Integrating Oracle E-Business Suite 11i in the Cisco Data Center

This document provides network design best practices to enhance an Oracle E-Business Suite 11i application environment. It introduces key concepts and options regarding the application deployment and detailed designs strategies available to a data center leveraging Cisco's application and networking technologies.

Introduction

Ever-increasing customer demands, volatile market forces, and global competition compel today's enterprise to deliver greater goods and services to customers at a lower cost. The Oracle E-Business Suite is an extensive set of business applications developed to assist enterprises in addressing these challenges. The E-Business application framework is a flexible environment designed to protect, extend, and evolve business processes.

Today's data center is an intricate system of computing power and storage resources that support enterprise business applications. Data centers are not simply a facility, but a competitive edge that is strategic to achieving the real business objectives that these applications address. Therefore, the physical and logical design of the data center network must provide a flexible, secure, and highly available environment to optimize these critical business applications and assist the enterprise in achieving its goals.

Scope

The Cisco Data Center Architecture is a proven multi-layer approach that delivers a highly-available and robust network infrastructure with integrated application services. This document describes the deployment of the Oracle E-Business Suite in a Cisco Data Center design, employing integrated load balancing and security services.

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

Application Architecture

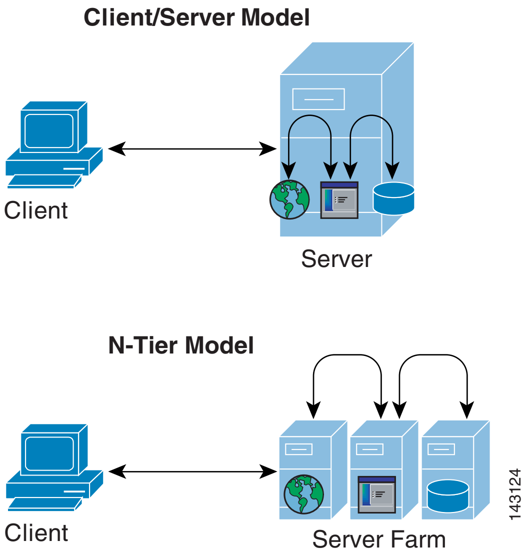
This section describes the application architecture of the Oracle E-Business Suite 11i.

Architecture Overview

The data center is a repository for enterprise software applications that are continuously changing to meet business requirements and to accommodate the latest technological advances and methods. Consequently, the logical and physical structure of the data center server farm and of the network infrastructure hosting these software applications is also continuously changing.

The server farm has evolved from the classic client/server model to an N-tier approach, where the "N" implies any number, such as 2-tier, or 4-tier; basically, any number of distinct tiers used in the architecture. The N-tier model logically or physically separates the enterprise application by creating functional areas. These areas are generally defined as the web front-end, the application business logic, and the database tiers. Figure 1 illustrates the progression of the enterprise application from the client/server to N-tier paradigm.

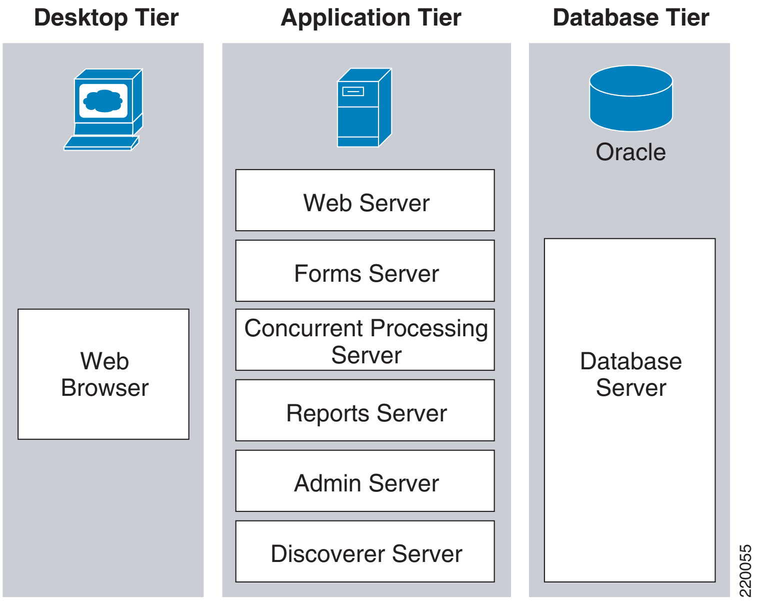
Figure 1 Client/Server and N-Tier Model



The N-tier model provides a more scalable and manageable enterprise application environment because it creates distinct serviceable areas in the software application. The application is distributed and becomes more resilient as single points of failure are removed from the design.

Oracle's Application Architecture uses the N-tier model by distributing application services across nodes in the server farm. The Oracle Application Architecture, as shown in Figure 2, uses the logical separation of tiers as desktop, application, and database. It is important to remember that each tier can consist of one or more physical hosts to provide the enterprise with the required performance or application availability.

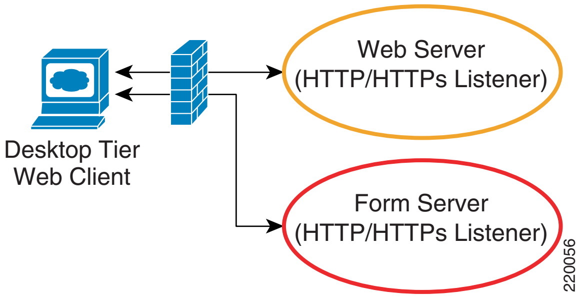
Figure 2 Oracle Applications Architecture



Desktop Tier

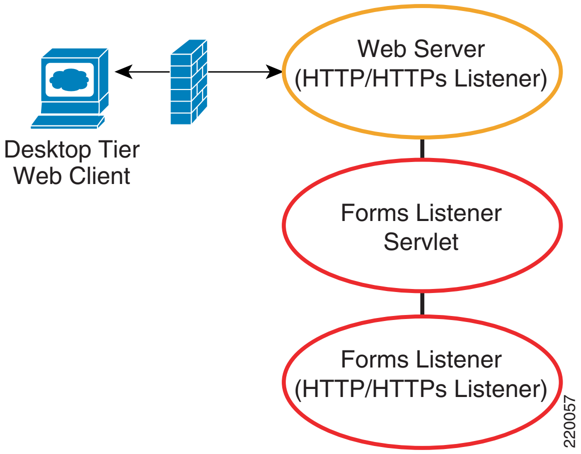
The desktop tier, traditionally called the presentation layer, consists of the client user interface, namely a web browser. The browser connects to the application tier via HTTP or HTTPS to the web server or the forms server. Historically, the forms server required the use of a client-side applet, Oracle JInitiator, which runs as an Active X or plug-in on the client's browser using a direct socket connection to the forms server. This direct-connect environment requires the client to access the forms server directly. This obviously exposes an enterprise to potential security risks when connectivity is allowed beyond the confines of the corporate LAN or WAN by requiring “holes” in firewalls. Figure 3 depicts the impact of a direct socket connection on the firewall and the security of the enterprise.

Figure 3 Traditional Desktop to Form Server Connections



In 2002, Oracle E-Business Suite offered a more “Internet friendly” forms server application by allowing a Java forms listener servlet to intercept forms server requests via the web listener. The forms listener servlet allows a single HTTP or HTTPS connection between the client, desktop tier, and the application tier. Figure 4 illustrates the more secure forms listener servlet deployment model, which can also take advantage of standard SSL offload and load balancing approaches.

Figure 4 Forms Listener Servlet Architecture



Note The forms listener servlet deployment model is common in today's enterprise data centers. The remainder of this document assumes the use of this forms strategy.

Application Tier

The application tier of the Oracle E-Business Suite provides administrative services and business logic, allowing end users at the desktop tier to make use of the information found at the database tier. Figure 2 shows the primary servers residing in this layer:

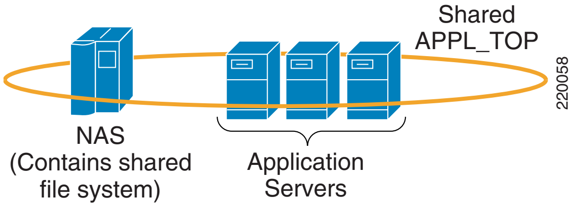
- Web server
- Forms server
- Concurrent processing server
- Admin server
- Reports server
- Discoverer server

Each of the application servers provides business process logic or management services to the Oracle E-Business Suite-enabled enterprise. The desktop tier communicates with the application tier via the web server listener (see Figure 4).

The application tier is commonly referred to as the APPL_TOP. The APPL_TOP is a file system that can reside on a single physical node or span multiple nodes in a “shared” multi-node application tier deployment. A shared APPL_TOP resides on a common disk mounted by each node in the 11i installation. A shared APPL_TOP allows any of the nodes to invoke the six primary server functions, such as the web server and forms server. The primary advantage to a shared application tier deployment is the ability to patch and or modify a single file system in a multi-node deployment, propagating those changes to all nodes simultaneously.

In addition, the use of a single file system requires the backup of only a single file system in despite the use of multiple nodes. Figure 5 depicts three server nodes sharing the application file system via NFS. The shared mount point in this case is a storage device located in the network.

Figure 5 Shared Application File System



Note Windows systems do not support a shared application tier in an Oracle 11i environment. For more information on shared application tier file systems, refer to Oracle Metalink Document 243880.1.

Database Tier

A database is a structured collection of data. This complex construct consists of tables, indexes, and stored procedures; each an important element to organize and access the data. Oracle provides a database management system (DBMS) or relational DBMS (RDBMS) to interface with the data collected by the application tier. The database tier does not directly communicate with the desktop tier; instead, the database relies on the application tier as an intermediary. To provide increased performance, scalability and availability Oracle offers Real Application Clusters (RAC), which allow multiple nodes to support a single database instance.

Note For more information on Oracle applications refer to "Oracle Applications Concepts Release 11i" part number B19295-02 at www.oracle.com.

Network Architecture

The data center infrastructure architecture must provide a highly available, scalable, and secure application environment. This section is a synopsis of the Cisco Data Center Network Architecture and describes the basics of this design. It includes the following topics:

- Data center network components
- Design goals

Note For more information on Cisco Systems' best practices and recommended data center designs, refer to the following URL:
http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html.

Data Center Network Components

The devices in the data center infrastructure can be divided into the front-end network and the back-end network, depending on their role:

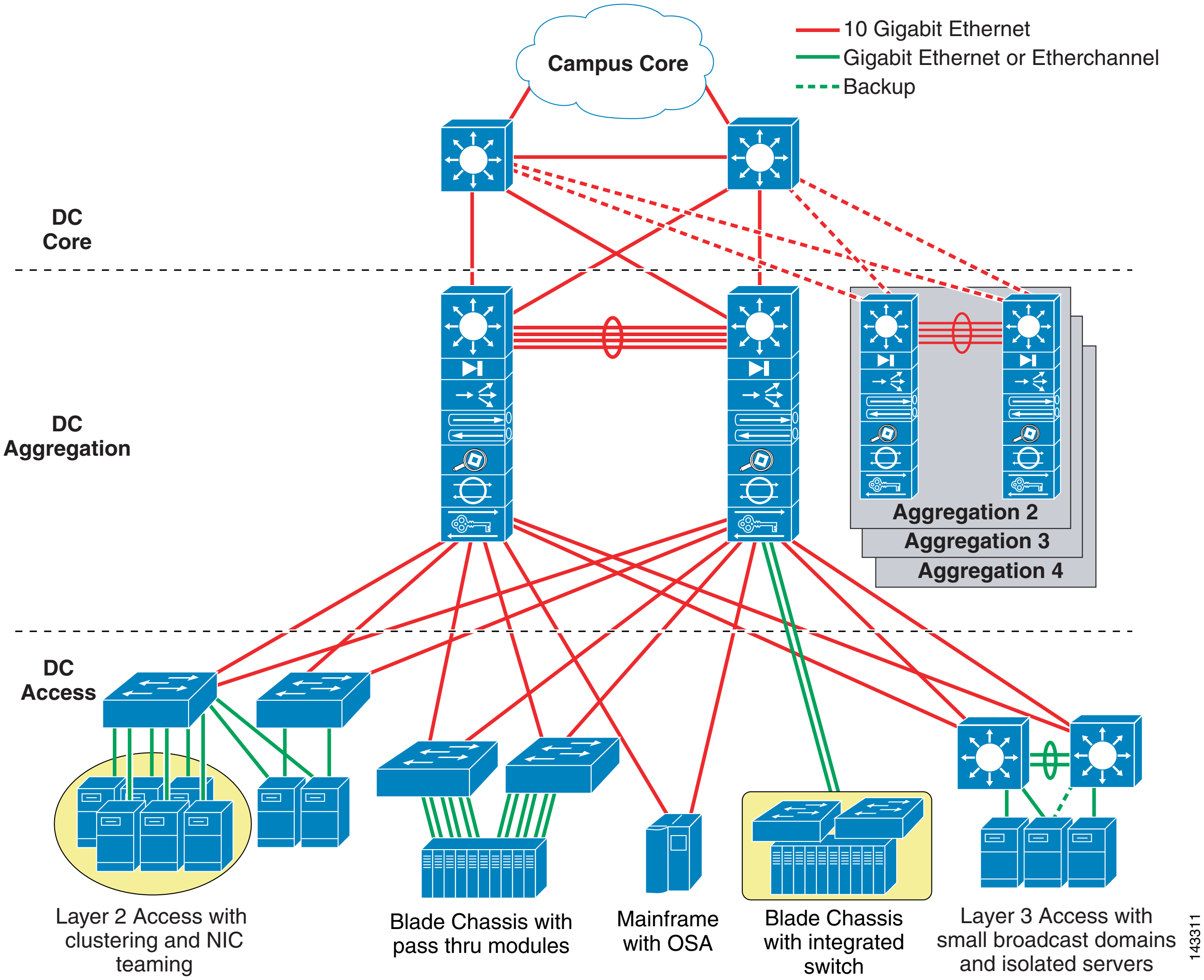
- The front-end network provides the IP routing and switching environment, including client-to-server, server-to-server, and server-to-storage network connectivity.

