : HTTP
 state       : ACTIVE
----------------------------------------------
   port      : 80      address     : 0.0.0.0         addr type  : -
   interval  : 5       pass intvl  : 5               pass count : 3
   fail count: 3       recv timeout: 10
               ------------------ probe results ------------------
   associations ip-address      port  porttype probes   failed   passed   health
   ------------ ---------------+-----+--------+--------+--------+--------+------
   serverfarm  : VIEW_SS_SLB
     real      : VIEW4-SEC1[80]
                 10.5.25.20      80    REAL     1002     0     1002        SUCCESS

     real      : VIEW4-SEC2[80]
                 10.5.25.21      80    REAL     1001     0     1001        SUCCESS
```

When a probe is sent to the SS, the SS sends an AJP13-based request (1:REQ:CPING) to the CS and if the CS is alive, it responds (1:RSP:CPONG). In addition to this CPING/CPONG, the SS sends another AJP13-based request to check for the "VMware View Connection Server" service's ability to serve the HTTP request.

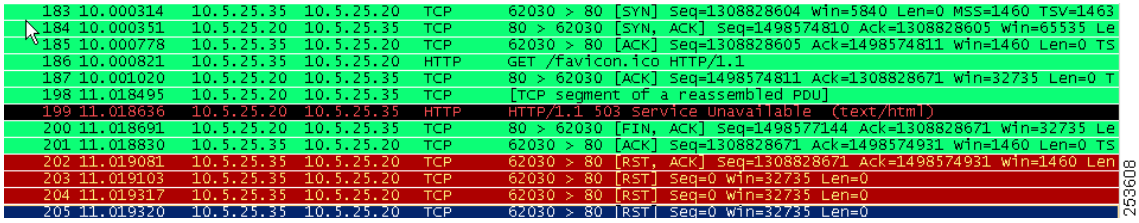
Figure 12 shows a small subset of a successful health probe sequence as seen via Wireshark on the View SS. The capture shows the probe from the Cisco ACE interface (10.5.25.35) to view4-sec1 (10.5.25.20). After the View SS receives the GET, it sends a sequence of AJP13 requests to its configured CS (view4-cs1 10.5.111.10). The CS responds with "200", which is what the Cisco ACE expects in the probe configuration.

Figure 12 Wireshark Capture—Successful Health Probe



When the CS fails or is down for service, the health probe fails and the Cisco ACE takes that failed *rserver* out of service. Figure 13 shows a failed health probe check. In this case, the CS was rebooted after an update. The SS responded to the Cisco ACE with a “503 Service Unavailable”. The Cisco ACE takes that SS out-of-service until the health probe passes.

Figure 13 Wireshark Capture—Failed Health Probe



The output from the **show probe** command on the Cisco ACE shows that the view4-sec1 (10.5.25.20) is failing the probe, and incoming client requests will not be sent to that SS until it passes the probes.

```
DMZ-ACE1/VIEW# show probe

 probe       : VIEW_SS_HTTP
 type        : HTTP
 state       : ACTIVE
----------------------------------------------
   port      : 80      address     : 0.0.0.0         addr type  : -
   interval  : 5       pass intvl  : 5               pass count : 3
   fail count: 3       recv timeout: 10
                ------------------ probe results ------------------
   associations ip-address      port  porttype probes   failed   passed   health

   ------------ ---------------+-----+--------+--------+--------+--------+------

   serverfarm  : VIEW_SS_SLB
     real      : VIEW4-SEC1[80]
                 10.5.25.20      80    REAL     29271    42       29229    FAILED

     real      : VIEW4-SEC2[80]
                 10.5.25.21      80    REAL     29272    0        29272    SUCCESS
```

This particular probe accomplishes two tasks, because the probe monitors both Security Servers that monitor the connection to each CS. If any one component goes down, the health probe takes the appropriate action to ensure that client connections are not sent to a dead service.

Real Server

The load balancer selects the real servers (called *rserver* in the Cisco ACE) to send the intended traffic based on a certain set of criteria. When configuring an rserver, be aware that the rserver name is case-sensitive. The minimum configuration needed for rserver configuration is the IP address and configuring the rserver as **inservice**. The name of the rserver is locally significant and need not match the real name or DNS name of the server.

To take a server out of rotation on a per-server farm basis, rserver should be specified as **no inservice** at the server farm level. The following is an example of configuring rserver on Cisco ACE:

```
rserver host VIEW4-SEC1
  ip address 10.5.25.20
  inservice
rserver host VIEW4-SEC2
  ip address 10.5.25.21
  inservice
```

Server Farm

A *server farm* is a logical collection of rservers that the load balancer selects based on a certain set of criteria. As with the rserver, the server farm name is also case-sensitive.

Basic server farm configuration includes adding rservers and probes to the server farm.

Key configuration options within server farm sub-configuration mode are as follows:

- *failaction*—Defines the action that the Cisco ACE should take with respect to currently established connections if an rserver is detected as probe_failed. The default behavior for Cisco ACE is to take no action and to allow the connections to close gracefully or time out.

  A configurable option is *failaction purge*, which forces Cisco ACE to remove the connections established to that rserver and send TCP RST(s) towards the client(s) and rserver(s).

- *predictor*—Refers to the load-balancing algorithm for the server farm. Options are:
  - *hash*—Based on source/destination IP address, URL, cookie, and header.
  - *leastconns*—Based on least number of connections. Slow start is enabled for leastconns and its timing can be tuned using predictor leastconns slow start. Slow start can be used to avoid sending a high rate of new connections to servers that have recently been put into service.
  - <1-65535> Specify slow start duration in seconds.
  - *roundrobin*—Load balance in a roundrobin fashion (default).

- *probe*—Allows a probe to be applied to the server farm. Multiple probes can be applied to the same server farm.

- *retcode*—Used to configure server health checks based on the HTTP return code. The configuration allows for the definition of a range of HTTP return codes and take an action when a threshold is reached. The syntax is as follows:

  retcode <*min*> <*max*> **check** <**remove** | **count** | **log**> <*threshold value*> **resume-service** <*value in seconds*>

- *rserver*—Used to associate real servers with a server farm. Port address translation, maximum and minimum connections, and weight are some common configurations that can be done in rserver sub-configuration mode.

- *transparent*—Equivalent to **no nat server** on the Content Switching Module (CSM) and **type transparent-cache** on the Content Services Switch (CSS). When configured, Cisco ACE does not perform NAT on a Layer-3 IP address from the VIP to the rserver's IP address.

The following is an example of the server farm configuration for the View SS. Note that it is important to define the server destination port 80 when using SSL offload because client connections using HTTPS must be translated to port 80 on the ACE-to-SS connection. Without the port definition the ACE would communicate with the View SS using the same port the client used (443) and this would fail as the View SS is configured to only accept port 80 connections:

```
serverfarm host VIEW_SS_SLB
  predictor leastconns slowstart 300
  probe VIEW_SS_HTTP
  rserver VIEW4-SEC1 80
    inservice
  rserver VIEW4-SEC2 80
    inservice
```

Load Balancing

The Cisco ACE can load balance HTTP/HTTPS sessions based on IP addresses and ports (Layer-3 and Layer-4 SLB) or can persistently load balance via Layer-7 information.

The following example shows the configuration steps needed.

Step 1 Configure the VIP using **class-map** of type **match-all** for HTTPS.

```
class-map match-all VIEW_SS
  2 match virtual-address 10.5.25.36 tcp eq https
```

Step 2 Configure the **policy-map** of type **loadbalance** to include the server farm.

```
policy-map type loadbalance http first-match VIEW_SS
  class class-default
    sticky-serverfarm SS_STICKY
```

Step 3 Configure **policy-map** of type **multi-match** to associate the **class-map** configured in Step 1. Other options listed allow the VIP to reply to ICMP echoes:

```
policy-map multi-match VIEW-SLB-MULTI
  class VIEW_SS
    loadbalance vip inservice
    loadbalance policy VIEW_SS
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 25
```

Step 4 Apply **policy-map** to the interface VLAN.

```
interface vlan 25
  ip address 10.5.25.35 255.255.255.0
  nat-pool 1 10.5.25.40 10.5.25.40 netmask 255.255.255.0 pat
  service-policy input VIEW-SLB-MULTI
```

Note The **nat dynamic 1 vlan25** and **nat-pool 1** configurations are required in one-arm mode to force return traffic from the SS back to the Cisco ACE. Without this configuration, the source IP address the SS sees is the IP address of the client. The return packets from the SS bypass the Cisco ACE and go directly to the client and break the connection. In this configuration, the source IP the SS sees is 10.5.25.40 and replies to that address for all return packets.

Step 5 Configure a sticky policy so that client connections "stick" to the same SS for both phase 1 and phase 2 (tunnel) connections. The **255.255.255.255 address source** entry indicates that each client will have a unique entry in the sticky database based on their source IP address. Normally, Cisco recommends using another form of persistence such as a cookie or JSessionID, but VMware View does not support this functionality.

```
sticky ip-netmask 255.255.255.255 address source SS_STICKY
  replicate sticky
  serverfarm VIEW_SS_SLB
!
policy-map type loadbalance http first-match VIEW_SS
  class class-default
    sticky-serverfarm SS_STICKY
```

Note As was mentioned in Step 5, Cisco does not normally recommend using sticky as the primary form of persistence, especially when clients are connecting from the Internet. Source IP-based sticky for Internet-based clients causes uneven distribution of SLB sessions because of the extensive use of NAT/PAT or proxy. If several users originate from behind the same NAT, the ACE sees only one IP address (the external NAT address) and it "sticks" those sessions to the same SS/CS. To avoid this, VMware should support another form of persistence like many other applications such as cookies or JSessionIDs.

SSL Termination

Note The discussion of certificates, other than the server certificate on the Cisco ACE, is outside the scope of this document. A thorough understanding of certificates and server authentication is required for anyone deploying the VMware View solution with or without the Cisco ACE.

With frontend SSL termination, client-to-Cisco ACE traffic is HTTPS, but the Cisco ACE-to-SS traffic is HTTP. It is important to understand that the certificate being configured on the Cisco ACE is known as a *server certificate* because the Cisco ACE is acting as a server to the client. Any client connecting to the Cisco ACE for the purpose of accessing the SS must trust the Cisco ACE server certificate by having the certification authority (CA) certificate (from the CA that issued the Cisco ACE certificate) in the client's certificate store.

There are two critical considerations to know when dealing with SSL offload on the Cisco ACE and the VMware View Security Servers:

- The *common-name* in the Cisco ACE CSR parameters must match the DNS name for the VIP that is used to terminate the SSL connection.
- The *clientHost*= value in the **locked.properties** file (also defined in the External URL field) must match the *common-name*.

In this document, the following values all match:

- *common-name* = **view-ext.ese.com**
- DNS for VIP = **view-ext.ese.com**
- *clientHost*=**view-ext.ese.com**
- External URL (if defined from View Administrator console) = **view-ext.ese.com**

The following configuration steps illustrate implementing frontend SSL termination:

Step 1 Generate the key.

```
DMZ-ACE1/VIEW# crypto generate key 1024 viewsslkey.pem
DMZ-ACE1/VIEW# show crypto key all
Filename                                 Bit Size Type
--------                                 -------- ----
viewsslkey.pem                           1024     RSA
```

Step 2 Define the CSR parameters set.

```
crypto csr-params VIEWSSL
  country US
  state California
  locality San Jose
  organization-name Cisco
  organization-unit ESE
  common-name view-ext.ese.com
```

Step 3 Generate the Certificate Signing Request (CSR).

```
DMZ-ACE1/VIEW# crypto generate csr VIEWSSL viewsslkey.pem
-----BEGIN CERTIFICATE REQUEST-----
MIIBrjCCARcCAQAwbjELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEx
ETAPBgNVBAcTCFNhbiBKb3NlMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDRVNF
MRkwFwYDVQQDExB2aWV3LWV4dC5lc2UuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQC2KG2jyBUEo7WZwwzBuYDLdxcb1wJ7dvcFBIl3CcjphPBRCo4Z4tKz
aHrqp0KIunB7iJpSR6OAp7mb6euMfEtD1BULH+SAgl1NCZODdblw1e4in+lcNIXq
Ycoj1evemdQLZD7u8DgXje7KKOpVaZLw9Soh9MnxnG4x17iEqrCHLQIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEAb+1iS5K8vx8Ipac9EPIABCHmyYiByVzKxDFGC0p0
Zm1TH1cz+rsmelewOH3qoswJkl4DTBLx5BrbnYw3XXpHgze2ZIoVt5OovCNgBaS1
MWNpCLR3qlCqgFPeJQXMrvFs0YJ3rAlVddM/77+GDCHXMYR7tfsnHUeeh+qbZvTC
q2k=
-----END CERTIFICATE REQUEST-----
```

Step 4 Obtain the certificate.

The SSL certificate can be obtained from various CA companies. Following is an example of using OpenSSL to obtain a certificate for testing. The above CSR output was captured to a **view-ssl-req.pem** file:

```
[root@SSL-1 sslcert]# openssl ca -out viewssl-cert.pem -config ./openssl.cnf -infiles
viewssl-req.pem
Using configuration from ./openssl.cnf
Enter pass phrase for ./private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'California'
localityName          :PRINTABLE:'San Jose'
organizationName      :PRINTABLE:'Cisco'
organizationalUnitName:PRINTABLE:'ESE'
commonName            :PRINTABLE:'view-ext.ese.com'
Certificate is to be certified until Dec  3 20:18:33 2010 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Step 5 Import the certificate on Cisco ACE:

```
DMZ-ACE1/VIEW# crypto import sftp 10.5.100.25 shmcfarl viewssl-cert.pem viewssl-cert.pem
Password:
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
##
Successfully imported file from remote server.
```

Note Optionally, the certificate can be imported from the terminal without copying the file over. See the Cisco ACE documentation on using the terminal method.

Step 6 Validate the certificate using the key.

```
DMZ-ACE1/VIEW# crypto verify viewsslkey.pem viewssl-cert.pem

Keypair in viewsslkey.pem matches certificate in viewssl-cert.pem.
```

Step 7 Configure SSL proxy service as follows:

```
ssl-proxy service SSL-Proxy-VIEW
 key viewsslkey.pem
 cert viewssl-cert.pem
```

Step 8 Apply the SSL proxy server policy.

```
policy-map multi-match VIEW-SLB-MULTI
  class VIEW_SS
    ssl-proxy server SSL-PROXY-VIEW
```

Step 9 Apply the policy-map as a **service policy** on the one-arm VLAN.

```
interface vlan 25
  ip address 10.5.25.35 255.255.255.0
  service-policy input VIEW-SLB-MULTI
```

The basic SSL offload configuration is complete. In addition to standard SSL offload, it is important to configure the ACE to perform redirection automatically for any client connection that may come in as HTTP. This happens frequently when a user does not have the "Use secure connection (SSL)" option checked in the VMware View Client or if a View portal user connects via http://view-ext.ese.com instead of https://view-ext.ese.com. The Cisco ACE can perform this HTTP-to-HTTPS redirection by using a redirection policy.

The following configuration example performs a redirection on HTTP traffic coming into the ACE. The **webhost-redirection https//%h%p 30**2 line is known as the relocation string and it reads the URL of the incoming HTTP connection and redirects to **https** and inserts the hostname **%h** and URL path **%p** that are read from the original HTTP URL. The **302** is the status code that is returned to the client. For example, if http://view-ext.ese.com comes in, the Cisco ACE reads **view-ext.ese.com** as the hostname (%h). There is no subordinate path in the string, thus %p is just the root URL. The Cisco ACE sends a 302 back to the client with the new URL of https://view-ext.ese.com:

```
rserver redirect VIEW_RDIR
  webhost-redirection https://%h%p 302
  inservice
!
serverfarm redirect RDIR_SERVERFARM
  rserver VIEW_RDIR
    inservice
!
class-map match-all VIEW_SS_RDIR
  2 match virtual-address 10.5.25.36 tcp eq www
!
policy-map type loadbalance http first-match VIEW_SS_RDIR
```

```
  class class-default
    serverfarm RDIR_SERVERFARM
!
policy-map multi-match VIEW-SLB-MULTI
  class VIEW_SS_RDIR
    loadbalance vip inservice
    loadbalance policy VIEW_SS_RDIR
```

A HTTP 302 redirect can be seen coming from the Cisco ACE to the View Client:

```
Hypertext Transfer Protocol
    HTTP/1.1 302 Found\r\n
      [Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n]
       Request Version: HTTP/1.1
       Response Code: 302
    Connection: close\r\n
   Location: https://view-ext.ese.com/broker/xml\r\n
```

View Portal

The VMware View Portal needs one additional item to be configured on the Cisco ACE for the View Portal to function properly. When using the View Portal, the user connects via HTTPS and authenticates. When authenticated to the View Portal, the second phase or tunnel phase begins, and this is where, by default, the issue exists. Because the SS is configured for SSL offload, it thinks that all connections coming to it are HTTP. Therefore, when it replies to connections, it replies via HTTP. This is fine except for when the SS sends an HTTP 302 Moved Temporarily message, which it does each time it tells a client to reconnect a second time to begin the RDP-in-HTTP tunnel process.

The following Wireshark capture shows the HTTP 302 Moved Temporarily from the Cisco ACE (on behalf of the SS) that has the HTTP-based redirect that actually causes the client to want to reconnect via HTTP (breaking the flow):

```
Source                Destination           Protocol ssl-id     Info
10.5.25.36            192.168.200.10        HTTP                HTTP/1.1 302 Moved
Temporarily

Internet Protocol, Src: 10.5.25.36 (10.5.25.36), Dst: 192.168.200.10 (192.168.200.10)
Transmission Control Protocol, Src Port: https (443), Dst Port: prolink (1678), Seq: 1104,
Ack: 3679, Len: 204
Secure Socket Layer
Hypertext Transfer Protocol
    HTTP/1.1 302 Moved Temporarily\r\n
    Location: http://view-ext.ese.com/index.jsp?action=launchTunnel\r\n
    Set-Cookie: JSESSIONID=94A7282F5E5E7A8DE19D6D0D51E61C13; Path=/\r\n
    Content-Length: 0\r\n
    \r\n
```

This incorrect redirection is easily solved by using an SSL URL rewrite configuration on the Cisco ACE:

```
action-list type modify http URLREWRITE
 ssl url rewrite location "view-ext\.ese\.com"
!
policy-map type loadbalance http first-match VIEW_SS
  class class-default
    action URLREWRITE
```

The following Wireshark capture shows the correct HTTP 302 Moved Temporarily string using the Cisco ACE SSL URL rewrite functionality:

```
Source                Destination           Protocol ssl-id     Info
10.5.25.36            192.168.200.10        HTTP                HTTP/1.1 302 Moved
Temporarily

Internet Protocol, Src: 10.5.25.36 (10.5.25.36), Dst: 192.168.200.10 (192.168.200.10)
```

```
Transmission Control Protocol, Src Port: https (443), Dst Port: sstsys-lm (1692), Seq:
710, Ack: 1334, Len: 205
Secure Socket Layer
Hypertext Transfer Protocol
    HTTP/1.1 302 Moved Temporarily\r\n
    Location: https://view-ext.ese.com/index.jsp?action=launchTunnel\r\n
    Set-Cookie: JSESSIONID=4A7F44A81F16BBFD65A0966B7BAB1F9D; Path=/\r\n
    Content-Length: 0\r\n
    \r\n
```

Redundancy/High Availability

To provide high availability and redundancy, the Cisco ACE appliance can be set up and configured in a redundant mode. A Cisco ACE can be configured in a typical active/backup redundancy mode or active/active (per context) redundancy mode. The following is a sample configuration for the Admin context:

```
! Configure FT interface
!
ft interface vlan 43
 ip address 10.5.43.1 255.255.255.0
 peer ip address 10.5.43.2 255.255.255.0
 no shutdown
!
! Configure FT peer
!
ft peer 1
 ft-interface vlan 43
 heartbeat interval 200
 heartbeat count 20
 ft-interface vlan 43
!
!  Create a fault tolerant group
!
ft group 1
 peer 1
 priority 120
 preempt
 associate-context admin
 inservice
!
ft group 2
  peer 1
  priority 120
  associate-context VIEW
  inservice
```

By assigning context(s) to an FT group, a network administrator can create multiple groups for multiple contexts in which the ACTIVE contexts can be distributed among the two Cisco ACE appliances. This setup provides active/active redundancy setup for load sharing and high availability.

Validation

This section describes a connection from a View Client to the View Agent VM via the Cisco ACE and SS.

Figure 14 shows the VMware View Client interface used for this connection. The connection server field has the name of *view-ext.ese.com*, which resolves in DNS to the VIP of the Cisco ACE (10.5.25.36).

Figure 14 VMware View Client GUI

After the user clicks **Connect**, the client performs a DNS lookup, if needed, to resolve the *view-ext.ese.com* name. The client then connects to the Cisco ACE VIP. The following **show conn** command output shows that there are two TCP connections. The first line is between the View Client (192.168.200.10) and the Cisco ACE VIP (10.5.25.36) on port 443 (HTTPS). The second line is between the View Security Server (10.5.25.20) and the Cisco ACE SNAT address (10.5.25.40) on port 80. When the ACE is terminating sessions, there should be two connections: in from the client and out to the server. This first connection is where the client asks for the broker (Connection Server) configuration for which the SS replies with the following:

```
DMZ-ACE1/VIEW# show conn

total current connections : 2

conn-id    np dir proto vlan source                destination           state
----------+--+---+-----+----+---------------------+---------------------+------+
92722      1  in  TCP   25   192.168.200.10:1815   10.5.25.36:443        ESTAB
92741      1  out TCP   25   10.5.25.20:80         10.5.25.40:2075       ESTAB
```

When the connection is established between the client and Cisco ACE, a sticky database entry is created based on the source IP address of the client. The **show sticky database** command shows that the client has a sticky database entry and the rserver (SS) that it is associated with is VIEW4-SEC1 (10.5.25.20). Again, this sticky entry is critical because VMware View needs to have both the first and second phase connections to be associated with the same SS:

```
DMZ-ACE1/VIEW# show sticky database
sticky group : SS_STICKY
type         : IP
timeout      : 1440          timeout-activeconns : FALSE
  sticky-entry          rserver-instance                 time-to-expire flags
  --------------------+--------------------------------+--------------+-------+
  3232286730            VIEW4-SEC1:80                    86382          -
```

Additional information can be found in the **show service-policy** command. There is a lot of information in this command, so only the relevant information is shown in the output.

```
DMZ-ACE1/VIEW# show service-policy VIEW-SLB-MULTI

Status     : ACTIVE
----------------------------------------
Interface: vlan 1 25
```

```
service-policy: VIEW-SLB-MULTI
  class: VIEW_SS
    ssl-proxy server: SSL-PROXY-VIEW
    nat:
      nat dynamic 1 vlan 25
      curr conns       : 1         , hit count        : 1
    loadbalance:
      L7 loadbalance policy: VIEW_SS
      VIP ICMP Reply       : ENABLED
      VIP State: INSERVICE
      Persistence Rebalance: ENABLED
      curr conns       : 1         , hit count        : 1
      dropped conns    : 0
```

Information about SSL can be found by using the **show stats crypto server** command. The following output has been highly summarized for the sake of clarity:

```
DMZ-ACE1/VIEW# show stats crypto server

+-----------------------------------------------+
+---- Crypto server termination statistics ----+
+-----------------------------------------------+
TLSv1 negotiated protocol:                      1
TLSv1 full handshakes:                          1
TLSv1 active connections:                       1
TLSv1 connections in data phase:                1

+-----------------------------------------------+
+------- Crypto server cipher statistics -------+
+-----------------------------------------------+
Cipher tlsv1_rsa_rc4_128_md5:                   1
```

A more detailed look at the flow process is shown in the following section. The connections are to the same VIP (10.5.25.36) as before and using the same rserver (SS) as before, based on the sticky database entry. The output shown below illustrates three connection pairs (only visible on the ACE for a brief time). The same commands referenced above can be used to check the status of the connections:

The same commands referenced above can be used to check the status of the connections:

- Connections 92762/92781 are the authentication connection pair (**username/password/domain**–<*do-submit-authentication*>).
- Connections 92782/92783 are the session configuration pair (<*get-tunnel-connection*/><*get-desktops*> and other parameters).
- Connections 92784/92785 are the actual session data flow: RDP-in-HTTPS.