- The back-end network supports the storage area network (SAN) fabric and connectivity between servers and other storage devices, such as storage arrays and tape drives.

The front-end network contains three distinct functional areas: the core, aggregation, and access layers.

Figure 6 depicts a multi-tier front-end network topology and a variety of services that are available at each of these layers.

Figure 6 Data Center Multi-Tier Model Topology


Campus Core
10 Gigabit Ethernet
Gigabit Ethernet or Etherchannel
Backup
DC Core
DC Aggregation
Aggregation 2
Aggregation 3
Aggregation 4
DC Access
Layer 2 Access with clustering and NIC teaming
Blade Chassis with pass thru modules
Mainframe with OSA
Blade Chassis with integrated switch
Layer 3 Access with small broadcast domains and isolated servers
143311

Core Layer

The core layer is a gateway that provides high-speed connectivity to external entities, such as the WAN, intranet, and extranet of the campus. The data center core is a Layer 3 domain where efficient and expeditious forwarding of packets is the fundamental objective. To this end, the data center core is built with high-bandwidth links (10GE) and employs routing best practices to optimize traffic flows.

Aggregation Layer

The aggregation layer is a point of convergence for network traffic that provides connectivity between server farms at the access layer, and the rest of the enterprise. The aggregation layer supports Layer 2 and Layer 3 functionality and is an ideal location for deploying centralized application, security, and management services. These data center services are shared across the access layer server farms and provide common services in a way that is efficient, scalable, predictable, and deterministic.

The aggregation layer provides a comprehensive set of features for the data center. The following devices support these features:

- Multilayer aggregation switches
- Load balancing devices
- Firewalls
- Intrusion detection systems
- Content engines
- Secure Sockets Layer (SSL) offloaders
- Network analysis devices

Access Layer

The primary role of the access layer is to provide the server farms with the required port density. In addition, the access layer must be a flexible, efficient, and predictable environment to support client-to-server and server-to-server traffic. A Layer 2 domain meets these requirements by providing the following:

- Layer 2 adjacency between servers and service devices
- A deterministic, fast converging, loop-free topology

Layer 2 adjacency in the server farm lets you deploy servers or clusters that require the exchange of information at Layer 2 only. It also readily supports access to network services in the aggregation layer, such as load balancers and firewalls. This enables an efficient use of shared, centralized network services by the server farms.

In contrast, if services are deployed at each access switch, the benefit of those services is limited to the servers directly attached to the switch. Through access at Layer 2, it is easier to insert new servers into the access layer. The aggregation layer is responsible for data center services and the Layer 2 environment focuses on supporting scalable port density.

The access layer must provide a deterministic environment to ensure a stable Layer 2 domain. A predictable access layer allows the spanning tree to converge and recover quickly during failover and fallback.

Note This document does not cover SAN best practices. For more information, refer to the following URL: http://www.cisco.com/en/US/netsol/ns742/networking_solutions_program_category_home.html.

Design Goals

The Cisco Data Center Architecture is a holistic approach that allows the network and the applications it supports to work together. The primary goals of this design are to increase the performance, availability, scalability, and manageability of enterprise applications in the data center, while simultaneously providing a secure environment. In addition, these designs reduce the complexity and implementation time of enterprise applications in the data center using virtualization technologies and network design best practices. The remainder of this document focuses on each of these objectives when deploying an Oracle E-Business Suite 11i application using the services of the Cisco Data Center Infrastructure.

Design and Implementation Details

This section details the integration of the Cisco Application Control Engine (ACE) and the Cisco Firewall Services Module (FWSM) to provide centralized application services in the enterprise data center. It includes the following topics:

- ACE one-arm mode design in the data center
- ACE transparent mode design in the data center

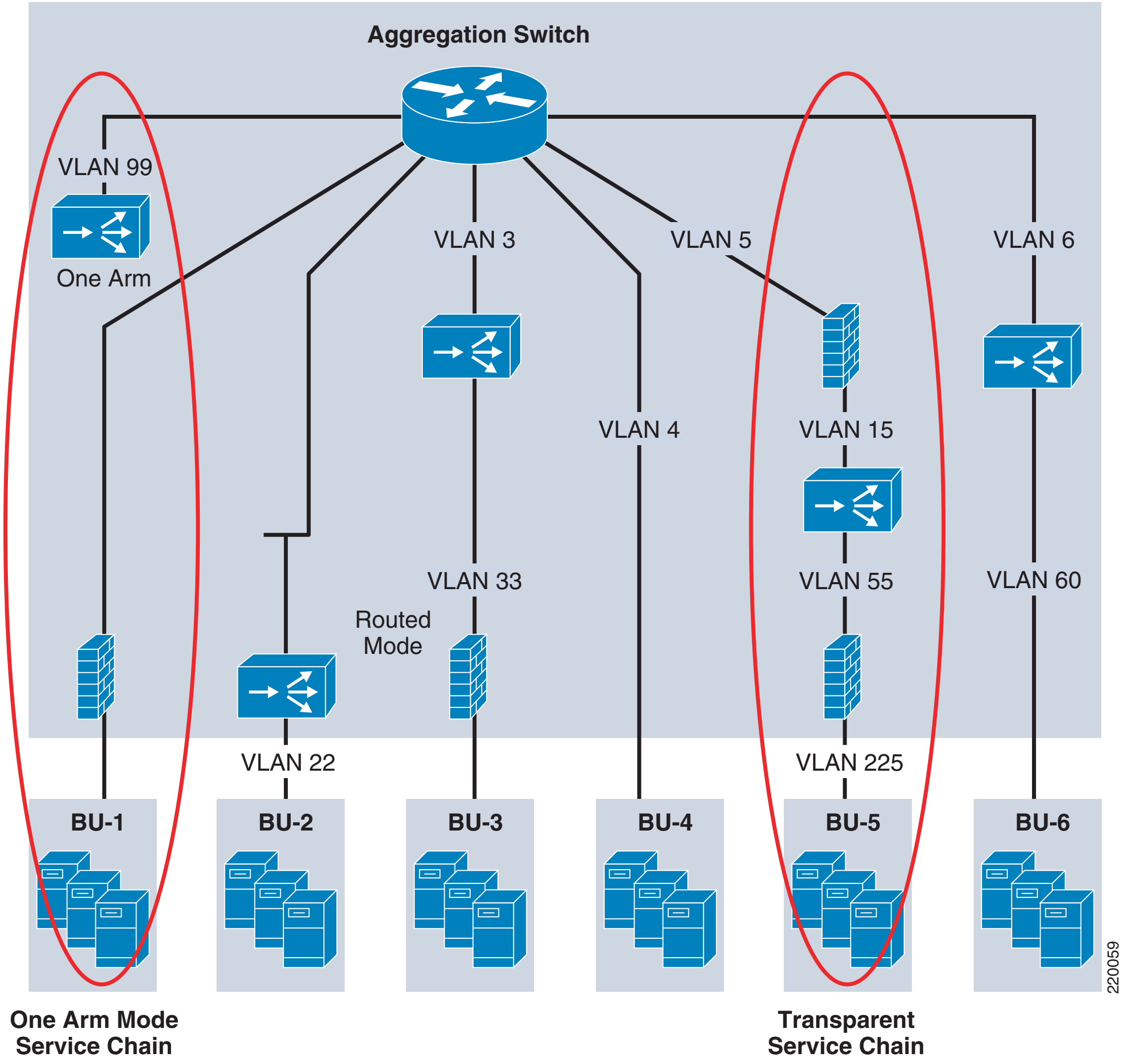
These designs specifically address a multi-tier deployment of Oracle's E-Business Suite application in Cisco Systems' Data Center Infrastructure Architecture. The designs provide centralized server load balancing, SSL offload, and firewall services for the application. In addition, the virtualization capabilities of both the FWSM and the ACE allow a single physical device to provide multiple logical devices. System administrators can assign a single virtual device to a business unit or application to achieve application performance goals or service-level agreements (SLAs).

Figure 7 illustrates the concept of "service chaining" within a single Catalyst 6500 Series aggregation switch. In this example, the virtualization of the ACE and FWSM allows multiple business units to define logically independent network service devices, known as contexts, within the same Catalyst device. 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.

Note Each virtual context has its own application rules and resource use levels, such as CPU, bandwidth, ACLs, and connections, defined.

Figure 7 illustrates some of the more common possible configurations, but does not represent all possible service chain combinations.

Figure 7 Business Units Service Chaining Examples



ACE One-Arm Mode Design

The ACE is an integrated service module for the Catalyst 6500 Series platform that provides high availability, scalability, and security services to the enterprise application. The ACE in one-arm mode supports these objectives by allowing the effective integration of these services with Oracle's E-Business Suite. This design provides server load balancing and firewall functionality to the application tiers of the architecture via the ACE and the FWSM.

The one-arm mode design allows the system administrator to bypass the ACE if the network traffic does not require its services, essentially optimizing the performance of the ACE by removing unnecessary load. In addition, one-arm mode optimizes the routing performance of the data center as the Catalyst 6500 Series Multilayer Switch Feature Card (MSFC) fulfills this role as the default gateway for the servers in the farm.

Figure 8 ACE One-Arm Mode Deployment with Transparent Firewall Services

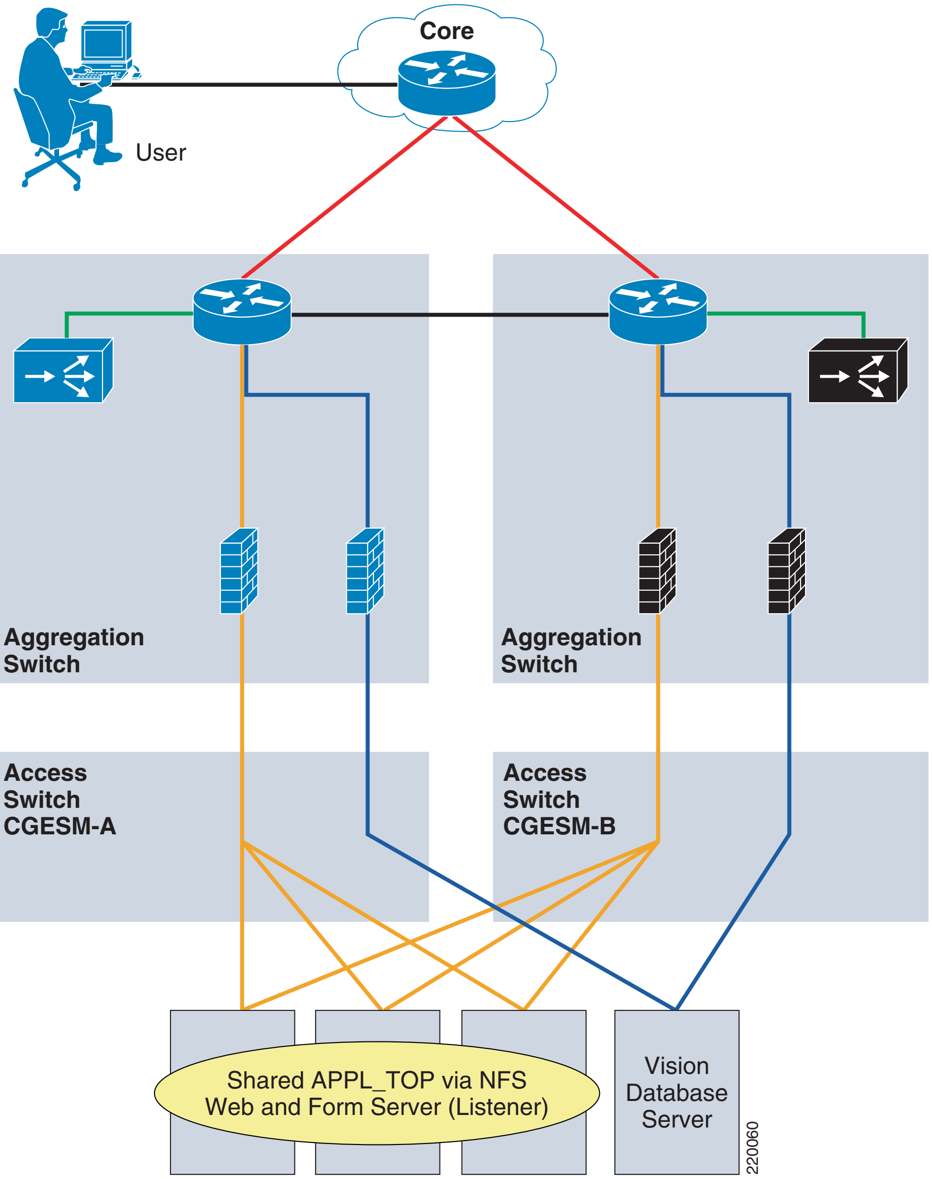


Figure 8 provides a logical view of a virtual ACE and FWSM context in a one-arm service chain configuration. The ACE and FWSM context reside in the aggregation layer. The MSFC is the default route of the shared APPL_TOP servers and Vision database. The FWSM enforces access control as two transparent devices positioned in front of the server farm.