Note Depending on the timing of the **show conn** command, some sessions may show with a state of "closed," or other connections used for View may open for different purposes.

The following output illustrates the basic setup of connections:

```
DMZ-ACE1/VIEW# show conn

total current connections : 6

conn-id    np dir proto vlan source               destination          state
----------+--+---+-----+----+--------------------+--------------------+------+
92762      1  in  TCP   25   192.168.200.10:1816   10.5.25.36:443       ESTAB
92781      1  out TCP   25   10.5.25.20:80         10.5.25.40:2083      ESTAB
92782      1  in  TCP   25   192.168.200.10:1817   10.5.25.36:443       ESTAB
92783      1  out TCP   25   10.5.25.20:80         10.5.25.40:2099      ESTAB
```

```
92784      1  in  TCP   25   192.168.200.10:1818   10.5.25.36:443        ESTAB
92785      1  out TCP   25   10.5.25.20:80         10.5.25.40:2106       ESTAB
```

The View Client has the same TCP port view as the Cisco ACE, with the only difference being that the client does not see the Cisco ACE-to-SS connection:

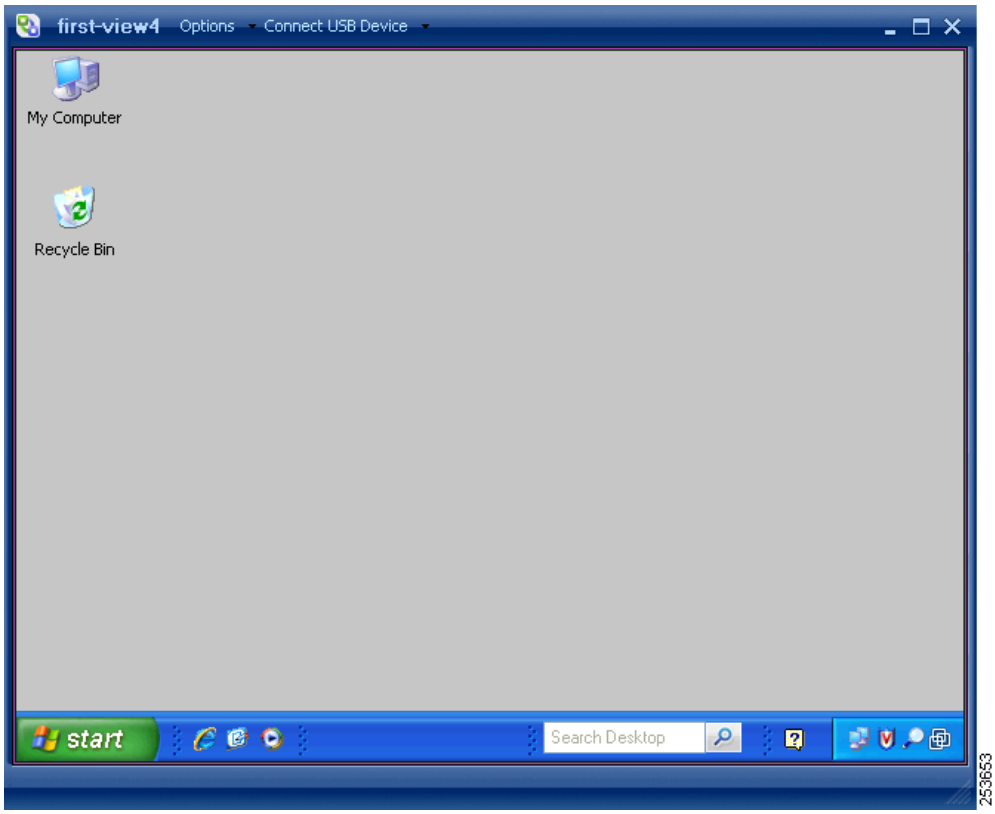
```
c:\>netstat

Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    XP-CLIENT1:1816        view-ext:https         ESTABLISHED
  TCP    XP-CLIENT1:1817        view-ext:https         ESTABLISHED
  TCP    XP-CLIENT1:1818        view-ext:https         ESTABLISHED
```

The SSL offload statistics reflect that a total of five connections have been made using only two transactions and that there are three active connections, which is accurate based on the **show conn** command from the previous output.

```
DMZ-ACE1/VIEW# show stats crypto server

+-----------------------------------------------+
+---- Crypto server termination statistics ----+
+-----------------------------------------------+
TLSv1 negotiated protocol:                      5
TLSv1 full handshakes:                          5
total transactions:                             2
TLSv1 active connections:                       3
TLSv1 connections in data phase:                3
```

Figure 15 shows that the View Client has a connection to the View Agent VM.

Figure 15 View Client Connection to View Agent VM



Cisco ACE Considerations for VMware View Connection Servers

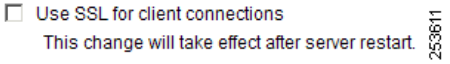
The steps to provide Layers 4 to 7 SLB for VMware View Connection Servers are identical to the way SLB is provided for VMware View Security Servers.

If SSL offload is going to be used for View CS, only two things need to be considered. The first consideration is based on the need or presence of the **locked.properties** file. The View CS does not need a **locked.properties** file to support SSL offload, but it does need the *External URL* field to be set in the View Administrator console on a per-CS basis. As was the case with the URL entry on the View SS, the External URL field must match the DNS entry for the Cisco ACE VIP serving the SSL sessions on behalf of the View CS, which also must match the SSL CSR *common name* located on the Cisco ACE. Figure 16 shows the External URL field in the View Administrator Console for a View CS.

Figure 16 View Administrator Console for View CS—External URL

The second consideration is based on the **use SSL for client connections** setting in the View Administrator Console. If SSL offload is going to be performed for the View CS, the checkbox for the SSL client connection option must be unchecked. Figure 17 shows the setting for the View CS SSL client connection requirement.

Figure 17 View Administrator Console for View CS—SSL Client Requirement



Various display protocols and deployment options are available when connecting View Clients to the View CS and View Agent VMs. With the View CS, the connection options include the following:

- RDP-in-HTTP or HTTPS (tunneled or proxy mode)—The same method used with the View SS that was previously discussed.
- RDP Direct Connect—The initial connection happens between the View Client and the View CS, but the actual RDP session happens between the View Client and the View Agent VM.
- PCoIP Direct Connect—The same as the RDP Direct Connect method except that the display protocol is using PCoIP instead of RDP.

As it relates to the Cisco ACE configuration, there is not much difference in the configuration to support any of the three deployment types.

For Cisco ASA or Cisco Firewall Services Module considerations for View CS, see Cisco ASA Configuration for VMware View Security Servers, page 30 and the VMware View documentation on port requirements for firewalls. The configuration is very similar for the View CS as compared to the View SS.

VMware View 4.0 Connection Server Configuration Summary

Other than the previously discussed considerations regarding SSL offload for the View CS, the installation and configuration of the View CS is straightforward. The VMware View documentation and setup routine makes the deployment of the View CS relatively pain-free.

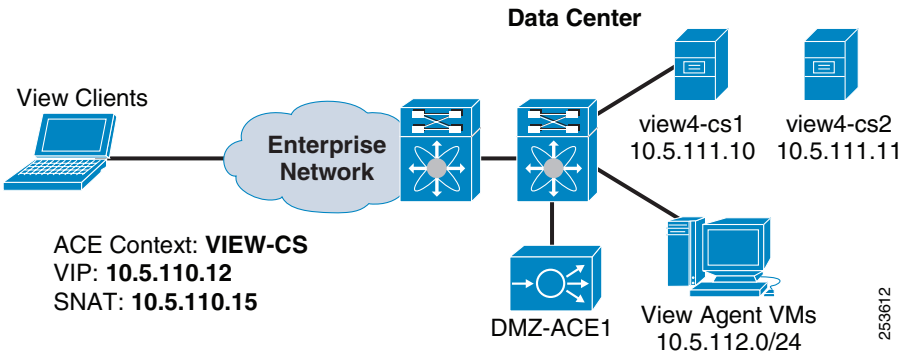
It is imperative that the reader study the VMware View documentation, especially the View Reference Architecture, to understand how many View Connection Servers need to be deployed to support the size of the customer deployment. This document uses the minimum number of View CS and View SS to illustrate SLB and SSL offload principles and to ensure a minimum level of availability for these View roles. The Cisco ACE with SSL offload and other features can significantly reduce the overall resource impact to the View CS server itself, but there are still guidelines that VMware has documented on what types of connection-to-CS ratios are recommended.

In this document, there are two View Connection Servers that are being load balanced by the Cisco ACE. One View CS is the standard installation and the second is the replica.

Note Because more details were provided in the View SS section regarding the actual Cisco ACE configuration for SSL offload, the following section dealing with configuration does not include the SSL commands.

Figure 18 shows the basic topology of the View CS along with the Cisco ACE.

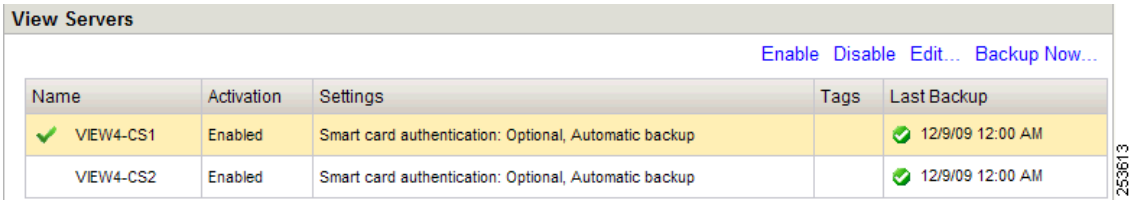
Figure 18 VMware View CS with Cisco ACE Topology



The Cisco ACE is deployed in one-arm mode, but bridged/transparent mode as well as routed mode are fully supported. View Client connection sources range from remote WAN/branch clients, campus clients, and remote VPN clients. As stated before regarding access for remote Internet clients, the View SS is not required for View Client connections coming from the Internet if an established remote access VPN solution has already been deployed. Cisco recommends that a remote access VPN be used instead of View SS because the VPN offering provides access to other services, not just View, and also reduces the overall View deployment complexity. Figure 18 has View Clients connecting over the enterprise network to the DC1-ACE1 VIP (10.5.110.12). DC1-ACE1 provides SLB services to the two View 4.0 Connection Servers (view4-cs1/view4-cs2). Once authenticated and the View configuration parameters are exchanged, the View Clients connect to the View Agent VM by either tunneled or "proxy" mode where the full RDP connection is tunneled in HTTP (only available for RDP); or connect directly to the View Agent VM itself, which bypasses the Cisco ACE for the data connection (available for RDP and PCoIP).

Figure 19 illustrates the View Administrator console display for the View CS (shown with tunneled mode settings).

Figure 19 VMware View Administrator Console—View CS



Cisco ACE Configuration for the View Connection Server

A detailed description of the connection process and command lines is not provided in this section because it is mostly redundant with the Cisco ACE section for the View SS.

As stated before, the View CS deployment in this section uses only Layers 4 to 7 SLB services and not SSL offload for the sake of brevity and clarity in the document. See the "SSL Offload" section on page 13 for details.

The following is a DC1-ACE1 configuration summary (VIEW-CS context only):

```
access-list EVERYONE line 10 extended permit icmp any any
access-list EVERYONE line 20 extended permit ip any any
```

```
probe http VIEW_CS_HTTP
  interval 5
  passdetect interval 5
  request method get url /favicon.ico
  expect status 200 200
  open 1

rserver host VIEW4-CS1
  ip address 10.5.111.10
  inservice
rserver host VIEW4-CS2
  ip address 10.5.111.11
  inservice

serverfarm host VIEW_CS_SLB
  predictor leastconns slowstart 300
  probe VIEW_CS_HTTP
  rserver VIEW4-CS1
    inservice
  rserver VIEW4-CS2
    inservice

sticky ip-netmask 255.255.255.255 address source CS_STICKY
  replicate sticky
  serverfarm VIEW_CS_SLB

class-map type management match-any MGMT
  201 match protocol snmp any
  202 match protocol http any
  203 match protocol xml-https any
  204 match protocol telnet any
  205 match protocol ssh any
  206 match protocol icmp any
  207 match protocol https any
class-map match-any VIEW_CS
  2 match virtual-address 10.5.110.12 tcp eq www

policy-map type management first-match MGMT
  class MGMT
    permit

policy-map type loadbalance first-match VIEW_CS-l7slb
  class class-default
    sticky-serverfarm CS_STICKY

policy-map multi-match VIEW-SLB-MULTI
  class VIEW_CS
    loadbalance vip inservice
    loadbalance policy VIEW_CS-l7slb
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 110

interface vlan 110
  ip address 10.5.110.9 255.255.255.0
  access-group input EVERYONE
  nat-pool 1 10.5.110.15 10.5.110.15 netmask 255.255.255.0 pat
  service-policy input MGMT
  service-policy input VIEW-SLB-MULTI
  no shutdown
```

Performance and Connection Mode Considerations

The Cisco ACE configuration does not impact the operation of using either RDP with tunneled/proxy mode or RDP/PCoIP with direct connect mode. If direct connect mode is used, the View Client does not attempt to reconnect to the Cisco ACE for the second connection and instead, establishes a connection directly to the assigned View Agent VM.

However, it is critical to understand the difference in performance impact between using tunneled/proxy mode and direct connect mode. When tunneled/proxy mode is used, *all* traffic between the View Client and View Agent VM traverses both the View CS as well as the Cisco ACE. The load on the intermediate devices can be substantial, based on the following:

- Size of the deployment
- Remote display protocol selection
- Supported applications and View policies (MMR, Adobe, USB redirection, multi-monitor, resolution, and so on)

It is imperative that testing and research be performed to understand the expected throughput and connection rates so that the proper Cisco ACE license is applied as well as the appropriate values for CPU, memory, and network are used for the View CS.

It is very common for VMware View deployments to use direct connect mode because it completely offloads the throughput and connection burden on intermediate devices such as load balancers and View Connection Servers for the actual remote display data path. Direct connect mode requires the network routing and security policies to permit connectivity between the View Client and the View Agent subnets.

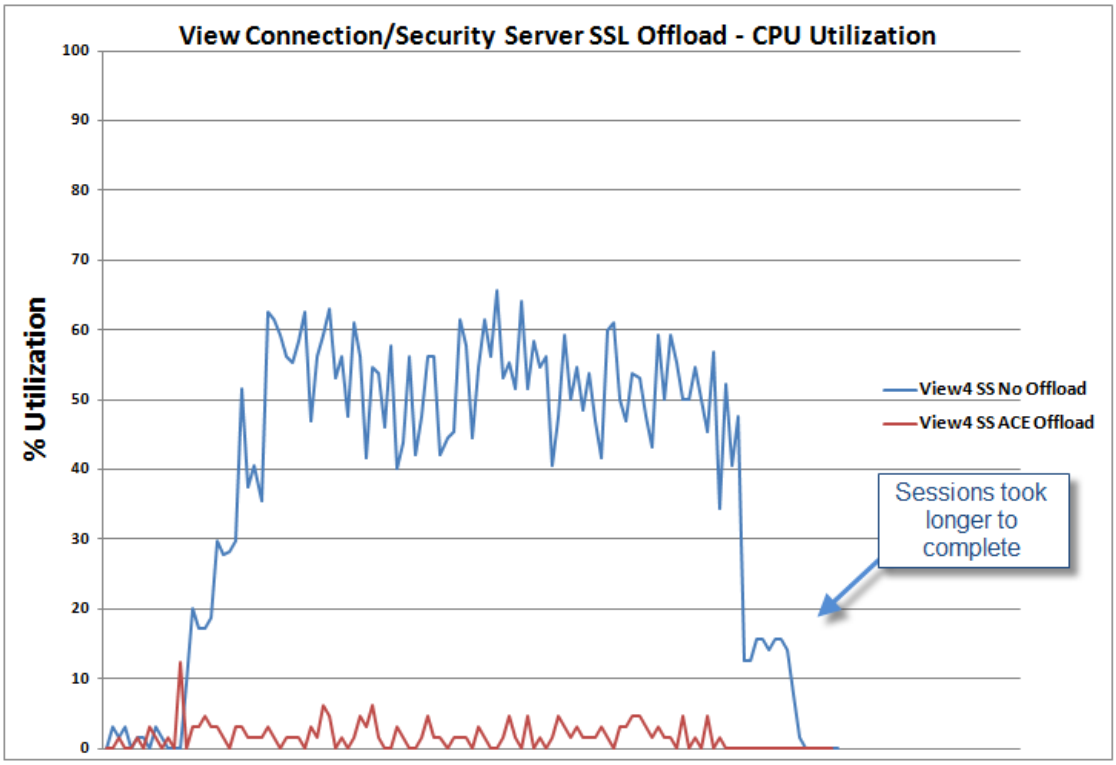
Cisco ACE SSL Offload Results

Note The following results are for reference only and are not to be taken as a baseline comparison for what can be expected in a production deployment. Session load, number of simultaneous sessions, levels of encryption, network configuration, and server hardware (CPU/memory/IO) cause performance numbers to vary wildly from deployment to deployment. The reader might experience radically different results (positive or negative) than the ones shown here. Readers should deploy a proof-of-concept in their own network to validate the true impact of Layers 4 to 7 SLB and SSL offload. The sole purpose of these results is to provide a reference validation for the View SS/CS roles when combined with Cisco ACE.

The previous subsections have shown the configurations and deployment considerations for Cisco ACE SSL offload for the View SS and CS roles. The following subsection shows a sample result that was reported during the prepost SSL offload of the View SS role.

Figure 20 shows a chart of the CPU utilization on one View SS with SSL termination directly on the server as compared with SSL termination (offload) directly on the Cisco ACE. The chart in Figure 20 illustrates the significant CPU utilization change when the CPU-intensive SSL processing is conducted on a scalable hardware platform such as the Cisco ACE instead of the server. By freeing up CPU cycles on the View SS server, more simultaneous sessions can be handled as well as faster time to completion for certain tasks.

Figure 20 CPU Utilization Comparison—Impact of SSL Offload



Deploying QoS for VMware View

Network QoS should be implemented for VMware View deployments, especially when sessions will traverse links that experience congestion. A common scenario with View that negatively impacts non-View traffic on the wire is when mission-critical or latency-sensitive applications such as IP telephony are deployed and QoS is not properly configured. If QoS is configured for voice traffic but nothing specific is configured for View traffic, the View traffic is most likely placed into "class-default" or some other low-priority class. During link congestion, this contention causes View traffic and the user experience to suffer greatly. Classifying, marking, queuing, and policing VMware View traffic helps protect View traffic as well as other competing applications.

When too much data needs to be transmitted across an interface, some of that data must be buffered. Depending on the type of buffer management enabled by default on a platform, some data may be dropped because of buffer exhaustion. Many platforms implement some sort of default mechanism such as First-In First-Out (FIFO) or similar mechanism to handle packet buffer issues. To prioritize and properly handle important traffic before it enters, while it is in and after the buffer, QoS should be deployed so that applications such as VMware View are treated as more important than a less critical application.

Note Cisco QoS has many highly advanced features and that are flexible. This section is not meant to be a primer or even a comprehensive configuration reference for Cisco QoS but more of a sample deployment that the reader may use to better protect VMware View traffic. This section is by no means the only way of configuring QoS for VMware View. For the sake of clarity and brevity, not all QoS configurations are shown for every platform used in this solution.

The QoS configurations for VMware View are relatively straightforward if the reader already understands how to work with the Cisco Modular QoS CLI (MQC) interface. The following configuration example is for the WAN/branch routers. Similar configurations need to be enabled on campus and data center switches to ensure that proper classification/marking, policing, and queuing are performed. Also, the DSCP values, ACLs, and bandwidth values for QoS vary depending on the number of classes used as well as the range of applications and their level of importance within the enterprise.

HQ WAN Router

ACLs are used to classify previously unmarked traffic; in this case, traffic matching RDP, RDP-in-HTTP, RDP-in-HTTPS, MMR, USB redirection, PCoIP control, and PCoIP data. Classification and marking should be done in the data center nearest to the application source and DSCP trust will allow these markings to be maintained throughout the network. It is also recommended to perform hardware-based classification (i.e., Catalyst/Nexus) versus software-based classification. Classification is being done on the HQ WAN router (DC1-WAN) only as a reference to show the full QoS configuration for View.

```
ip access-list extended MMR
 permit tcp any eq 9427 any
ip access-list extended PCOIP-TCP
 permit tcp any eq 50002 any
ip access-list extended PCOIP-UDP
 permit udp any eq 50002 any
ip access-list extended RDP
 permit tcp any eq 3389 any
ip access-list extended RDP-HTTP-VIEW
 permit tcp host 10.5.110.12 eq www any
ip access-list extended RDP-HTTPS-VIEW
 permit tcp host 10.5.110.13 eq 443 any
ip access-list extended USB
 permit tcp any eq 32111 any
```

Define QoS classes and tie the ACLs above to the classes:

```
class-map match-all TELEPRESENCE
 match  dscp cs4
class-map match-all BROADCAST-VIDEO
 match  dscp cs5
!
# Associate ACL with class-map for USB-Redirection
class-map match-any BULK-DATA
 match  dscp af11  af12  af13
 match access-group name USB
!
class-map match-all NETWORK-CONTROL
 match  dscp cs6
class-map match-all MULTIMEDIA-CONFERENCING
 match  dscp af41  af42  af43
class-map match-all OAM
 match  dscp cs2
!
# Associate ACL with class-map for RDP, HTTP, HTTPS and PCoIP
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match access-group name RDP
 match access-group name RDP-HTTPS-VIEW
 match access-group name RDP-HTTP-VIEW
 match access-group name PCOIP-UDP
 match access-group name PCOIP-TCP
!
class-map match-all VOICE
 match  dscp ef
class-map match-all SCAVENGER
```

```
 match  dscp cs1
class-map match-all CALL-SIGNALING
 match  dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match  dscp af21  af22  af23
!
# Associate ACL with class-map for MMR
class-map match-any MULTIMEDIA-STREAMING
 match  dscp af31  af32  af33
 match access-group name MMR
!
```

Define a service policy that is used to set the DSCP values for View (only those classes relevant to View are shown). Here, the HQ-LAN-EDGE-IN service policy is used as an input policy for traffic being sourced from the data center.

```
policy-map HQ-LAN-EDGE-IN
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class MULTIMEDIA-STREAMING
  set ip dscp af31
 class BULK-DATA
  set ip dscp af11
```

Define a service policy that is for egress interfaces (WAN-facing). The service policy WAN-EDGE is applied to the serial WAN interfaces connecting to the branch sites.

```
policy-map WAN-EDGE
 class VOICE
    priority percent 10
 class TELEPRESENCE
    bandwidth percent 15
    queue-limit 128 packets
 class NETWORK-CONTROL
    bandwidth percent 2
 class OAM
    bandwidth percent 1
 class CALL-SIGNALING
    bandwidth percent 2
 class BROADCAST-VIDEO
    bandwidth percent 5
 class MULTIMEDIA-CONFERENCING
    bandwidth percent 5
     random-detect dscp-based
 class MULTIMEDIA-STREAMING
    bandwidth percent 5
     random-detect dscp-based
 class TRANSACTIONAL-DATA
    bandwidth percent 25
     random-detect dscp-based
 class BULK-DATA
    bandwidth percent 4
     random-detect dscp-based
 class SCAVENGER
    bandwidth percent 1
 class class-default
    bandwidth percent 25
     random-detect
```

Apply the service policies to the appropriate interface(s).

```
interface GigabitEthernet0/0
 description DC1 Core
 service-policy input HQ-LAN-EDGE-IN
!
```

```
interface Serial0/0/0:0
 description To Branches
 max-reserved-bandwidth 100
 service-policy output WAN-EDGE
```