The ACE provides a highly-available Oracle environment through its health monitoring capabilities. As stated previously, Oracle's E-Business Suite uses standard protocols (HTTP/HTTPS) for messaging. Therefore, it is prudent to use one or more of the following health probes to determine the state of the application server:

- TCP probe
- HTTP probe

- HTTPS probe
- TCL script

Note For more information on the server health monitoring capabilities of the ACE module, refer to the following URL:
http://www.cisco.com/en/US/products/ps6906/index.html.

The load balancing predictors, algorithms, supported by the ACE include:

- Round-robin
- Least connections
- Hash address
- Hash cookie
- Hash header
- Hash URL

These algorithms give the system administrator ample flexibility to distribute workload in their application environment.

In addition, the ACE is able to provide session affinity because it understands how to read the cookie or URL data created by the Oracle applications, or to insert its own cookie. With this piece of information, the ACE effectively binds a user of an application to a single server for the duration of their session. Session affinity to a single device allows the application to use the local cache of the server to retrieve session state information instead of using the resources of a shared session state database or another instance of the application server.

Typically, the APPL_TOP servers provide session persistence in an Oracle solution, using processor resources to ensure affinity between clients and applications servers. By positioning the ACE logically in front of the web and application tiers, the network is able to provide session affinity, in addition to health monitoring and server load balancing, the ACE relieves the web server of its session affinity and load balancing responsibilities. This ACE functionality delivers an increase in the overall performance of the application and decreases its complexity.

The integrated SSL (HTTPS) capabilities of the ACE allow for more secure e-business transactions. The ACE provides hardware-based SSL acceleration, moving the processor-intensive functionality from the CPU or NIC of the server into the network. Centralized SSL services in the network allow secure transactions to be efficiently processed and inspected by other network-based services, such as IDS, IPS, or other network analysis devices that cannot be applied without unencrypted “clear” traffic.

Figure 8 indicates firewall services between the application and database tiers. The logical segmentation of the network via VLANs provides this logical division. Administrators can apply granular security policies and traffic filtering rules to each network segment: application and database.

The load balancer provides an increased level of availability by removing unresponsive servers from its load balancing calculations, and by making server farm transactions more efficient. Combined with the security services of a firewall, Oracle application traffic can be secure and optimized.

Note One-arm designs require the use of source Network Address Translation (SNAT) or Policy-Based Routing (PBR) to guarantee the load balancer observes all aspects of the server-to-server application connections. SNAT is easy to configure on the ACE module. For the remainder of this document, assume that SNAT is being used to guarantee symmetric traffic flows to the ACE.

Traffic Pattern Overview for the ACE One-Arm Mode Design

This section describes the traffic pattern in the data center for the following flows:

- Client-to-server
- Server-to-database

Client-to-Server Traffic Flow

Figure 9 depicts the client-to-server traffic flow through the data center when using the ACE in one-arm mode. The client is requesting a web page in the enterprise data center. Figure 9 is also representative of HTTPS (SSL) transactions in the network.

A successful transaction with the one-arm data center design includes the following steps:

1. The client requests a URL associated with a Versatile Interface Processor (VIP) on the ACE module.
2. The MSFC routes the request to the ACE module.
3. The ACE context makes both security and load balancing decisions to select a real server, based on the system administrators' application policies. At this point, the ACE context replaces the VIP address with the IP address of the real server and assigns a SNAT address from the local NAT pool. The ACE context forwards the request to its default gateway on the MSFC using the destination IP address of the real server and its own SNAT address.

   Note The ACE context can use Policy Based Routing (PBR) if the client’s IP address must be maintained. Another option is to use a combination of HTTP header insertion and SNAT to place the client's original IP address within the HTTP header for downstream logging functions.

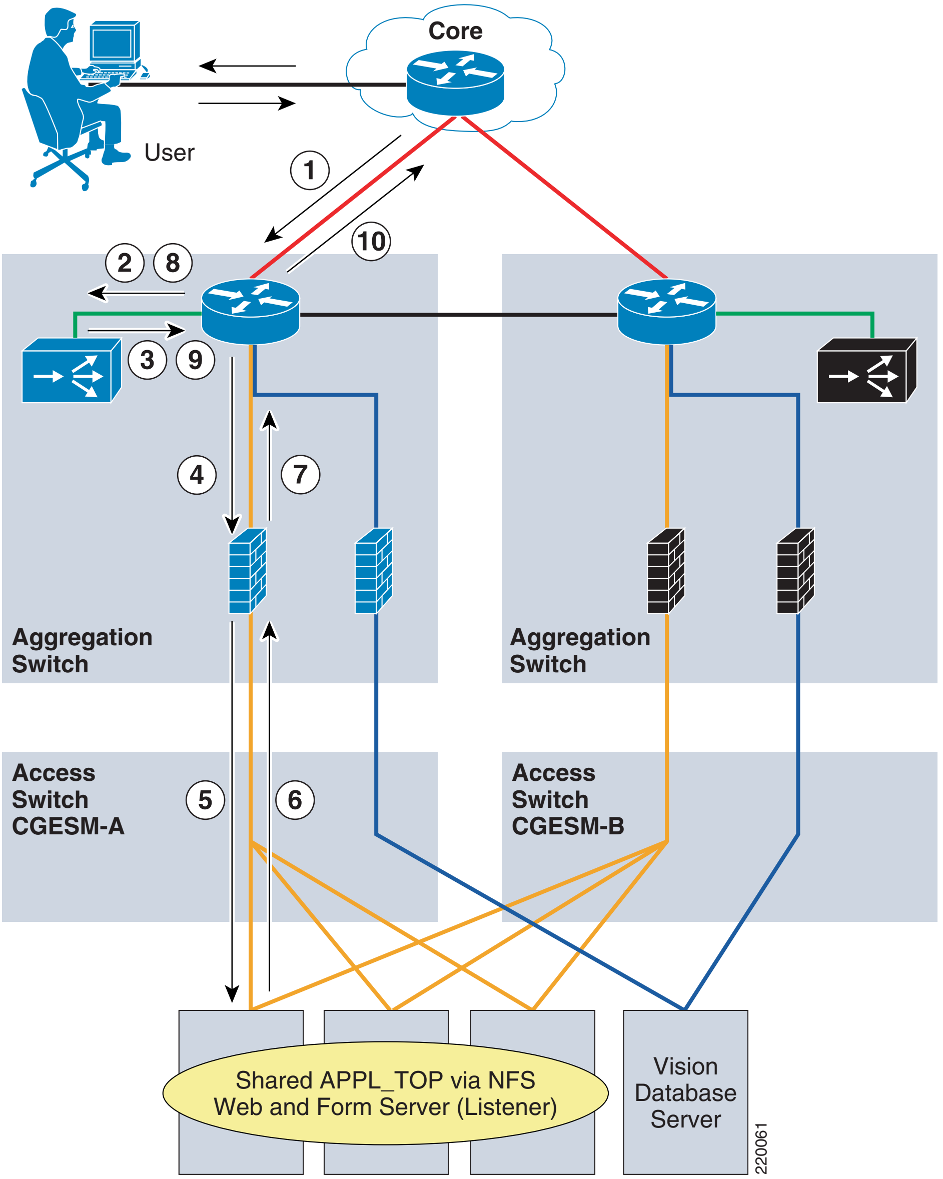
   The ACE context has access control and HTTP deep packet inspection capabilities. HTTP deep packet inspection allows the system administrator to monitor the HTTP protocol, permitting or denying traffic based on user-defined traffic policies. The security features covered by HTTP application inspection include:

   - RFC compliance monitoring and RFC method filtering (RFC 2616)
   - Content, URL, and HTTP header length checks
   - Transfer-encoding methods
   - Content type verification and filtering
   - Port 80 misuse

   Using the regular-expression capabilities of the ACE against HTTP data payloads allows for “signature” based security decisions that are usually reserved for IDS/IPS devices.
4. The MSFC directs the request to the real servers protected by the FWSM context in transparent mode.
5. The FWSM context is bridging traffic between the “inside” and “outside” networks, applying the appropriate security policies to the network segment. The switch forwards the packet to the Oracle 11i APPL_TOP server.
6. The server replies, sending the traffic at L2 to the MSFC, containing its own source IP address and the SNAT address of the ACE as the destination IP address.
7. The FWSM bridges the traffic to the MSFC.
8. The MSFC routes the traffic to the ACE module where the SNAT address resides.

9. The ACE context rewrites the source IP address of the return traffic from the real server IP address to the VIP of the ACE context. The rebuilt packet is sent to the default gateway of the ACE context, the MSFC.
10. The MSFC routes the traffic to the end user.

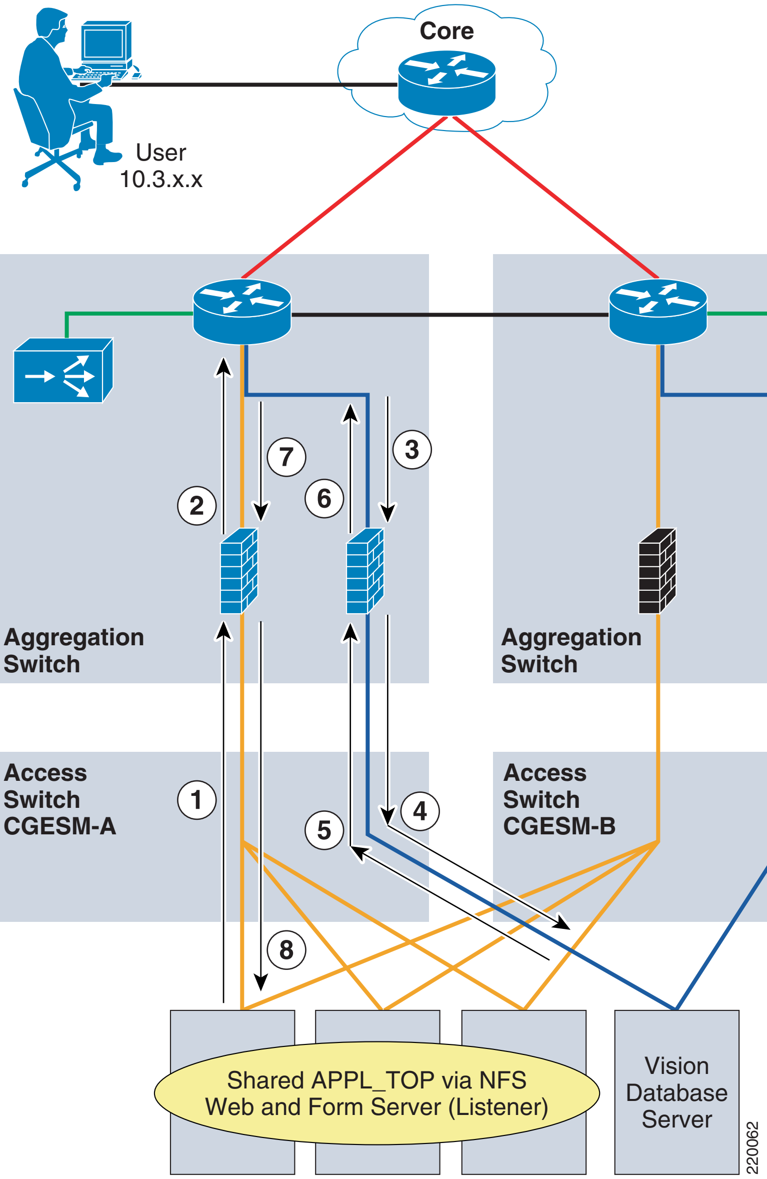
Figure 9 Client to Server Traffic Pattern



Server to Database Traffic Flow

Figure 10 depicts the APPL_TOP server-to-database server traffic flow through the data center when using the ACE in one-arm mode with the FWSM in transparent mode. The APPL_TOP servers are requesting information from the database server in the enterprise data center. The APPL_TOP -to-database server traffic is not leveraging ACE services, but only the stateful inspection services of the FWSM.

Figure 10 Server to Database Traffic Pattern



A successful transaction between the between the APPL_TOP server and the database server in this one-arm data center design includes the following steps:

1. The APPL_TOP server initiates a database request via a TCP connection. The request is directed to its default gateway on the MSFC. The destination IP address is that of the database server and the destination port is 1521, the well-known TNS port.
2. The application tier firewall context receives the request on its inside interface. The FWSM context bridges the traffic to the MSFC, creating a valid connection entry in its local connection table.
3. The MSFC forwards the TNS request to the database server.
4. The database tier firewall context receives the request on its outside interface. The FWSM context determines that TNS traffic is permitted and forwards the request to the database server, creating a new connection in its local connection table.

5. The database server replies to the TNS request and forwards the response to its default gateway, the MSFC. The firewall context bridges the traffic to the MSFC.
6. The MSFC routes the database server response to the APPL_TOP server via the application layer firewall.
7. The response is transparently bridged by the FWSM context to the originating server, based on the valid connection entry originally created by the initial TCP SYN packet.
8. The TNS response reaches the APPL_TOP server.

Architecture Details for the ACE One-Arm Mode Design

This section documents the application and network topology of the testbed and includes the following topics:

- Oracle E-Business Suite 11i Environment
- Oracle E-Business Suite 11i Environment with Integrated Network Services
- Additional integrated service options

Oracle E-Business Suite 11i Environment

This section provides an overview of the test application topology, identifying the hardware and software used during testing.

Hardware

A single HP p-Class BladeSystem houses the nodes comprising the application and database tiers. A combination of BL25p and BL30p were used as the server platforms. The BL25p database server is Fibre channel attached to a Diamond Atto array were the Vision database file system was stored. A single APPL_TOP node, a BL25p, was Fibre channel attached to another Diamond Atto array where the “shared” APPL_TOP resides. The remaining APPL_TOP server nodes use NFS to mount the shared file system available from the Fibre channel attached BL25p.

Software

Red Hat's Enterprise Linux AS release 4 (Nahant Update 2) is the operating system used for all nodes in the test bed. The Oracle test environment consists of the following software packages:

- E-Business Suite 11i version 11.5.10.2
- Oracle Database version 9.2.06.0

Oracle's E-Business Suite contains a sample database, named Vision. The Vision database allowed us to generate valid application traffic in the testbed using production ready applications in the 11i suite.

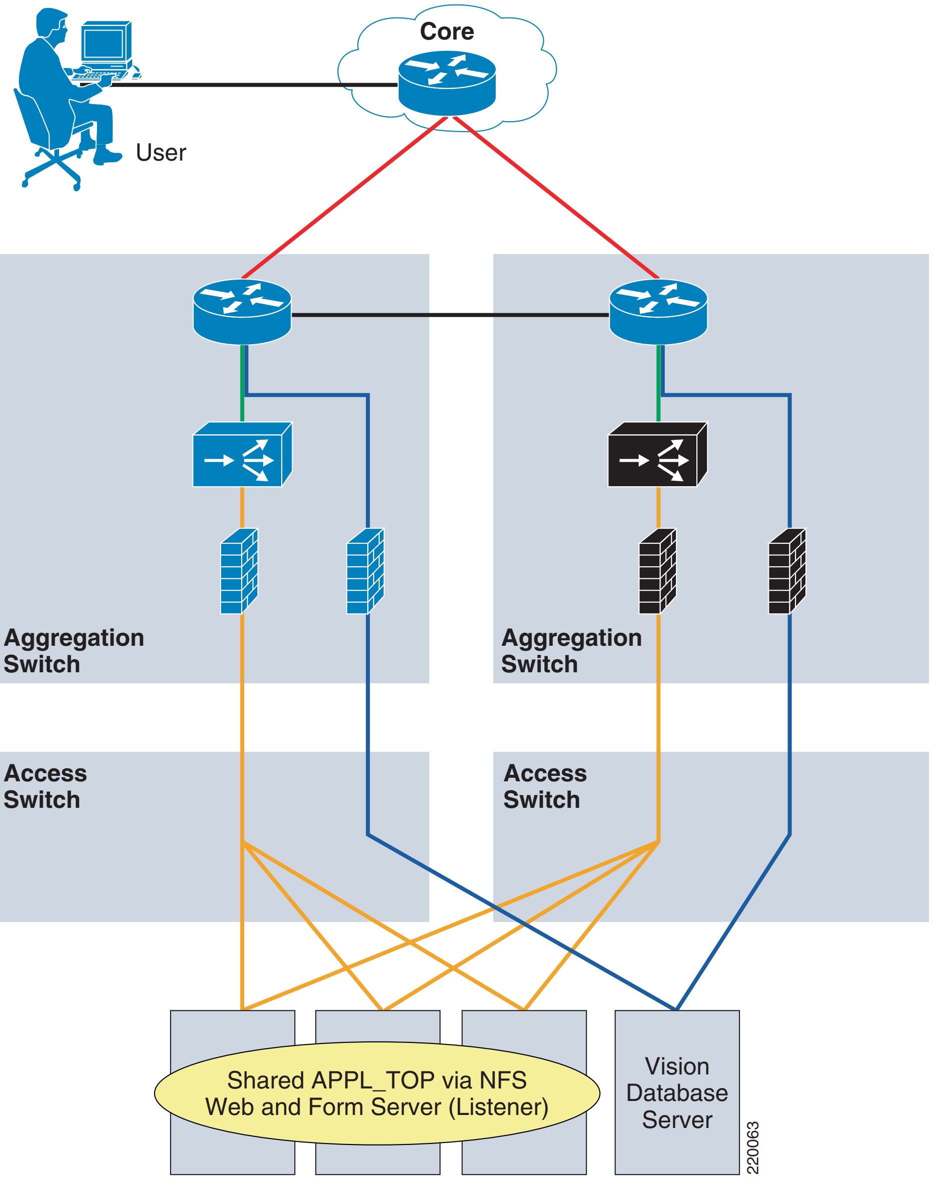
Oracle E-Business Suite 11i Environment with Integrated Network Services

This section covers the introduction of network services into the Oracle E-Business Suite solution topology. The main topics include:

- Software
- Hardware
- Test topology

Figure 11 shows the physical topology used for all of the designs in this document.

Figure 11 CE One-Arm Mode Design



Software

The software images used for this testing include:

- Cisco Native Internetwork Operating System (IOS) software version 12.2(18)SXF5 for the Catalyst 6500 Supervisor 720s
- Cisco FWSM software version 3.1(1)
- Cisco ACE software version 3.0(0)A1(2)

- CGESM software version 12.2(25)SED
- Cisco MDS software version 2.1(2b)

Hardware

The network equipment used for this testing includes:

- Catalyst 6500 with Supervisor 720
- Cisco Firewall Services Module (FWSM)
- Cisco Application Control Engine (ACE)
- Cisco Gigabit Ethernet Switch (CGESM) for the HP p-Class BladeSystem
- Cisco MDS 9216i

Figure 11 depicts the physical topology used for all of the designs described in this document. The HP blade servers are dual-homed to the integrated CGESM switches, providing IP connectivity to the Catalyst 6513 aggregation switches. Each of the Catalyst 6500 Series switches contain integrated network service modules, providing application and security services. The aggregation layer uses 10 Gigabit Ethernet line cards to provide upstream connectivity to the core cloud, and an inter-switch link (ISL) comprised of two 10 Gigabit Ethernet links.

The testbed uses shared storage via two MDS 9216i devices that provide redundant connectivity to a pair of storage arrays. Two of the blade servers take advantage of the fabric. The database server stores the database file on one logical unit number (LUN). One application server accesses the APPL_TOP file system, which is housed on another LUN in the SAN.

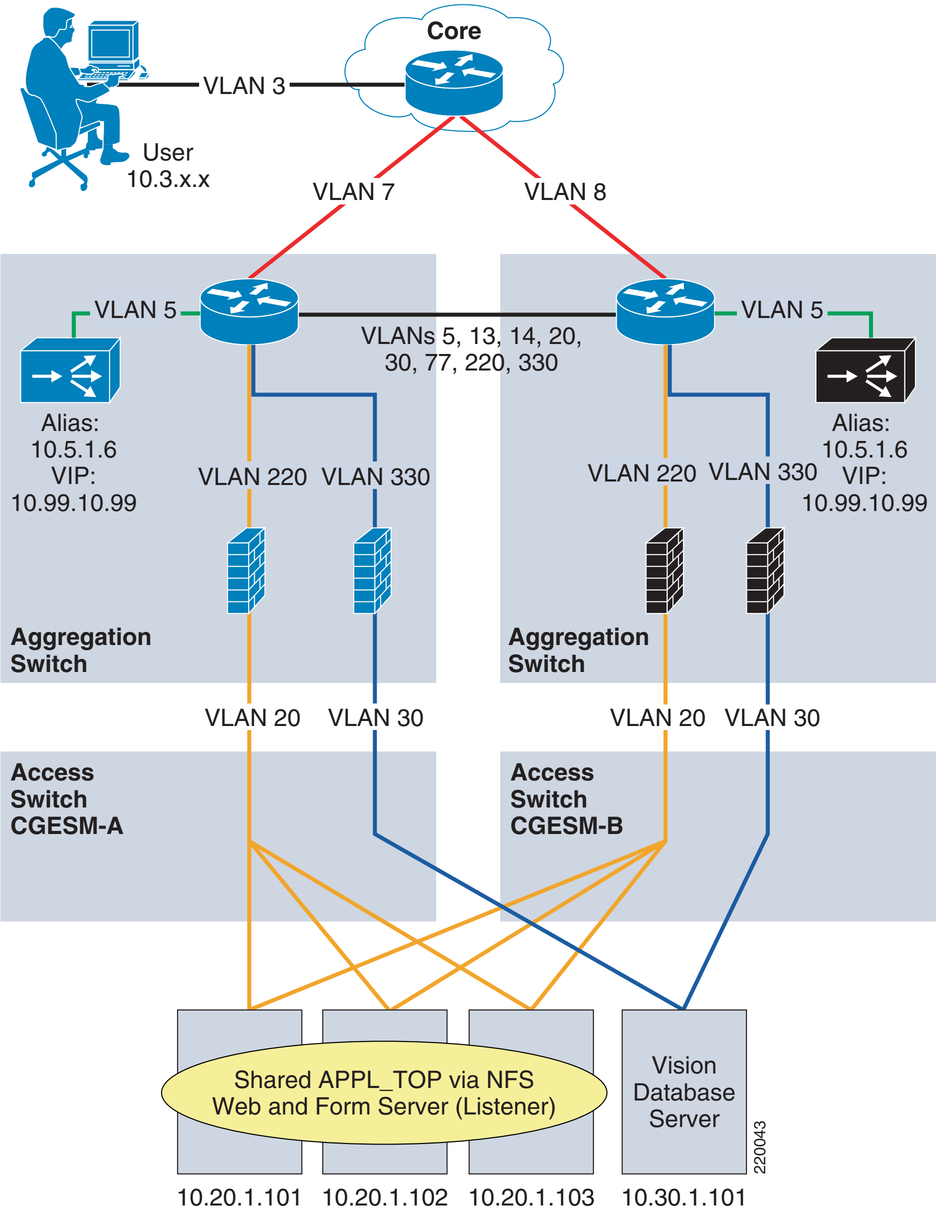
Note The application server accessing the APPL_TOP file system in the SAN simultaneously provides NFS services and exports the APPL_TOP directories. NFS allows the other application servers to “mount” and share the APPL_TOP file-system in the SAN.

Topology

Figure 12 illustrates the logical topology of the Oracle E-Business Suite 11i testbed using the Cisco ACE in a one-arm mode design. The ACE provides load balancing and session persistence for client connections to the Oracle application environment. The FWSM provides stateful inspection to the all transactions in the server farm. Each virtual firewall context bridges traffic between the inside and outside interfaces of this multi-tier environment. In this manner, the FWSM provides granular traffic filtering that is independently applied by each virtual firewall context.

Note In Figure 12, the ISL between the two aggregation switches carries the production traffic VLANs 5, 20, 30, 220, and 330 as well as the fault tolerant and replication VLANs of 13, 14 and 77.

Figure 12 ACE One-Arm Mode Testbed Topology



Note Session persistence was achieved using source-destination IP or via ACE cookie insertion. Each of these methods are supported by Oracle and documented in the configuration examples in this section. Refer to the "Oracle Metalink document 217368.1" for more information on supported load balancing schemes.

The application and database servers use the MSFC as a default gateway and are dual-homed to the integrated CGESM access switches. The integrated blade switches connect to the aggregation layer Catalyst 6500s Series switch using the Link Aggregation Control Protocol (802.3ad) to bundle four Gigabit Ethernet ports into a single logical channel. The channel uses the trunk failover feature, also known as link state tracking, of the integrated blade switch. Trunk failover is a high availability mechanism available on Cisco blade switches that binds the link state of an external uplink with the internal server ports on the blade switch. This feature optimizes the NIC teaming functionality of the server to provide higher application availability.

The virtual ACE and FWSM contexts in the testbed are deployed in an active/standby scenario, allowing for failure conditions through redundancy. Convergence times in the data center are dependent on the type and location of the failure. The ACE failover time is less than 1 second, and is imperceptible from the end users perspective as active connection state is maintained between the two virtual devices in addition to cookie persistence data.

Data center infrastructure failover and recovery times are available at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCI_SRND_2_5_book.html.

For detailed configurations, refer to Network Configuration Examples, page 35 and Application Configuration Details, page 27.