Branch Router

The following is the sample configuration for the branch router:

```
ip access-list extended MMR
 permit tcp any any eq 9427
ip access-list extended PCOIP-TCP
 permit tcp any any eq 50002
ip access-list extended PCOIP-UDP
 permit udp any any eq 50002
ip access-list extended RDP
 permit tcp any any eq 3389
ip access-list extended RDP-HTTP-VIEW
 permit tcp any host 10.5.110.12 eq www
ip access-list extended RDP-HTTPS-VIEW
 permit tcp any host 10.5.110.13 eq 443
ip access-list extended USB
 permit tcp any any eq 32111

class-map match-all TELEPRESENCE
 match  dscp cs4
class-map match-all BROADCAST-VIDEO
 match  dscp cs5
class-map match-any BULK-DATA
 match  dscp af11  af12  af13
 match access-group name USB
class-map match-all NETWORK-CONTROL
 match  dscp cs6
class-map match-all MULTIMEDIA-CONFERENCING
 match  dscp af41  af42  af43
class-map match-all OAM
 match  dscp cs2
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match access-group name RDP
 match access-group name RDP-HTTPS-VIEW
 match access-group name RDP-HTTP-VIEW
 match access-group name PCOIP-UDP
 match access-group name PCOIP-TCP
class-map match-all VOICE
 match  dscp ef
class-map match-all SCAVENGER
 match  dscp cs1
class-map match-all CALL-SIGNALING
 match  dscp cs3
class-map match-all TRANSACTIONAL-DATA
 match  dscp af21  af22  af23
class-map match-any MULTIMEDIA-STREAMING
 match  dscp af31  af32  af33
 match access-group name MMR
!
policy-map WAN-EDGE
 class VOICE
    priority percent 10
 class TELEPRESENCE
    bandwidth percent 15
    queue-limit 128 packets
 class NETWORK-CONTROL
    bandwidth percent 2
```

```
 class OAM
    bandwidth percent 1
 class CALL-SIGNALING
    bandwidth percent 2
 class BROADCAST-VIDEO
    bandwidth percent 5
 class MULTIMEDIA-CONFERENCING
    bandwidth percent 5
     random-detect dscp-based
 class MULTIMEDIA-STREAMING
    bandwidth percent 5
     random-detect dscp-based
 class TRANSACTIONAL-DATA
    bandwidth percent 25
     random-detect dscp-based
 class BULK-DATA
    bandwidth percent 4
     random-detect dscp-based
 class SCAVENGER
    bandwidth percent 1
 class class-default
    bandwidth percent 25
     random-detect
!
policy-map BRANCH-LAN-EDGE-IN
 class BRANCH-TRANSACTIONAL-DATA
  set ip dscp af21
 class MULTIMEDIA-STREAMING
  set ip dscp af31
 class BULK-DATA
  set ip dscp af11
!
interface GigabitEthernet0/1
 service-policy input BRANCH-LAN-EDGE-IN
!
interface Serial2/0:0
 max-reserved-bandwidth 100
 service-policy output WAN-EDGE
```

QoS policy statistics can be seen for View traffic. The following output shows the input policy where the View traffic is classified and marked with the appropriate DSCP value:

```
DC1-WAN#show policy-map interface

 GigabitEthernet0/0

  Service-policy input: HQ-LAN-EDGE-IN

    Class-map: BRANCH-TRANSACTIONAL-DATA (match-any)
      7588 packets, 2854459 bytes
      30 second offered rate 5000 bps, drop rate 0 bps
      Match: access-group name RDP
        1147 packets, 1061611 bytes
        30 second rate 0 bps
      Match: access-group name RDP-HTTPS-VIEW
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group name RDP-HTTP-VIEW
        29 packets, 12102 bytes
        30 second rate 0 bps
      Match: access-group name PCOIP-UDP
        5305 packets, 1445962 bytes
        30 second rate 4000 bps
      Match: access-group name PCOIP-TCP
```

```
      165 packets, 19140 bytes
      30 second rate 0 bps
    QoS Set
      dscp af21
        Packets marked 7588

  Class-map: MULTIMEDIA-STREAMING (match-any)
    3532 packets, 5249960 bytes
    30 second offered rate 9000 bps, drop rate 0 bps
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name MMR
      3532 packets, 5249960 bytes
      30 second rate 9000 bps
    QoS Set
      dscp af31
        Packets marked 3532

  Class-map: BULK-DATA (match-any)
    74 packets, 9306 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match:  dscp af11 (10) af12 (12) af13 (14)
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: access-group name USB
      74 packets, 9306 bytes
      30 second rate 0 bps
    QoS Set
      dscp af11
        Packets marked 74
```

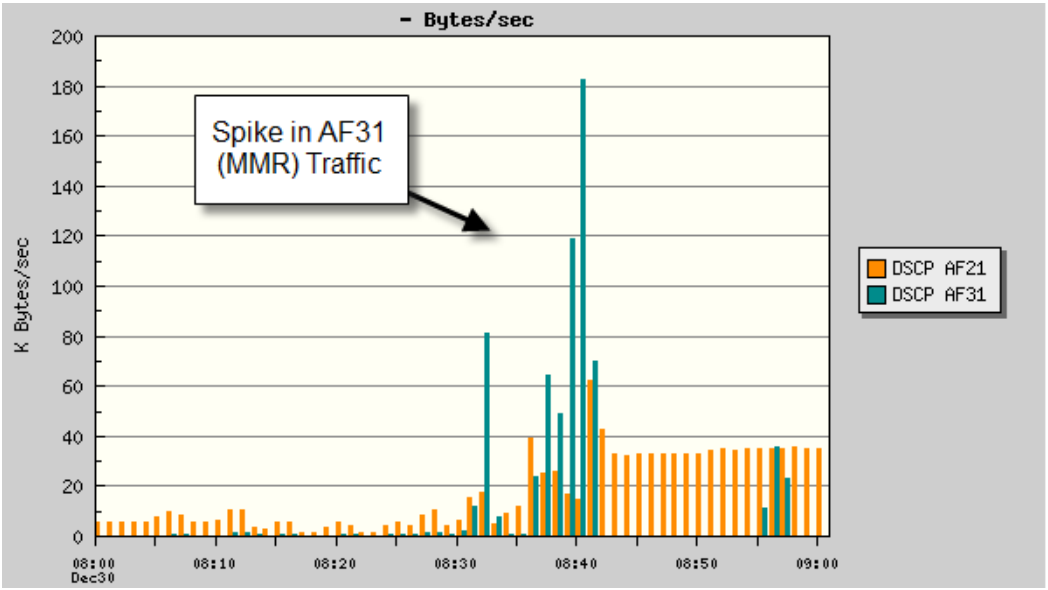
The following output shows the output policy where the View traffic is queued/policed based on the View policies defined. Listed below is the MULTIMEDIA-STREAMING (MMR) and TRANSACTIONAL-DATA (display protocols) information. An MMR and PCoIP session are active. Note that the "bandwidth 5%" for the MULTIMEDIA-STREAMING policy is well below the current output rate of 393000 bps. If higher priority traffic is active on this link and the link is congested, Cisco QoS begins dropping packets from this class:

```
Serial0/0/0:0

  Service-policy output: WAN-EDGE

    Class-map: MULTIMEDIA-STREAMING (match-any)
      5456 packets, 8052828 bytes
      30 second offered rate 393000 bps, drop rate 0 bps
      Match:  dscp af31 (26) af32 (28) af33 (30)
        5456 packets, 8052828 bytes
        30 second rate 393000 bps
      Match: access-group name MMR
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 5456/8052828
      bandwidth 5% (76 kbps)
      Exp-weight-constant: 9 (1/512)
      Mean queue depth: 25 packets
      dscp     Transmitted       Random drop      Tail drop          Minimum
Maximum     Mark
               pkts/bytes        pkts/bytes       pkts/bytes          thresh
thresh     prob
```

```
     af31       13333/19719645       12/18048          0/0                 32
40  1/10

    Class-map: TRANSACTIONAL-DATA (match-all)
      12898 packets, 3475078 bytes
      30 second offered rate 114000 bps, drop rate 0 bps
      Match:  dscp af21 (18) af22 (20) af23 (22)
      Queueing
      queue limit 64 packets
     (queue depth/total drops/no-buffer drops) 0/0/0
     (pkts output/bytes output) 12898/3475078
      bandwidth 25% (384 kbps)
      Exp-weight-constant: 9 (1/512)
      Mean queue depth: 0 packets
      dscp     Transmitted       Random drop      Tail drop          Minimum
Maximum     Mark
               pkts/bytes        pkts/bytes       pkts/bytes          thresh
thresh     prob

     af21       39109/13157348       0/0               0/0                 32
40  1/10
```

The Cisco NAM can be configured to perform real-time monitoring and reporting on DiffServ traffic. Figure 21 shows a report of both AF21 (Transactional-Data–display protocols) and AF31 (Multimedia-Streaming–MMR) traffic.

Figure 21 Cisco NAM Report—DiffServ AF21/AF31 Traffic



Configuring the Cisco WAAS Solution

This section describes Cisco WAAS solution considerations in the context of VMware View integration.

Cisco WAAS Implementation Overview

The Cisco WAAS solution can optimize VMware View traffic and, depending on the implementation model used with View, significantly reduce the overall WAN bandwidth requirement while improving the end-user experience for branch and remote users.

Cisco WAAS can optimize the following protocol/service types used in a VMware View environment:

- HTTP/HTTPS (when using RDP/HTTP tunneled (proxy) mode)
- Microsoft RDP
- USB redirection
- MMR
- PCoIP control channel (TCP) (Cisco WAAS does not optimize PCoIP UDP data traffic)

The Cisco WAAS solution uses symmetric caching to provide bandwidth compression and optimized delivery of application traffic. The WAAS service is hosted within the WAE (Wide Area Engine) or WAAS appliance. The WAE device is needed in the data center location as well as the potential branch site(s). Moreover, in order to provide centralized management of all the WAE devices, a WAAS central manager is required.

This solution uses a single branch site deployment which requires one Cisco WAE in the enterprise data center and the other at the branch site. The enterprise data center Cisco WAE is placed at the WAN edge connected to the WAN router. The third Cisco WAE is used for the Central Manager (CM).

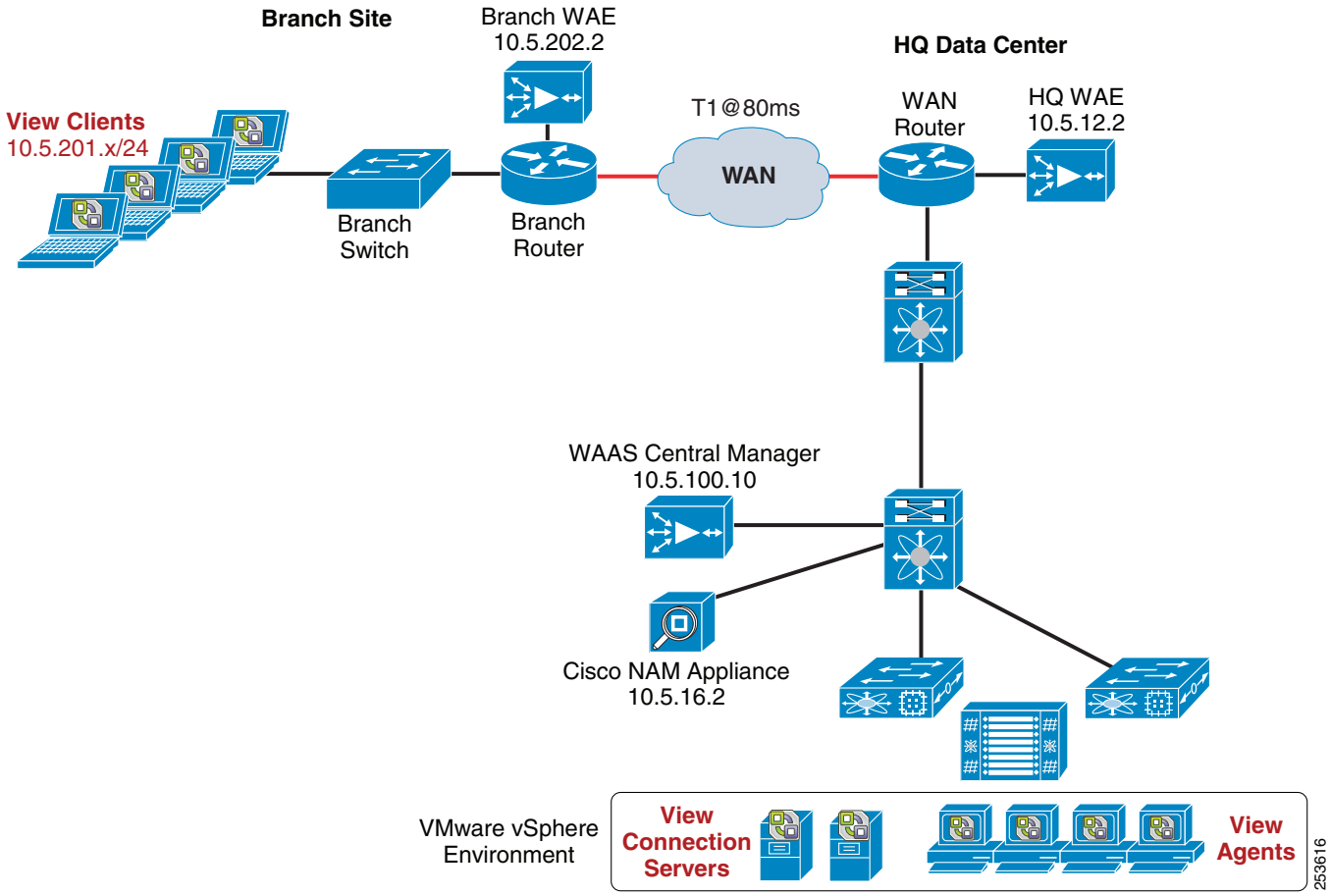
The following configuration information is meant to be a reference and is not a thorough guide for configuring everything needed for full integration of WAAS, WAAS Mobile, and the Cisco NAM. The reader is encouraged to consult the Cisco documentation at the following URLs:

- Cisco WAAS Configuration Guide—
http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v413/configuration/guide/cnfg.html
- Cisco WAAS Mobile Guides—
http://www.cisco.com/en/US/products/ps9523/products_installation_and_configuration_guides_list.html
- Cisco NAM User Guide—
http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.1/user/guide/userguide.html

Cisco WAAS Network Topology

Figure 22 provides a summary topology for the Cisco WAAS networking environment as described in this solution.

Figure 22 Cisco WAAS Network Topology



Cisco WAAS High Availability

Cisco WAAS deployments are transparent to the application. Web Cache Communications Protocol (WCCP) provides load balancing and high availability for multiple WAAS devices thereby providing a scalable WAN optimization for VMware View. When WCCP is not active, or if Cisco WAAS devices are not functioning, WCCP does not forward traffic to the Cisco WAEs, which results in non-optimal traffic flow. This is the worst case scenario; traffic flow continues, but is not optimized.

Device High Availability

The Cisco WAEs have many built-in high availability features. The disk subsystem is recommended to be configured with Redundant Array of Inexpensive Disks (RAID) 1 protection. RAID 1 is mandatory when two or more drives are installed in the Cisco WAE. With RAID 1, failure of the physical drive does not affect normal operations. Failed disks can be replaced during planned downtime. For network redundancy a pair of network interfaces can be grouped in a standby group configuration where one interface is active and the other serves as standby. A standby interface group guards against network interface failure on the Cisco WAE and switch. When connected to separate switches in active/standby mode, the standby interface protects the Cisco WAE from switch failure.

N+1 Availability

Cisco WAEs and the network provide additional high availability capabilities. Routers can be configured redundantly to provide Hot Standby Routing Protocol (HSRP) or Gateway Load Balancing Protocol (GLBP) services. Cisco WAEs can be configured in a *N+1* configuration to provide scalability and availability. This design calls for N number of Cisco WAEs for a specific workload, and then adds a standby Cisco WAE. Because the workload always distributes evenly among the Cisco WAEs, the standby Cisco WAE is used, reducing overall workload. In the event that a Cisco WAE fails, the rest of the Cisco WAEs can resume normal workload.

Cisco WAAS Configuration Task Lists

The following subsections describe the configurations used in this design.

Central Manager (CM)

The CM is the management component of Cisco WAAS. CM provides a GUI for configuring, monitoring, and managing multiple branch and data center Cisco WAEs. CM can scale to support thousands of Cisco WAE devices for large-scale deployments. The CM is necessary for making any configuration changes via the web interface.

Cisco WAEs must connect to the CM on the initial setup. The registration process adds the Cisco WAE to the CM and initializes the local Cisco WAE database.

Centralized reporting can be obtained from the CM. Detailed reports, such as total traffic reduction, application mix, and pass-through traffic, can be obtained from the CM GUI.

The following sample configuration process summarizes the steps needed to configure CM.

Note At least one Cisco WAE must be the CM. Adding backup CMs increases availability. CMs should be installed in the data center with other critical servers, not near the branch- or WAN-facing segments.

Step 1 Configure the device to be the CM. It is set to application-accelerator mode by default.

```
device mode central-manager
```

Step 2 Configure the CM IP address:

```
interface GigabitEthernet 1/0
 ip address 10.5.100.10 255.255.255.0
```

Step 3 Set up the default gateway:

```
ip default-gateway 10.5.100.1
```

Step 4 Set the primary interface. Cisco WAAS supports multiple network interface types, port channels, and standby interfaces. Cisco WAAS uses the primary interface for traffic interception and delivery. The primary interface must be defined.

```
primary-interface GigabitEthernet 1/0
```

Step 5 Define the Network Time Protocol (NTP) server. Traffic statistics are captured and forwarded to the CM. The time stamp on each packet must be accurate. All Cisco WAEs and routers should synchronize to the same NTP server.

```
ntp server 10.5.99.1
```

Step 6 Initialize the Configuration Management System (CMS) database. The CMS contains configuration rules and information. The CM is the repository of CMS data.

```
cms enable
```

Step 7 Log in to the CM web GUI.

Branch and HQ Cisco WAE

Table 6 compares the basic configurations in the branch and HQ Cisco WAEs. The configuration is highly similar to the CM detailed in the preceding section.

Table 6 Comparison of Branch and HQ Cisco WAE Configurations

HQ Cisco WAE	Branch Cisco WAE
device mode application-accelerator ! hostname dc1-wae ! clock timezone Pacific -8 0 ! ip domain-name ese.com ! primary-interface GigabitEthernet 2/0 ! interface GigabitEthernet 2/0 ip address 10.5.12.2 255.255.255.0 exit ! ip default-gateway 10.5.12.1 ! ip name-server 10.5.100.50 ! ntp server 10.5.99.1 ! wccp router-list 1 10.5.12.1 wccp tcp-promiscuous router-list-num 1 l2-redirect mask-assign wccp version 2 ! egress-method negotiated-return intercept-method wccp	device mode application-accelerator ! hostname branch1-wae ! clock timezone Pacific -8 0 ! ip domain-name ese.com ! primary-interface GigabitEthernet 2/0 ! interface GigabitEthernet 2/0 ip address 10.5.202.2 255.255.255.0 exit ! ip default-gateway 10.5.202.1 ! ip name-server 10.5.100.50 ! ntp server 10.5.99.1 ! wccp router-list 1 10.5.202.1 wccp tcp-promiscuous router-list-num 1 l2-redirect mask-assign wccp version 2 ! egress-method negotiated-return intercept-method wccp

Cisco WAE Deployment with Cisco NAM

The following configuration is used for sending flow information to the Cisco NAM (10.5.16.2) located in the data center aggregation layer:

```
flow monitor tcpstat-v1 host 10.5.16.2
flow monitor tcpstat-v1 enable
```

The Cisco NAM is configured to use the WAEs as data sources:

```
waas device 10.5.12.2
!
waas data-source
  index 15
  device 10.5.12.2
  segment CoreWan
  exit
!
waas data-source
  index 16
  device 10.5.12.2
  segment CoreLan
  exit
!
waas device 10.5.202.2
!
waas data-source
  index 17
  device 10.5.202.2
  segment EdgeLan
  exit
!
waas data-source
  index 18
  device 10.5.202.2
  segment EdgeWan
  exit
```

The WAAS data source information can be seen from the Cisco NAM via either CLI or the GUI console. The following is the CLI output from the NAM console:

```
root@nam2220.cisco.com# show waas device
Id:         3
Name:       dc1-wae (00:1a:64:f2:00:cb) Cisco WAAS 4.1.3a-b32 [OE512]<br> Last collection:
Mon Dec 21 12:27:51 2009
 (188 bytes)
Address:    10.5.12.2
State:      active
Export PTT: disabled

Id:         4
Name:       branch1-wae (00:14:5e:85:54:11) Cisco WAAS 4.1.3a-b32 [OE612]<br> Last
collection: Mon Dec 21 12:28:12 2009
 (188 bytes)
Address:    10.5.202.2
State:      active
Export PTT: disabled
```

Enabling WAAS for VMware View-Specific Optimization

TFO, DRE, and LZ-compression are enabled by default on many application policies on the Cisco WAE; however, only TFO is enabled by default for the remote desktop policy due to the fact that RDP is encrypted by default. Later in this document RDP compression and encryption will be disabled so that Cisco WAAS can fully optimize the flow. In addition to optimization for RDP and other protocols used with VMware view, it is important to identify common protocols with user-defined names so that statistics and reporting are easier to read.

Application Policy Definitions

Application policies include the classifier, application category, and action (optimization level or passthrough). In this design, certain application policies were either modified or created to have better visibility into the application behavior.

The "MS-Terminal-Services" policy is enabled by default in WAAS but uses only TFO optimization. Here the policy has been modified to provide full optimization.

It is not required to create the other three policies shown in Figure 23 because WAAS discovers these applications and optimizes them. However, it is useful to create specific policies with user-defined names so that in the reporting and connection statistics screens, these applications are easily recognized. In Figure 23**,** three new policies were built for MMR, USB redirection, and PCoIP control traffic. Nothing new or special is done for the HTTP flows used with VMware View.

Figure 23 WAAS Application Policy Definitions—VMware View

Application Policies

Classifier	Application	Action	Enabled
MS-Terminal-Services	Remote-Desktop	Optimize(DRE,LZ)	Enabled
Wyse-MMR	Streaming	Optimize(DRE,LZ)	Enabled
USB-Redirection	Remote-Desktop	Optimize(DRE,LZ)	Enabled
PCoIP-TCP	Remote-Desktop	Optimize(DRE,LZ)	Enabled

253617

Cisco WAAS for HTTPS Optimization

In addition to optimizing and reporting on HTTP, RDP, MMR, USB redirection, and other View traffic types, the Cisco WAAS can also optimize HTTPS flows. Depending on the needs of the branch View Clients or site security policies, it may be necessary to enable HTTPS for tunneled mode connections. The branch View Clients can connect to the View CS or Cisco ACE via HTTPS and Cisco WAAS optimizes those flows.

The reader must understand the Cisco ACE SSL configuration as well as the recommended steps to enable HTTPS optimization on the Cisco WAAS. Earlier in this document, details were provided on how to enable SSL offload on the View SS/CS roles. For instructions on how to enable HTTPS optimization, see the *Cisco WAAS SSL Application Optimizer Deployment Guide* at the following URL: http://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps6870/deployment_guide_c07-541981.html.

Figure 24 shows that the Cisco WAAS is configured with an SSL Accelerated Service named **View**. This service accelerates SSL connections between branch View Clients and the Cisco ACE SSL VIP (10.5.110.13) that is deployed to perform SLB and SSL offload of the View CS role. Note that a certificate has been imported from the Cisco ACE. The certificate common name (**view-int-vip.ese.com**) matches the DNS name of the Cisco ACE VIP as well as the View CS External URL name previously discussed.

Figure 24 Cisco WAAS SSL Accelerated Services

Preparing VMware View for Optimization

Depending on the method of deployment used with VMware View, additional steps may be required to ensure full optimization of the protocols used with View. If Microsoft RDP is the protocol of choice used between branch View Clients and the View Connection Server (proxy mode) or the View Agent (direct mode), it is important to configure the Microsoft Active Directory and View environment to allow Cisco WAAS to perform the compression and caching functions in addition to the standard TCP optimizations (TFO).

Microsoft RDP, by default, performs compression in software and also some level of encryption, which prevents the most optimal optimization the WAAS can perform on the traffic. The following section helps the reader configure the environment for the best possible optimization of Microsoft RDP using WAAS.

Note The following information is for reference only and assumes the reader knows or has access to expertise regarding the configuration of Microsoft Active Directory (AD) Group Policy Objects (GPO) and registry modification using “regedit”.

Two requirements must be met to allow for both compression of RDP sessions and for encryption of RDP sessions to be disabled/lowered. The first requirement is to disable RDP compression using either Microsoft AD GPO (for domain-joined clients) or manual policy modification per client (for non-domain-joined clients). This step is specifically for the View Client-side of the solution. The second requirement is to modify the RDP encryption settings on the View Agent VMs via registry modification.