Additional Integrated Service Options

This document addresses the integration of network services with the Oracle enterprise class application, E-Business Suite 11i. Server load balancing and security are fundamental services used by data center applications. However, these are not the only integrated network services available for the enterprise. The following network services are also readily available as service modules or appliances:

- SSL offloading (hardware-based option integrated into the ACE platform)
- Intrusion prevention systems
- Intrusion detection systems
- Network analysis devices
- WAN optimization systems (WAAS, AVS)
- Caching devices

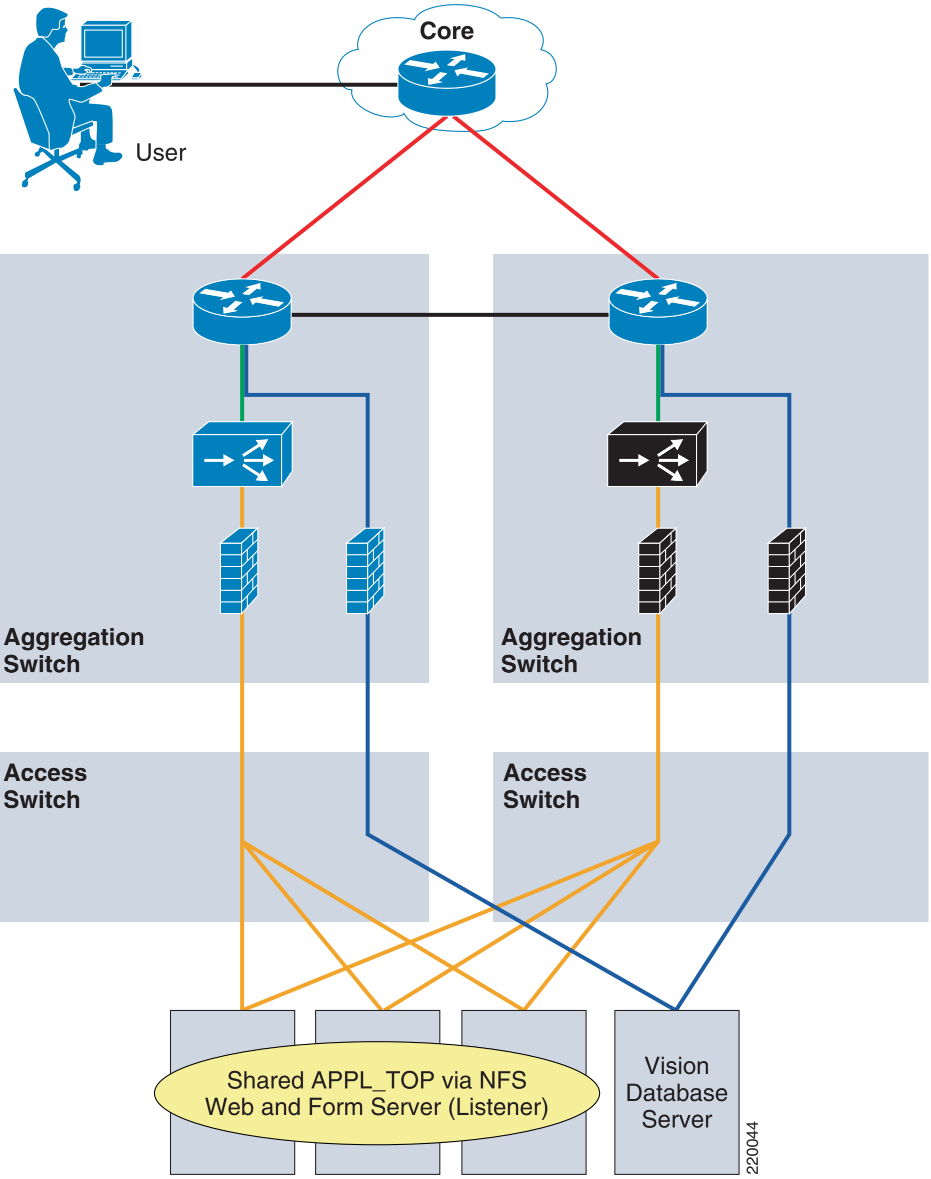
ACE Transparent Mode Design

The ACE context in a transparent deployment model permits the seamless integration of intelligent network services within the data center. A transparent ACE context bridges Layer 2 traffic, applying application security and load balancing services as the system administrators' policies dictate. In a transparent deployment, the default gateway for the servers in the server farm is not the ACE, but another Layer 3 device, such as a router, firewall, or load-balancer.

The aggregation layer is an ideal location to deploy network application services because much of the traffic converges in this area of the data center. Figure 13 is a logical view of a virtual ACE and FWSM contexts configured in a transparent bridging model. The ACE and FWSM service modules are physically located in the aggregation switches of the data center and provide services via virtual device contexts. In this model, the MSFC is the default gateway for the server farm. All ingress and egress server traffic will traverse the ACE, firewall virtual contexts, which means that stateful packet inspection, load balancing, and application services are uniformly applied. These functions provide a highly available, scalable, and secure application environment.

The transparent service chain allows the ACE to provide load-balancing, session persistence, and SSL offload functionality, similar to the one-arm design. The significant difference is that all traffic must pass through the ACE and FWSM. This requires high performance and hardware-based services that both the FWSM and ACE can provide.

Figure 13 ACE Transparent Mode Design



Traffic Pattern Overview for the ACE Transparent Mode Design

This section provides information about traffic patterns.

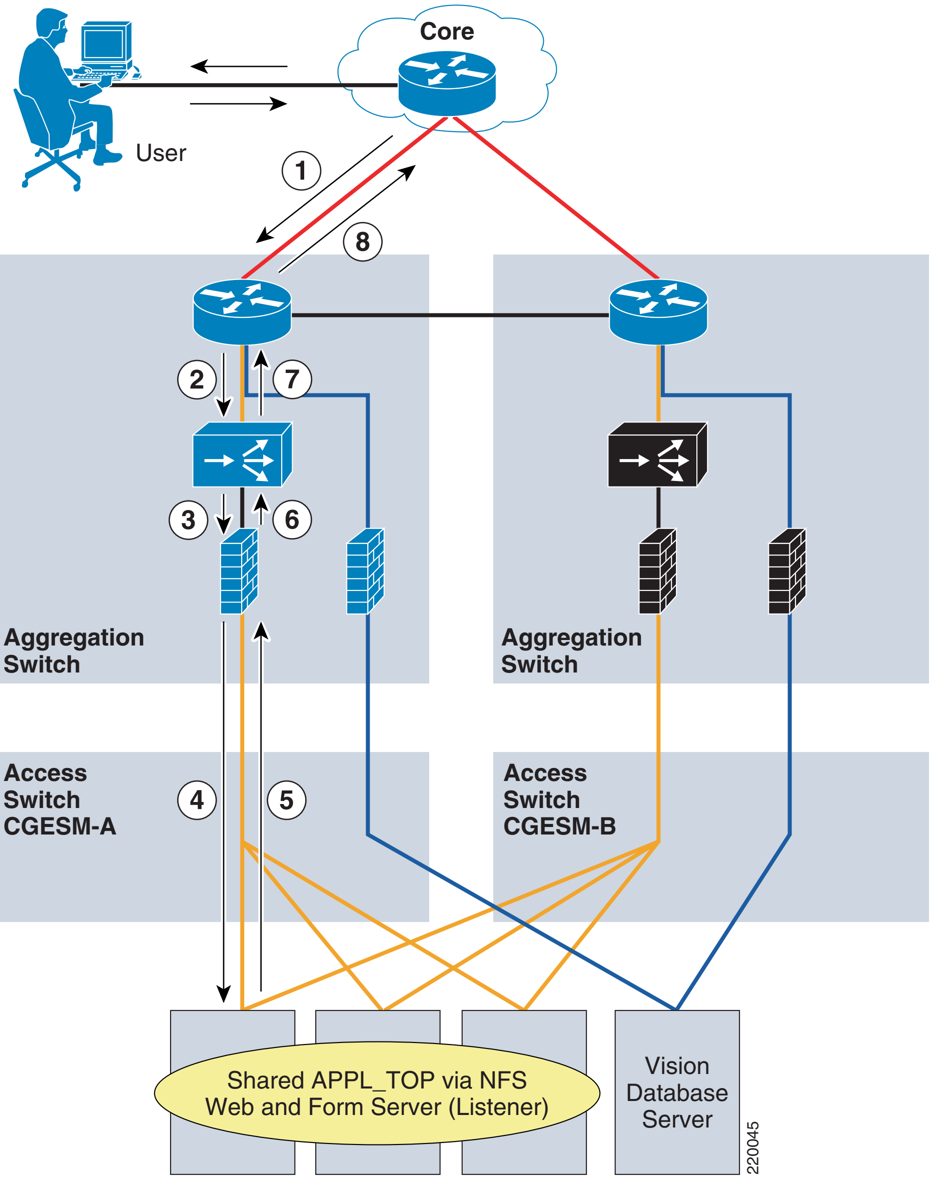
Client to Server Traffic Flow

Figure 14 depicts the client-to-server traffic flow through the data center when using the ACE and FWSM in transparent mode. The client is requesting a web page in the enterprise data center. A successful transaction with the transparent data center design includes the following steps:

1. A client requests an URL associated with a VIP on the ACE module.
2. The MSFC routes the request to the ACE module.

3. The ACE module receives the request on its transparent context that is associated with the VIP address. The ACE provides security and load balancing services. Source-destination IP address or cookie-based persistence methods are available for use in the 11i environment. The ACE replaces the VIP address with the IP address of a real server in the APPL_TOP server farm. The ACE forwards the traffic to the FWSM context, protecting the APPL_TOP servers.
4. The FWSM transparent context receives the request traffic and permits the traffic, based on the system administrator's access rules. The request is passed to the real server.
5. The real server receives and responds to the request using the destination IP address of the client.
6. The transparent FWSM bridges the traffic.
7. The transparent ACE replaces the source IP address of the real server with that of the VIP and bridges the reply to the MSFC.
8. The MSFC routes the reply to the client.

Figure 14 Client to Server Traffic Pattern—Transparent Mode



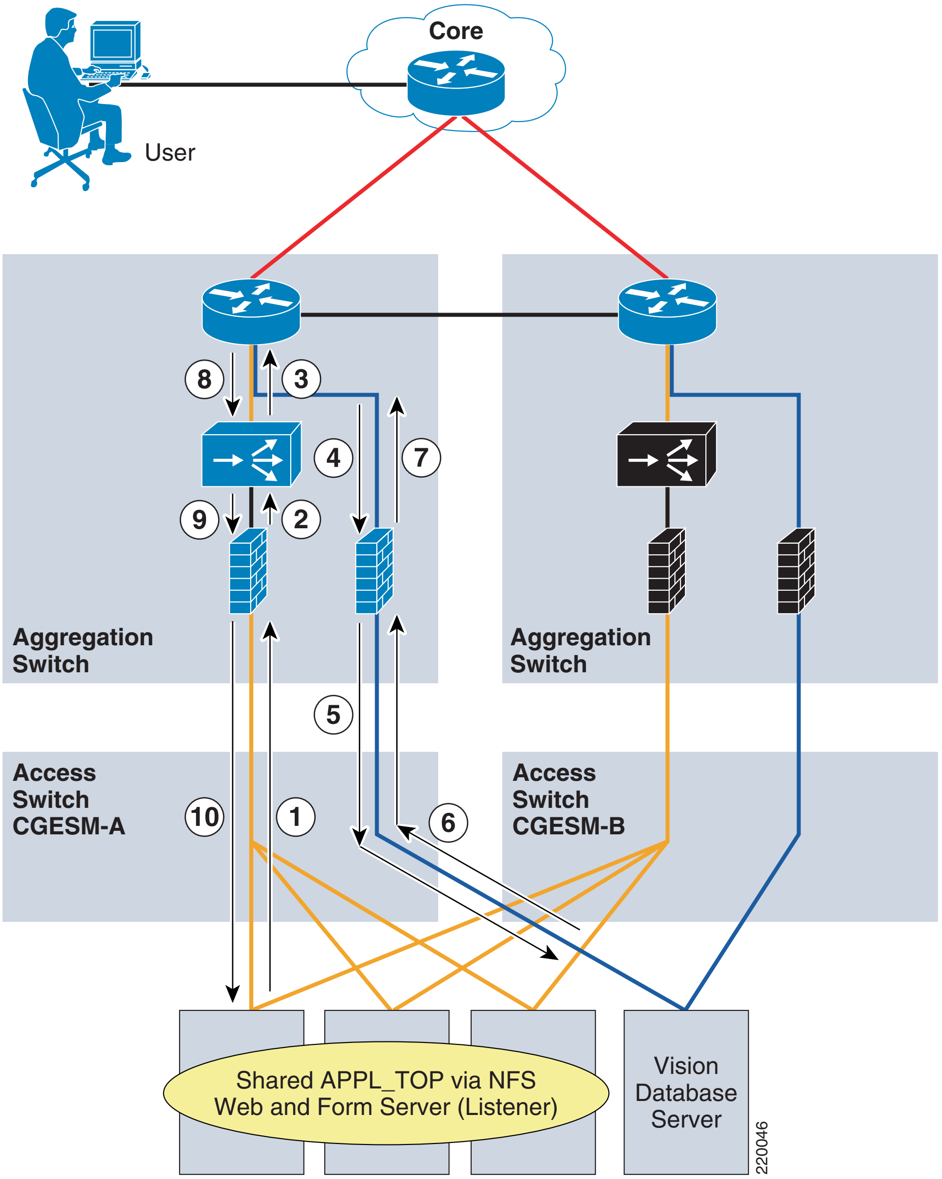
Server to Database Traffic Flow

Figure 15 depicts the APPL_TOP server to database server traffic flow through the data center when using the ACE and FWSM contexts in transparent mode. The APPL_TOP servers are making requests of the database server via TCP on the TNS port. The following steps comprise a successful transaction between the APPL_TOP and database tiers in this topology:

1. The APPL_TOP server initiates a database request via a TCP connection to port 1521. The request is sent to the default gateway of the servers, in this case the MSFC.
2. The FWSM context, in transparent mode, bridges the traffic from its inside to outside interface. Forwarding of traffic is dependent on the security rules established by the system administrator; in this case, APPL_TOP traffic to the database server on port 1521 is acceptable.

3. The ACE context, in transparent mode, bridges the traffic from its inside to outside interface, passing the traffic to the default gateway of the APPL_TOP servers, the MSFC. The ACE is not configured to provide load balancing services. APPL_TOP- to-database traffic is simply bridged, but ACLs may be applied.
4. The MSFC routes the traffic to the database server.
5. The database tier firewall context receives the request on its outside interface. The FWSM context determines that TNS traffic is permitted and forwards the request to the database server, creating a new connection in its local connection table.
6. The database server replies to the TNS request and forwarding the response to its default gateway the MSFC.
7. The firewall context bridges the traffic to the MSFC.
8. The MSFC routes the database server response to the APPL_TOP server via the application layer ACE context. The ACE bridges the traffic from its outside to inside interface.
9. The response is transparently bridged by the FWSM context to the originating server, based on the valid connection entry originally created by the initial TCP SYN packet.
10. The TNS response reaches the APPL_TOP server.

Figure 15 Server-to-Database Traffic—Transparent Mode



Architecture Details for the ACE Transparent Mode Design

This section documents the application and network topology of the testbed and includes the following topics:

- Oracle E-Business Suite 11i Environment
- Oracle E-Business Suite 11i Environment with Integrated Network Services
- Additional integrated service options

Oracle E-Business Suite 11i Environment

The Oracle 11i application topology documented in the Architecture Details for the ACE One-Arm Mode Design, page 15 section remains the same. This is significant because adding, removing, or modifying network services is transparent to the application environment it supports. For details on the software and hardware used for the transparent mode design, refer to the Architecture Details section.

Oracle E-Business Suite 11i Environment with Integrated Network Services

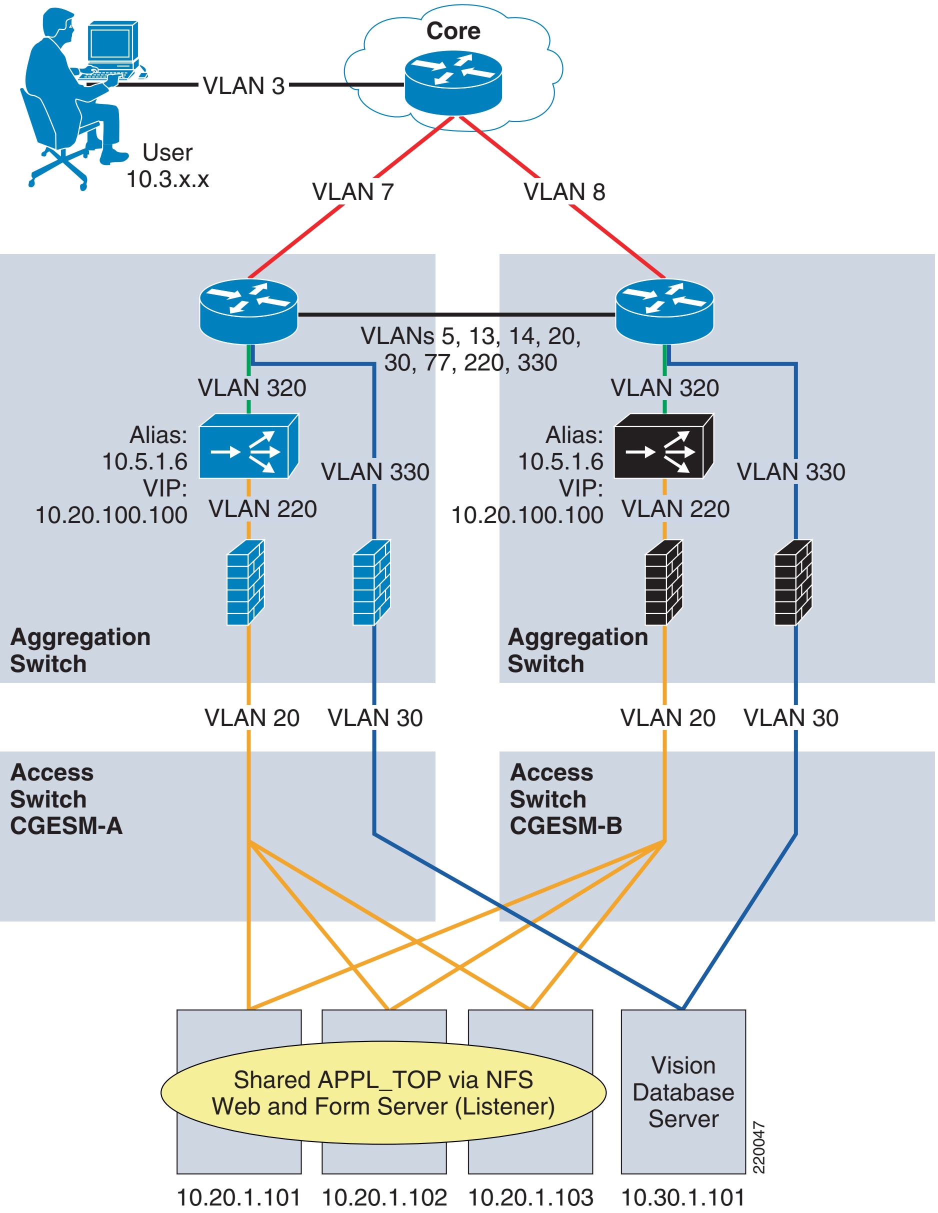
The network services introduced in this section use the identical software and hardware that is documented in Oracle E-Business Suite 11i Environment with Integrated Network Services, page 15. The physical infrastructure of the application and network is the same for both one-arm and transparent designs. Refer to the previous section for more information.

Topology

Figure 16 depicts the logical design of a transparent service chain consisting of a single ACE virtual context and two FWSM virtual contexts. The ACE contexts provides load balancing and session persistence via a virtual IP address that leverages the real APPL_TOP servers residing behind the FWSM context.

Note In Figure 16, the ISL between the two aggregation switches carries the production traffic VLANs 20, 30, 220, and 330 as well as the fault tolerant and replication VLANs of 13, 14 and 77.

Figure 16 Transparent Testbed Topology



Note Session persistence was achieved using source-destination IP or via ACE cookie insertion. Each of these methods are supported by Oracle and documented in the configuration listings below. Refer to the “Oracle Metalink document 217368.1” for more information on supported load balancing schemes.

The APPL_TOP servers are unaware of the transparent services offered by the Catalyst 6500 Series service modules. The APPL_TOP servers use the MSFC as their default gateway as does the database server behind its own virtual firewall context. The connection entries across the transparent virtual devices maintain the client and server IP addressing to provide simplified logging at the application and network levels.

Following is a sample server-to-server connection across the transparent service chain:

```
ace# show connection
conn-id    np dir proto vlan source                destination           state
----------+--+---+-----+----+---------------------+---------------------+------+
7          1  in  TCP   220  10.20.1.102:32869     10.30.1.101:1521      ESTAB
6          1  out TCP   320  10.30.1.101:1521      10.20.1.102:32869     ESTAB

fwsm# show connection
TCP out 10.30.1.101:1521 in 10.20.1.102:32869 idle 0:00:05 Bytes 155360 FLAGS - UOI
```

Figure 16 also shows the ACE and FWSM configured in an active/standby scenario. Each is capable of replicating their connection and sticky entries to their peer device to provide a highly available and persistent connection for both client-to-server and server-to-server traffic. The ACE failover time is sub-second in this configuration.

Data center infrastructure failover and recovery times are available at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCI_SRND_2_5_book.html.

For detailed configurations, refer to Network Configuration Examples, page 35 and Application Configuration Details, page 27.

Additional Service Integration Options

This document addresses the integration of network services with the Oracle enterprise class application, E-Business Suite 11i. Server load balancing and security are fundamental services used by data center applications. However, these are not the only integrated network services available for the enterprise. The following network services are also readily available as service modules or appliances:

- SSL offloading (hardware-based option integrated into the ACE platform)
- Intrusion prevention systems
- Intrusion detection systems
- Network analysis devices
- WAN optimization systems (WAAS, AVS)
- Caching devices

Application Configuration Details

This section documents the application environment, including any special modifications to the software environment including:

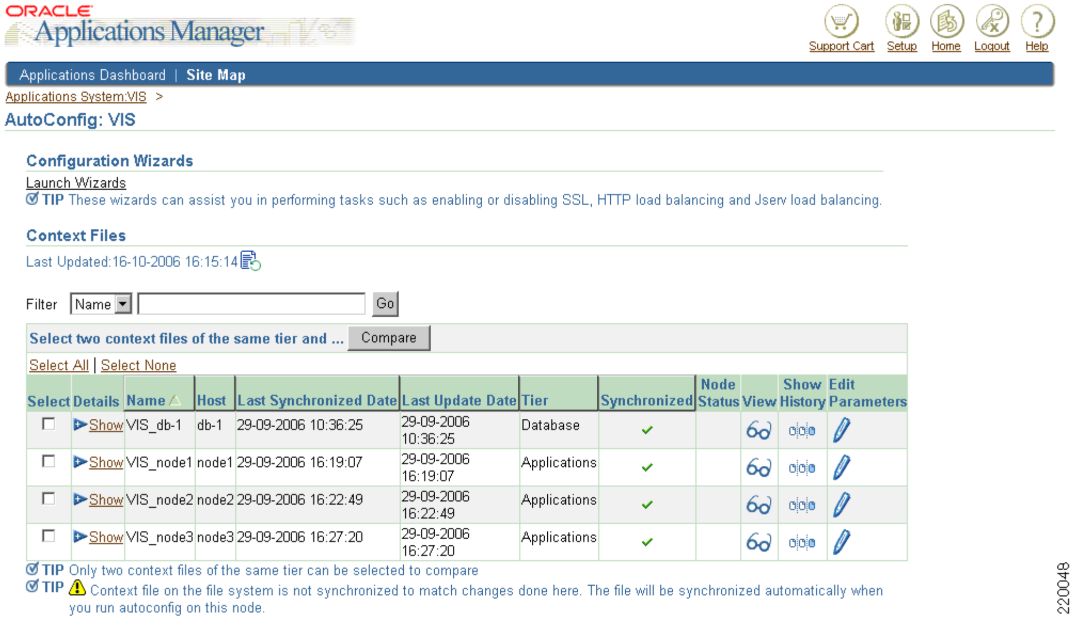
- HTTP load balancing
- Forms listener servlet
- SSL accelerator
- Cookie and session persistence

This section relies heavily upon the Oracle management tool known as AutoConfig. AutoConfig manages changes in the Oracle Applications systems using an application context file and a series of scripts. The context file uses an XML format and represents the application environment on a single node. The Oracle AutoConfig tool simplifies and standardizes the application environment.

Note The context file naming convention is *SID_hostname*.xml. For example, in our Vision database environment the context file for node1 is name VIS_node1.xml

The Oracle Applications Manager (OAM) GUI, shown in Figure 17, allows you to configure the context files directly, or to modify existing applications nodes through a set of configuration wizards. Explaining the functionality of AutoConfig and OAM is beyond the scope of this document, but it is important to note that beyond using the OAM to manage the content of the individual context file, one must use a local **adautocfg** script on each server node before any changes will be reflected in the application environment.

Figure 17 Oracle Applications Manager



AutoConfig: VIS

Configuration Wizards

Launch Wizards

TIP These wizards can assist you in performing tasks such as enabling or disabling SSL, HTTP load balancing and Jserv load balancing.

Context Files

Last Updated:16-10-2006 16:15:14

Filter Name [Go]

Select two context files of the same tier and ... [Compare]

Select All | Select None

Select	Details	Name	Host	Last Synchronized Date	Last Update Date	Tier	Synchronized	Node Status	View	Show History	Edit Parameters
☐	▶Show	VIS_db-1	db-1	29-09-2006 10:36:25	29-09-2006 10:36:25	Database	✓				
☐	▶Show	VIS_node1	node1	29-09-2006 16:19:07	29-09-2006 16:19:07	Applications	✓				
☐	▶Show	VIS_node2	node2	29-09-2006 16:22:49	29-09-2006 16:22:49	Applications	✓				
☐	▶Show	VIS_node3	node3	29-09-2006 16:27:20	29-09-2006 16:27:20	Applications	✓				

TIP Only two context files of the same tier can be selected to compare

TIP ⚠ Context file on the file system is not synchronized to match changes done here. The file will be synchronized automatically when you run autoconfig on this node.

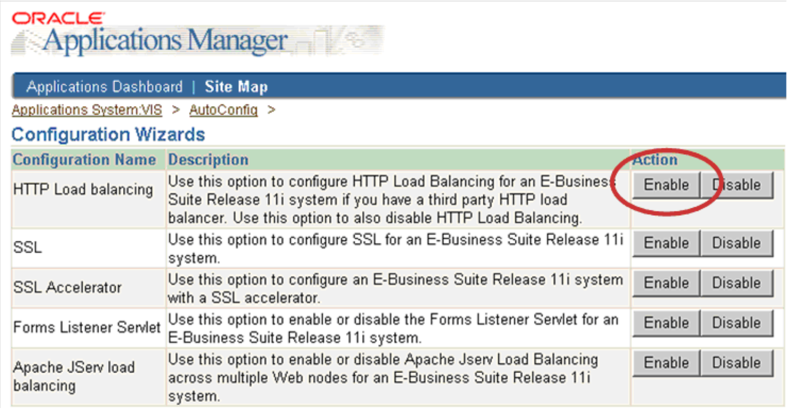
HTTP Load Balancing

Perform the following steps to use a hardware-based load balancer with the Oracle E-Business Suite 11i:

Step 1 Log in to the OAM and select the **Site Map - System Administration** tab, then select **AutoConfig** (see Figure 17).