Microsoft AD GPO Modification using VMware .adm Files

VMware provides a collection of GPO **.adm** files with the installation of the View Connection Server. These **.adm** files, located in the **C:\Program Files (x86)\VMware\VMware View\Server\Extras\GroupPolicyFiles** directory, can be imported into the Microsoft AD GPO environment.

The following files are included:

- **pcoip.adm**
- **vdm_agent.adm**
- **vdm_client.adm**
- **vdm_common.adm**
- **vdm_server.adm**

For the purposes of disabling compression for the View Clients, only the **vdm_client.adm** file needs to be imported into Microsoft AD GPO.

Most administrators will create a new GPO in the domain that applies only to the View user group that has been created and linked to the existing AD user environment.

Step 1 Copy the **vdm_client.adm** file to the **c:\Windows\Inf** directory on one of the Microsoft AD hosts.

Step 2 Open the Group Policy Editor (**gpedit.msc**).

Step 3 Under the User Configuration > Policies > Administrative Templates folder, right-click and select **Add/Remove Templates**.

Step 4 In the Add/Remove Templates screen, click **Add** and browse to the **c:\Windows\Inf** directory (or wherever the **.adm** file was copied). Click **Open** when the **.adm** file is selected.

Step 5 The **vdm_client.adm** file should be displayed in the Add/Remove Templates screen. Click **Close**.

Step 6 Expand the folder hierarchy: User Configuration > Policies > Administrative Templates > Classic Administrative Templates (ADM) > VMware View Client Configuration > RDP Settings.

Step 7 Double-click to edit the **Enable compression** properties window. Select **Disabled** and click **OK**.

Step 8 Close the Group Policy Editor console and allow for the policy to be distributed to the View Clients. You can use **gpupdate /force** to instigate synchronization of the GPO policy if needed.

Using Registry Modification to Lower RDP Encryption

Now that RDP compression has been handled, the RDP encryption settings need to be altered. These registry changes are executed on the View Agent VM. In the solution documented here, there are multiple View Agent VMs that have been cloned using the VMware Linked-Clone technology associated with View Composer. The registry changes occur on the parent VM from which the linked-clones source.

On the View Agent VM, edit the following registry keys:

- Set HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\MinEncryptionLevel to 1.
- Create HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\SecurityLayer as a DWORD value and set it to 0.

Validating the VMware View and Cisco WAAS Solution

This section briefly describes the testing setup for the VMware View 4.0 on the Cisco WAAS solution.

WAN Simulation

During this testing, a WAN delay generator was deployed to simulate common WAN latency and loss. The results shown in this publication are based on a WAN configuration of a single T1 link (1.5 Mbps) and a WAN delay of 80 msec.

Test Procedure

A combination of scripts was used to launch VMware View sessions into the VMware View 4.0 environment. When logged in, each user session launched one of several AutoIT scripts inside the View session to perform various application tasks. Some applications such as Microsoft Word and Excel varied typing speed, wait times, and use random combinations of text. The testing of VMware View used a suite of applications that mimics the common applications used in many knowledge worker use cases.

The following applications were used:

- *Microsoft Outlook 2007*—Open, minimize, maximize and close Outlook as well as send messages
- *Microsoft Word 2007*—Open, minimize, close, write random words/numbers, save modifications.
- *Microsoft PowerPoint 2007*—Open, minimize, close, conduct a slide show presentation.
- *Microsoft Excel 2007*—Open, minimize, close, write random numbers, insert and delete columns/rows, copy and paste formulas, save modifications

- *Internet Explorer 8*—Open, minimize, close, browse pages.
- *Adobe Acrobat 9*—Open, minimize, close, browse pages in PDF document

Validation

Note The following results are for reference only and are not to be taken as a baseline comparison for what can be expected in a production deployment. RDP sessions and the bandwidth, response times, and transaction times vary significantly from session to session based on a number of factors that include bandwidth, network and application delay, length of session, applications and activity in the session, features enabled in the RDP session (font smoothing, audio redirection, and so on), and the levels of compression and encryption used. The reader might experience substantively different results (positive or negative) to those shown here. Readers should deploy a proof-of-concept in their own network to validate the true impact that any WAN optimization solution might provide. The sole purpose of these results is to provide a reference validation for the VMware View roles when combined with the Cisco WAAS product in the test environment shown.

Figure 25 illustrates three View sessions using RDP-over-HTTP (proxy mode). The "% of Comp" increases over the life of the flow as redundant objects are cached and compressed.

Figure 25 HTTP Sessions on WAAS

Source IP:Port	Dest IP:Port	Peer Id	Applied Policy	Open Duration	Org Bytes	Opt Bytes	% Comp	Classifier Name
10.5.201.210:2663	10.5.111.10:80	DCAAL-DC1-WAE512		0:8:15	9.427 MB	2.5444 MB	73%	HTTP
10.5.201.225:2143	10.5.111.10:80	DCAAL-DC1-WAE512		0:7:9	6.4136 MB	1.2905 MB	80%	HTTP
10.5.203.5:2241	10.5.111.10:80	DCAAL-DC1-WAE512		0:0:43	738.2715 KB	148.2871 KB	80%	HTTP

253619

Figure 26 shows two View sessions using RDP direct mode with USB redirection and MMR enabled. The focus of this test was to optimize MMR. The byte count gives some indication of where the bulk of the traffic is coming from flow-wise. The first connection (source 10.5.201.210) has a slightly lower "% Comp" value because it is helping to seed the DRE cache and compression capabilities of the WAE. It is very common for the very first MMR flow to show "-" in the "% Comp" field when an MMR flow first begins because it needs to warm the cache. In this case, both View sessions are hitting the MMR media for the second time (warm cache). While impossible to show in text, the quality of the video and audio were substantially improved over running the media natively across the WAN via RDP or PCoIP with or without MMR enabled.

Figure 26 RDP Direct Sessions with USB-Redirection on WAAS

Source IP:Port	Dest IP:Port	Peer Id	Applied Policy	Open Duration	Org Bytes	Opt Bytes	% Comp	Classifier Name
10.5.201.210:1199	10.5.112.14:3389	DCAAL-DC1-WAE512		0:3:41	1.4938 MB	228.3711 KB	85%	MS-Terminal-Services
10.5.201.210:1200	10.5.112.14:32111	DCAAL-DC1-WAE512		0:3:39	6.3232 KB	3.1504 KB	50%	USB-Redirection
10.5.201.225:1213	10.5.112.13:3389	DCAAL-DC1-WAE512		0:2:53	1.2198 MB	157.0684 KB	87%	MS-Terminal-Services
10.5.201.225:1214	10.5.112.13:32111	DCAAL-DC1-WAE512		0:2:52	6.3076 KB	3.0059 KB	52%	USB-Redirection
10.5.201.210:1201	10.5.112.14:9427	DCAAL-DC1-WAE512		0:2:32	17.1452 MB	5.2307 MB	69%	Wyse-MMR
10.5.201.225:1215	10.5.112.13:9427	DCAAL-DC1-WAE512		0:1:40	15.9979 MB	3.6475 MB	77%	Wyse-MMR

253620

Figure 27 shows a single View session that has a USB flash drive attached to the View Client computer. A local Microsoft Excel 2007 file was opened on the View Agent VM, edited, and then saved to the USB-redirected flash drive over the WAN connection. The WAAS solution optimized the USB redirection flow by 94 percent.

Figure 27 RDP Direct Sessions with MMR on WAAS

	Source IP:Port	Dest IP:Port	Peer Id	Applied Policy	Open Duration	Org Bytes	Opt Bytes	% Comp	Classifier Name
🔍	10.5.203.5:1274	10.5.112.22:3389	DCAAL-DC1-WAE512		0:4:51	1.1976 MB	321.5859 KB	74%	MS-Terminal-Services
🔍	10.5.203.5:1277	10.5.112.22:32111	DCAAL-DC1-WAE512		0:4:49	8.5416 MB	552.6611 KB	94%	USB-Redirection

253621

Figure 28 shows the Cisco WAAS connection status screen for an active HTTPS session between the branch View Client and the Cisco ACE (10.5.110.13), which is performing SSL offload for the View CS. Notice the SSL Acceleration icon in the "Applied Policy" column as well as the "HTTPS" label in the "Classifier Name" column:

Figure 28 WAAS Connection Status—HTTPS Acceleration for View

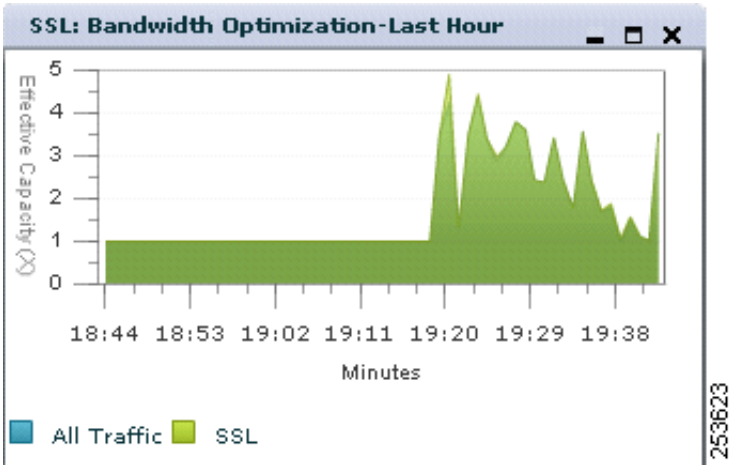
	Source IP:Port	Dest IP:Port	Peer Id	Applied Policy	Open	% Comp	Classifier Name
🔍	10.5.201.210:3990	10.5.110.13:443	DCAAL-DC1-WAE512		0:0:34	80%	HTTPS

SSL Acceleration Applied

253622

Figure 29 shows the Cisco WAAS optimization chart for SSL over the last hour:

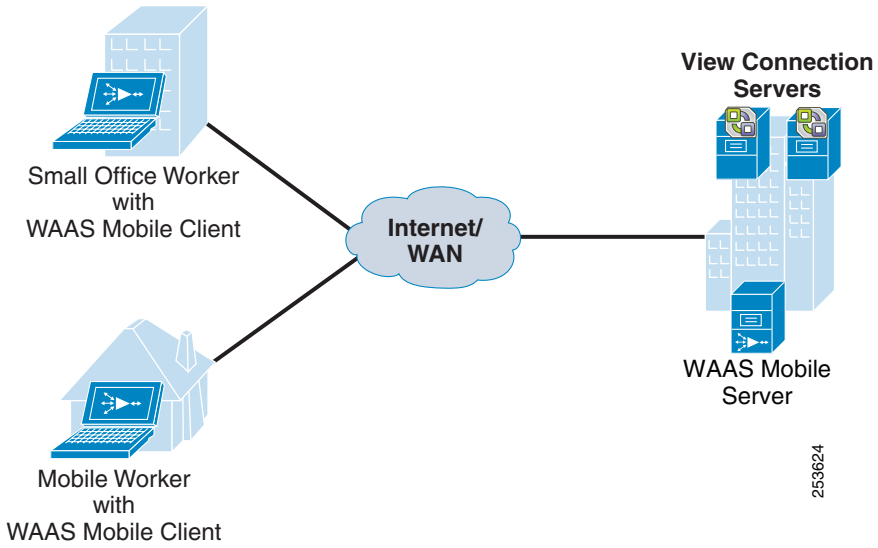
Figure 29 Cisco WAAS SSL BW Optimization—Last Hour



VMware View + Cisco WAAS Mobile

In addition to the Cisco WAAS solution using Cisco WAE appliances, the Cisco WAAS Mobile solution was used to validate remote workers using VMware View. Figure 30 shows the high-level topology used during the testing of the Cisco WAAS Mobile solution with VMware View.

Figure 30 Cisco WAAS Mobile with VMware View



Cisco WAAS Mobile is easy to configure and deploy. The primary configuration component for successfully deploying Cisco WAAS Mobile for VMware View Clients is to ensure that the "Proxied Process List" (located on the WAAS Mobile Server Client Configuration screen) contains the View Client process (*wswc.exe*). This proxied process list is the trigger point for the WAAS Mobile Client software running on the View Client to optimize traffic sourced for that process.