Step 2 Click **Launch Wizards**.

Step 3 Enable HTTP Load Balancing.



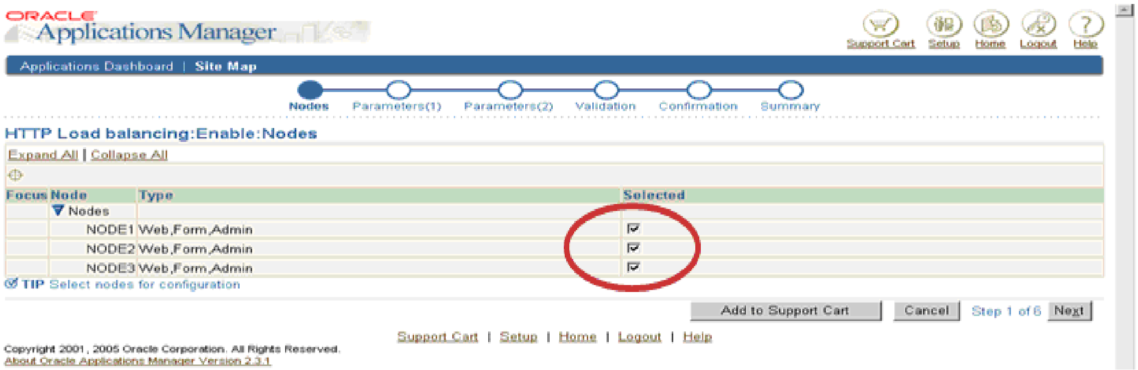
ORACLE
Applications Manager
Applications Dashboard | Site Map
Applications System:VIS > AutoConfig >

Configuration Wizards

Configuration Name	Description	Action
HTTP Load balancing	Use this option to configure HTTP Load Balancing for an E-Business Suite Release 11i system if you have a third party HTTP load balancer. Use this option to also disable HTTP Load Balancing.	Enable Disable
SSL	Use this option to configure SSL for an E-Business Suite Release 11i system.	Enable Disable
SSL Accelerator	Use this option to configure an E-Business Suite Release 11i system with a SSL accelerator.	Enable Disable
Forms Listener Servlet	Use this option to enable or disable the Forms Listener Servlet for an E-Business Suite Release 11i system.	Enable Disable
Apache JServ load balancing	Use this option to enable or disable Apache Jserv Load Balancing across multiple Web nodes for an E-Business Suite Release 11i system.	Enable Disable

220049

Step 4 Select the nodes to be included as real servers in the ACE server farm configuration.



HTTP Load balancing:Enable:Nodes

Expand All | Collapse All

Focus	Node	Type	Selected
	Nodes		
	NODE1	Web,Form,Admin	☑
	NODE2	Web,Form,Admin	☑
	NODE3	Web,Form,Admin	☑

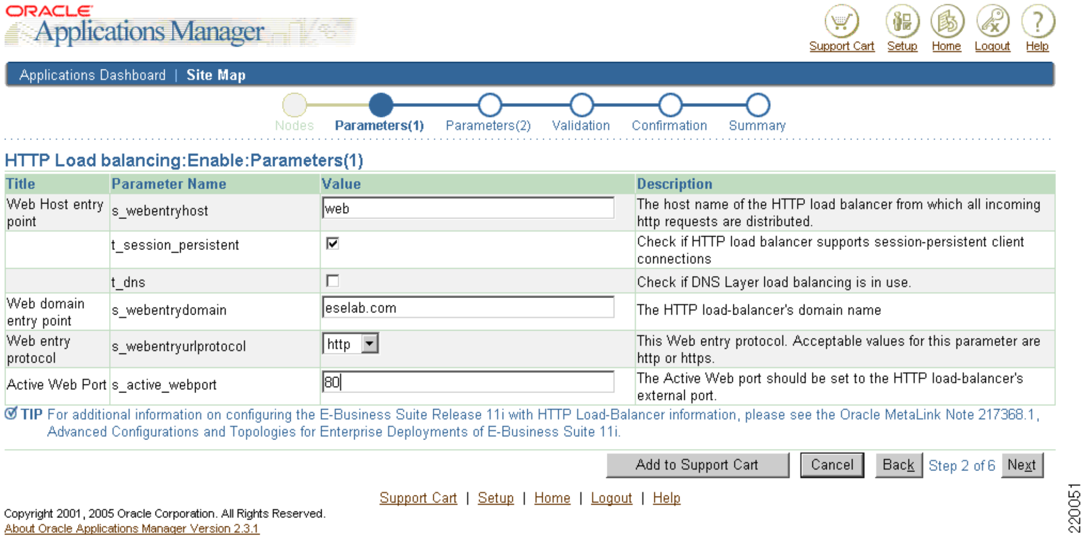
TIP Select nodes for configuration

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.
About Oracle Applications Manager Version 2.3.1

220050

Step 5 Provide the information necessary for the Oracle applications to create well-formed URLs.

- s_webentryhost—DNS name of the ACE VIP utilized by clients.
- t_session_persistent—Place a check mark in the check box if you will be using cookie or src-dst IP based sticky on the ACE context.
- s_webentrydomain—domain name associated with the VIP.
- s_webentryprotocol—http or https.
- Active Web Port s_active_webport—by default this value is 8000, change this to a value of your choice or use '80' which is the well known HTTP port value.



HTTP Load balancing:Enable:Parameters(1)

Title	Parameter Name	Value	Description
Web Host entry point	s_webentryhost	web	The host name of the HTTP load balancer from which all incoming http requests are distributed.
	t_session_persistent	☑	Check if HTTP load balancer supports session-persistent client connections
	t_dns	□	Check if DNS Layer load balancing is in use.
Web domain entry point	s_webentrydomain	eselab.com	The HTTP load-balancer's domain name
Web entry protocol	s_webentryurlprotocol	http	This Web entry protocol. Acceptable values for this parameter are http or https.
Active Web Port	s_active_webport	80	The Active Web port should be set to the HTTP load-balancer's external port.

TIP For additional information on configuring the E-Business Suite Release 11i with HTTP Load-Balancer information, please see the Oracle MetaLink Note 217368.1, Advanced Configurations and Topologies for Enterprise Deployments of E-Business Suite 11i.

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.
About Oracle Applications Manager Version 2.3.1

Step 6 At this point, a series of validation and confirmation panels will be displayed. After successfully completing these steps, basic load-balancing configurations will be saved on the context-files of each server node selected.

Step 7 Stop all currently running Oracle applications using the **adstpall** script on each impacted node.

Step 8 Run the **adautocfg** script on each node.

Step 9 Start all the server nodes using the **adstrtall** script.

Caution Do not stop the database because each node requires access to the database server during this process.

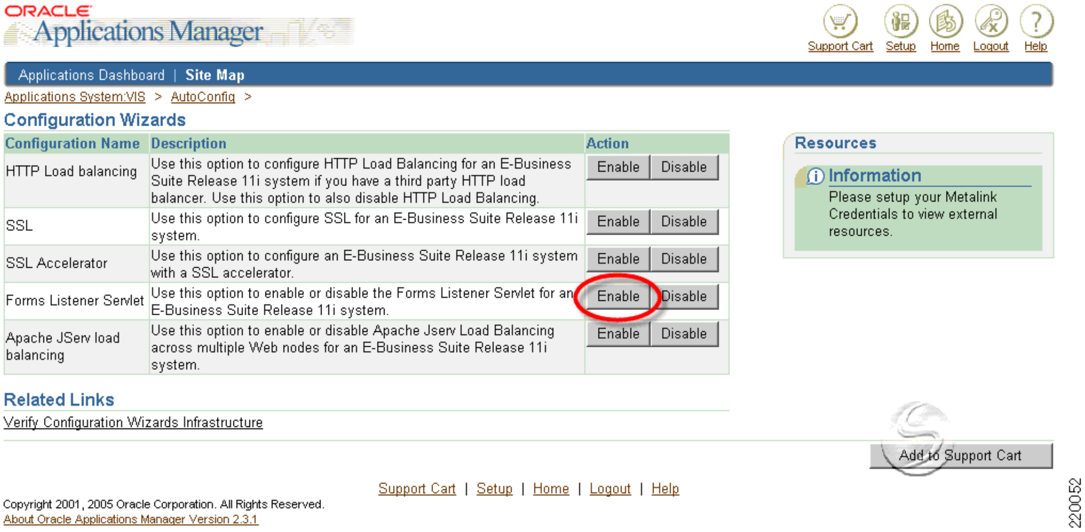
Forms Listener Servlet

The forms listener servlet allows you to access the forms server in the Oracle Applications environment via the web server. Refer to Desktop Tier, page 3 for more information. Perform the following steps to enable the forms listener servlet:

Step 1 Log into the OAM and select the **Site Map - System Administration** tab, then select **AutoConfig** (see Figure 17).

Step 2 Select **Launch Wizards**.

Step 3 Click the **Enable Forms Listener Servlet** button.


ORACLE Applications Manager
Support Cart
Setup
Home
Logout
Help
Applications Dashboard | Site Map
Applications System:VIS > AutoConfig >
Related Links
Verify Configuration Wizards Infrastructure
Add to Support Cart
Support Cart | Setup | Home | Logout | Help
220052

Configuration Wizards

Configuration Name	Description	Action
HTTP Load balancing	Use this option to configure HTTP Load Balancing for an E-Business Suite Release 11i system if you have a third party HTTP load balancer. Use this option to also disable HTTP Load Balancing.	Enable Disable
SSL	Use this option to configure SSL for an E-Business Suite Release 11i system.	Enable Disable
SSL Accelerator	Use this option to configure an E-Business Suite Release 11i system with a SSL accelerator.	Enable Disable
Forms Listener Servlet	Use this option to enable or disable the Forms Listener Servlet for an E-Business Suite Release 11i system.	Enable Disable
Apache JServ load balancing	Use this option to enable or disable Apache Jserv Load Balancing across multiple Web nodes for an E-Business Suite Release 11i system.	Enable Disable

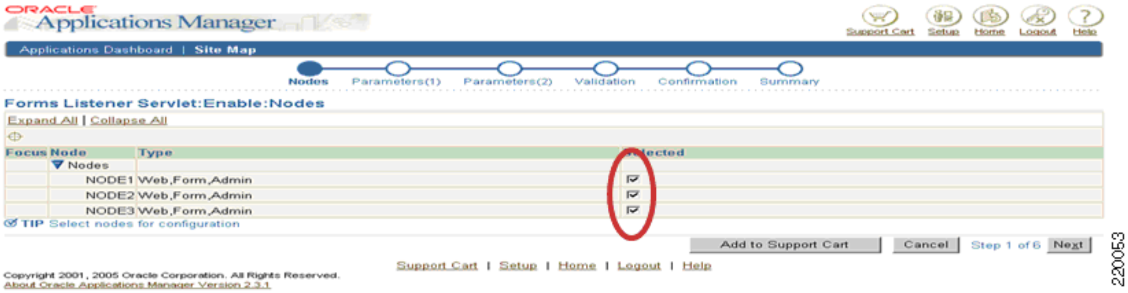
Resources

Information

Please setup your Metalink Credentials to view external resources.

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.
About Oracle Applications Manager Version 2.3.1

Step 4 Select the application server nodes that will be using the forms listener servlet.



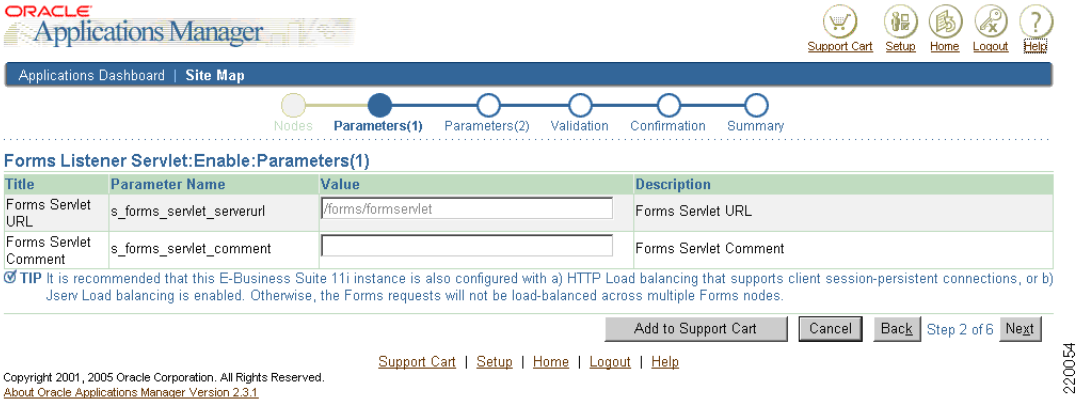
Forms Listener Servlet:Enable:Nodes

Focus	Node	Type	Selected
	Nodes		
	NODE1	Web,Form,Admin	☑
	NODE2	Web,Form,Admin	☑
	NODE3	Web,Form,Admin	☑

TIP Select nodes for configuration

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.
About Oracle Applications Manager Version 2.3.1

Step 5 The forms listener servlet parameters are exposed. The default forms servlet URL is provided, modify it only if necessary. Verify the **s_forms_servlet_comment** is blank to enable the service or place a **#** in the field to disable the forms listener servlet.