Figure 31 shows the Proxied Process List from the WAAS Mobile Administrator Console.

Figure 31 Cisco WAAS Mobile Proxied Process List—View Client Process

Select	Process Name	Min Version	Max Version	Command Line	Acceleration Type	Application Name	Auto Reset Connection
☐	wswc.exe	*	*	*	1	View4 Client	

253625

Testing can begin after the WAAS Mobile Server and Client configurations are completed and the WAAS Mobile Client application has been installed on the View Client PC.

Figure 32 illustrates the amount of data transferred to the remote View Client running an RDP direct session. This graph shows the amount of data transferred from the View Agent located in the data center to the remote View Client located on the Internet. The *Native* bar shows the amount of data transferred without the Cisco WAAS Mobile Client being used. The *WAAS Mobile 1st Session* shows the RDP session being optimized by the Cisco WAAS Mobile solution for the first time. There is a significant drop-off in data transferred over the network because of the optimization of the RDP data by the Cisco WAAS Mobile Client. The second session re-ran the test again. *Cisco WAAS Mobile 2nd Session* illustrates that the client can leverage data that is still in the local delta cache located on the client instead of downloading all the data again over the Internet connection.

Figure 32 Cisco WAAS Mobile Comparison Chart—Data Transferred

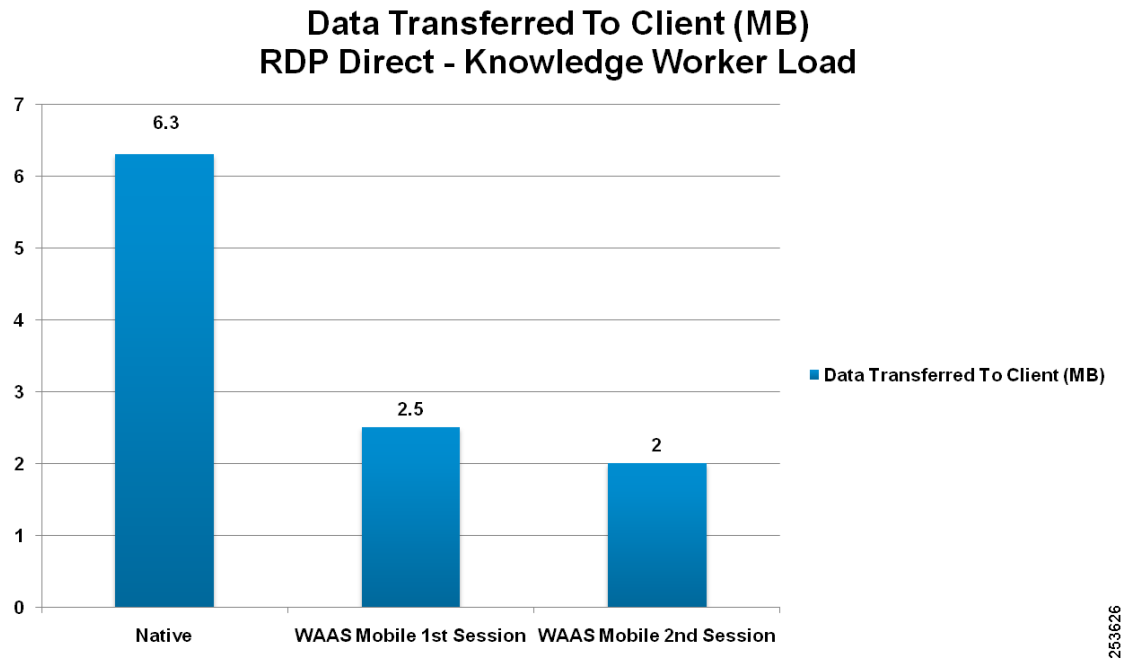


Figure 33 shows the amount of data transferred to the remote View Client from the View Agent via USB redirection. This graph shows the amount of data transferred via USB redirection when the View Agent copies an Excel spreadsheet file to the redirected USB flash drive that is locally connected to the PC running the View Client. The *Native* bar shows the amount of data transferred without the Cisco WAAS Mobile Client being used. The *WAAS Mobile 1st Copy* shows the USB redirection session being optimized by the Cisco WAAS Mobile solution for the first time. Again, there is a drop-off in data transferred over the network because of the optimization of the USB data by the Cisco WAAS Mobile Client. The file was edited and re-saved to the USB flash drive on the last session. *WAAS Mobile Re-Copy Post Edit* shows that the client can leverage data that is still in the local delta cache located on the client. Similar results were observed when the file was uploaded from the View Client to the View Agent. Cisco WAAS Mobile optimizes traffic in both directions.

Figure 33 Cisco WAAS Mobile Comparison Chart —Data Transferred USB Redirection

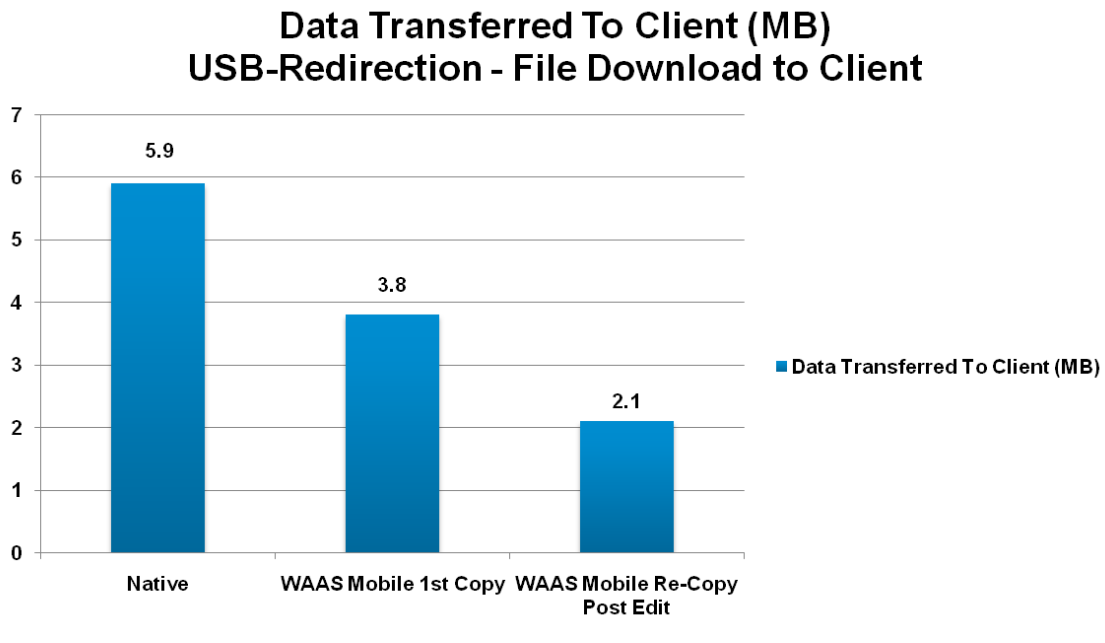


Figure 34 shows the time savings for a file copy over USB redirection when Cisco WAAS Mobile is used.

Figure 34 Cisco WAAS Mobile Comparison Chart—Time to Copy Savings

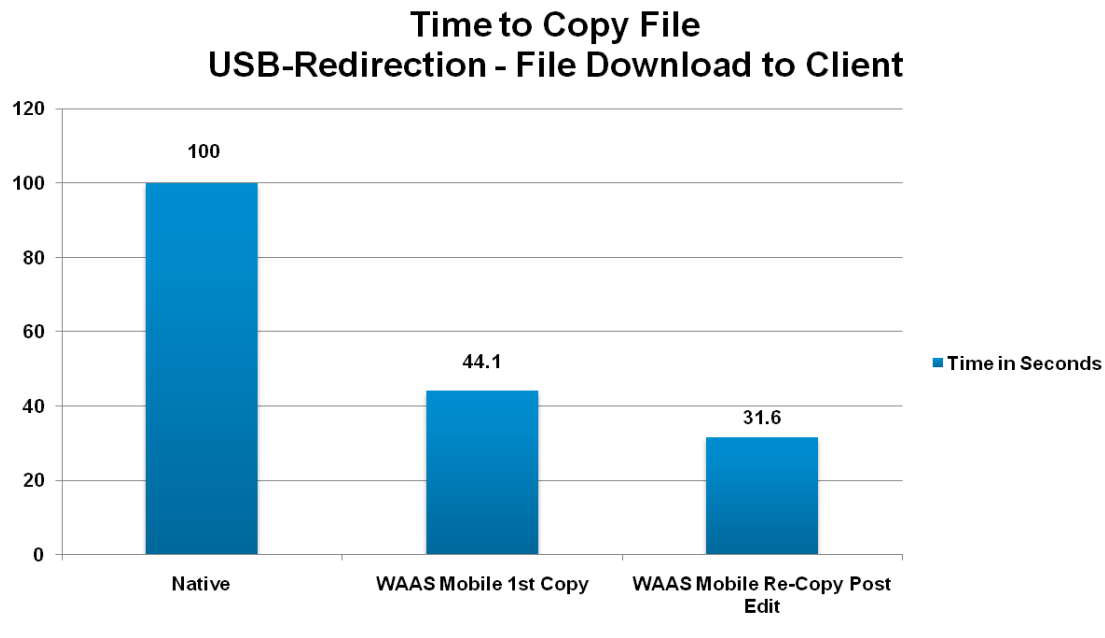
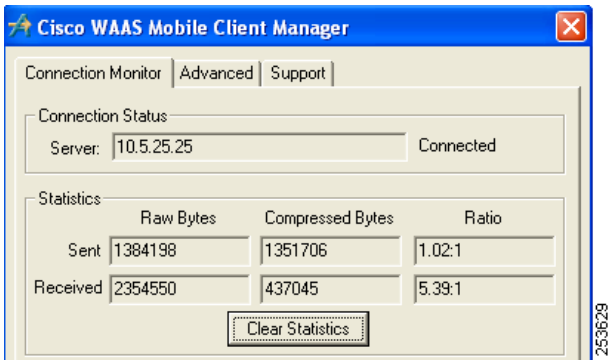


Figure 35 shows the Cisco WAAS Mobile Client. The *Ratio* shows 5.39:1 for the received data during a test run.

Figure 35 Cisco WAAS Mobile Client Statistics



Conclusion

VMware View 4.0, along with the Cisco solution discussed in this publication, provides a scalable, available, and feature-rich user-experience for VDI. The Cisco ASA offers perimeter protection for VMware View. Cisco provides server load balancing and SSL offload through the Cisco ACE for VMware View roles such as the View Connection Server and Security Server. WAN optimization for protocols used by VMware View is provided by Cisco WAAS and Cisco WAAS Mobile. The Cisco Nexus 1000V offers centralized configuration, management, policy control, and security to VMware View components such as View Agents and Connection Servers as well as other virtual machines. The capabilities presented in this document demonstrate that the Cisco solution for VMware View 4.0 offers improved security, lower bandwidth utilization, optimal server utilization, and increased availability—all of which combine to yield a more streamlined user-experience and increased productivity.

Related Documents

- Cisco Connection Online–Data Center—http://www.cisco.com/go/dc
- Cisco Design Zone—http://www.cisco.com/go/designzone
- Cisco ACE 4700 Series ACE Configuration Guides—http://www.cisco.com/en/US/products/ps7027/products_installation_and_configuration_guides_list.html
- Cisco WAAS Software Configuration Guides—http://www.cisco.com/en/US/products/ps6870/products_installation_and_configuration_guides_list.html
- Cisco WAAS Mobile Configuration Guides—http://www.cisco.com/en/US/products/ps9523/products_installation_and_configuration_guides_list.html
- Cisco ASA 5500 Configuration Guides—http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html
- Cisco Nexus 1000V Switch Configuration Guides—http://www.cisco.com/en/US/products/ps9902/products_installation_and_configuration_guides_list.html

- Cisco Enterprise Medianet QoS Solution Reference Network Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html
- Cisco Medianet Campus QoS Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html
- Cisco Branch QoS for TelePresence (Updated QoS recommendations used in this paper)—http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/tpqosbranch.html
- VMware View—http://www.vmware.com/products/view/
- VMware View Documentation—http://www.vmware.com/support/pubs/view_pubs.html