Forms Listener Servlet:Enable:Parameters(1)

Title	Parameter Name	Value	Description
Forms Servlet URL	s_forms_servlet_serverurl	/forms/formservlet	Forms Servlet URL
Forms Servlet Comment	s_forms_servlet_comment		Forms Servlet Comment

TIP It is recommended that this E-Business Suite 11i instance is also configured with a) HTTP Load balancing that supports client session-persistent connections, or b) Jserv Load balancing is enabled. Otherwise, the Forms requests will not be load-balanced across multiple Forms nodes.

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.
About Oracle Applications Manager Version 2.3.1

Step 6 At this point, a series of validation and confirmation panels will be displayed. After successfully completing these steps, basic load-balancing configurations will be saved on the context-files of each server node selected.

Step 7 Stop all currently running Oracle applications using the **adstpall** script on each impacted node.

Step 8 Run the **adautocfg** script on each node.

Step 9 Start all the server nodes using the **adstrtall** script.

⚠ **Caution** Do not stop the database because each node requires access to the database server during this process.

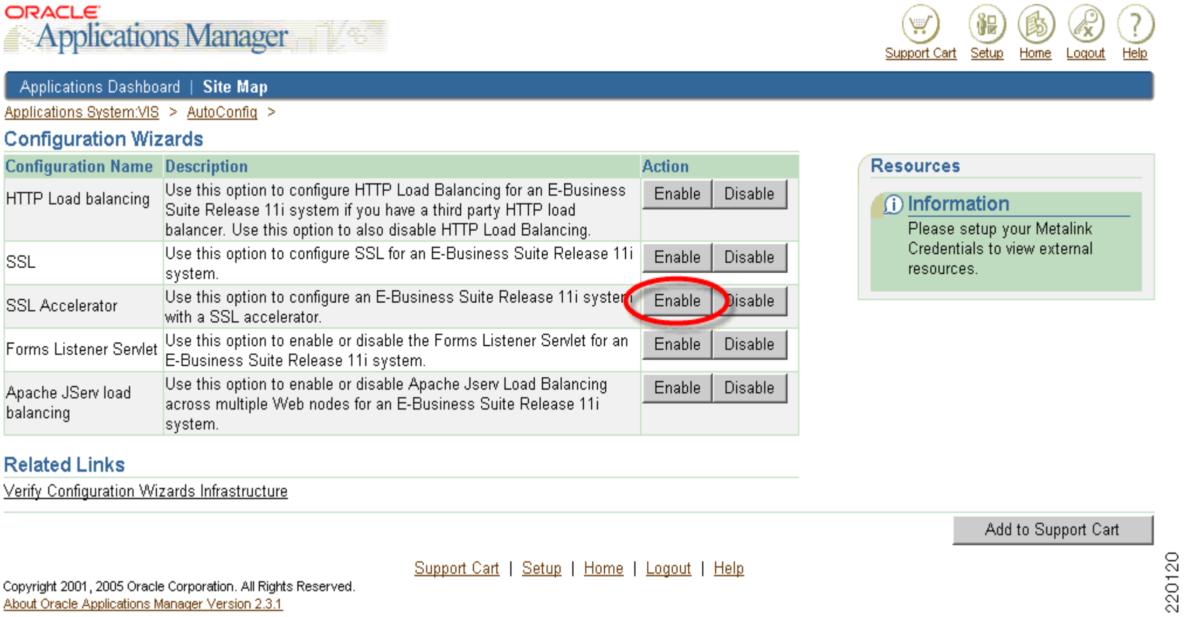
SSL Accelerator

The SSL Accelerator wizard configures the Oracle 11i environment to use an external device for encryption services and server offload. The following steps summarize how to enable SSL acceleration in the E-Business Suite:

Step 1 Login to the OAM and select the **Site Map—System Administration** tab, then select **AutoConfig** (see Figure 17).

Step 2 Select **Launch Wizards**.

Step 3 Click the **Enable SSL Accelerator** button.


ORACLE
Applications Manager
Support Cart
Setup
Home
Logout
Help
Applications Dashboard | Site Map
Applications System:VIS > AutoConfig >
Add to Support Cart
Support Cart | Setup | Home | Logout | Help
220120

Configuration Wizards

Configuration Name	Description	Action
HTTP Load balancing	Use this option to configure HTTP Load Balancing for an E-Business Suite Release 11i system if you have a third party HTTP load balancer. Use this option to also disable HTTP Load Balancing.	Enable Disable
SSL	Use this option to configure SSL for an E-Business Suite Release 11i system.	Enable Disable
SSL Accelerator	Use this option to configure an E-Business Suite Release 11i system with a SSL accelerator.	Enable Disable
Forms Listener Servlet	Use this option to enable or disable the Forms Listener Servlet for an E-Business Suite Release 11i system.	Enable Disable
Apache JServ load balancing	Use this option to enable or disable Apache Jserv Load Balancing across multiple Web nodes for an E-Business Suite Release 11i system.	Enable Disable

Resources

Information

Please setup your Metalink Credentials to view external resources.

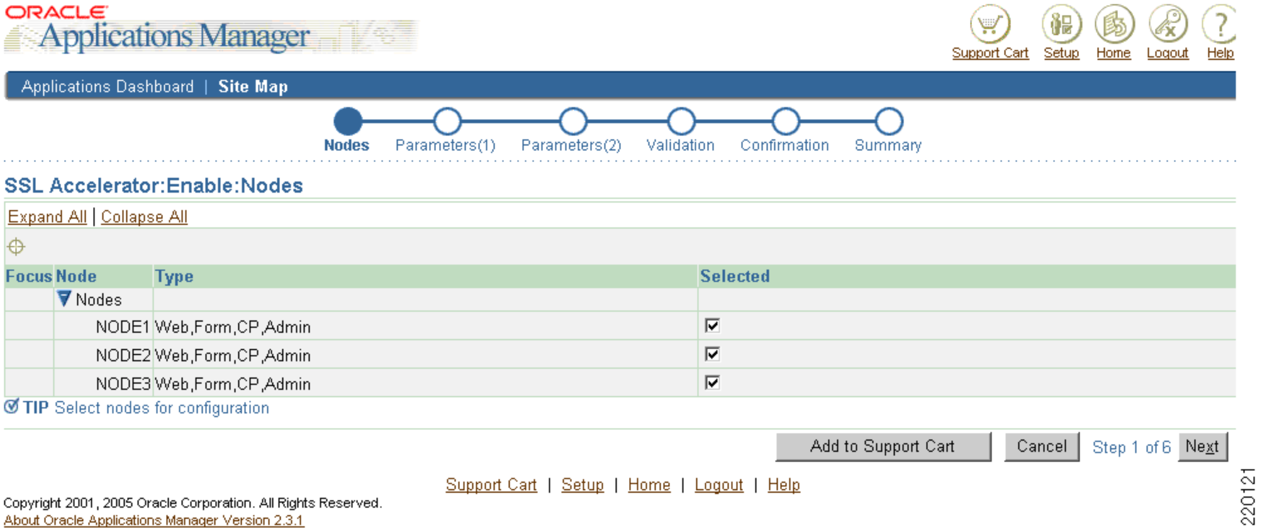
Related Links

Verify Configuration Wizards Infrastructure

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.

About Oracle Applications Manager Version 2.3.1

Step 4 Select the nodes using the SSL accelerators service.



SSL Accelerator:Enable:Nodes

Expand All | Collapse All

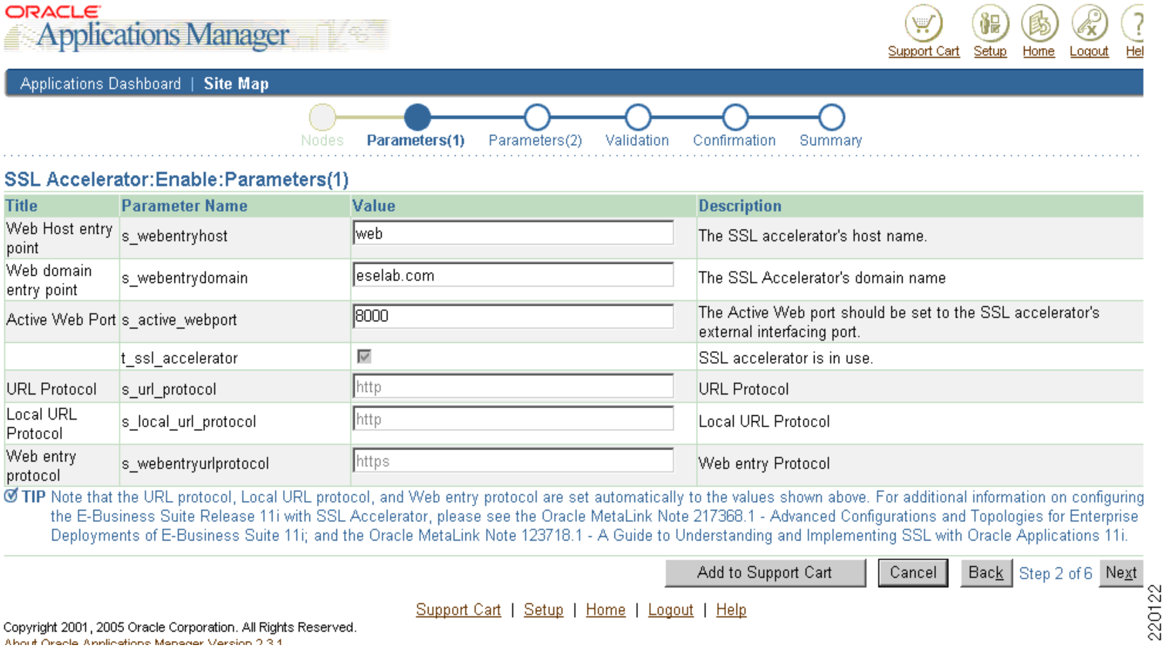
Focus	Node	Type	Selected
	▼ Nodes		
	NODE1	Web,Form,CP,Admin	☑
	NODE2	Web,Form,CP,Admin	☑
	NODE3	Web,Form,CP,Admin	☑

TIP Select nodes for configuration

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.
About Oracle Applications Manager Version 2.3.1

Step 5 Provide the information necessary for the Oracle applications to create well-formed URLs:

- s_webentryhost—DNS name of the ACE VIP used by clients
- s_webentrydomain—Domain name associated with the VIP
- Active Web Port s_active_webport—By default this value is 8000; change this to a value of your choice or use 443, which is the well known HTTPS port value



SSL Accelerator:Enable:Parameters(1)

Title	Parameter Name	Value	Description
Web Host entry point	s_webentryhost	web	The SSL accelerator's host name.
Web domain entry point	s_webentrydomain	eselab.com	The SSL Accelerator's domain name
Active Web Port	s_active_webport	8000	The Active Web port should be set to the SSL accelerator's external interfacing port.
	t_ssl_accelerator	☑	SSL accelerator is in use.
URL Protocol	s_url_protocol	http	URL Protocol
Local URL Protocol	s_local_url_protocol	http	Local URL Protocol
Web entry protocol	s_webentryurlprotocol	https	Web entry Protocol

TIP Note that the URL protocol, Local URL protocol, and Web entry protocol are set automatically to the values shown above. For additional information on configuring the E-Business Suite Release 11i with SSL Accelerator, please see the Oracle MetaLink Note 217368.1 - Advanced Configurations and Topologies for Enterprise Deployments of E-Business Suite 11i; and the Oracle MetaLink Note 123718.1 - A Guide to Understanding and Implementing SSL with Oracle Applications 11i.

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.
About Oracle Applications Manager Version 2.3.1

Step 6 At this point, a series of validation and confirmation panels will be displayed. After successfully completing these steps, basic load-balancing configurations will be saved on the context-files of each server node selected.

Step 7 Stop all currently running Oracle applications using the **adstpall** script on each impacted node.

Step 8 Run the **adautocfg** script on each node.

Step 9 Start all the server nodes using the **adstrtall** script.

Caution Do not stop the database because each node requires access to the database server during this process.

Cookie and Session Persistence

Cookies are pieces of data set by web servers to maintain information regarding the user and their unique session. A web browser configured to accept cookies will resend all cookies associated with a cookie-enabled website on each subsequent request. This behavior allows the ACE to use the cookie data to provide session persistence. The ACE module is capable of using server generated or ACE generated cookies to provide connection sticky. Table 1 shows the HTTP headers for the initial login page of the testbed's Oracle E-Business website. The **Set-Cookie** command, shown in the following example, has been introduced by the ACE virtual context; succeeding HTTP requests from a cookie-enabled web browser will include this data and any additional cookies associated with the website. The ACE module will maintain a sticky table and will return the client to the same APPL_TOP server based on this cookie.

```
GET /OA_HTML/AppsLocalLogin.jsp HTTP/1.1
Accept: */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: web.eselab.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Set-Cookie: acecookie=R193696788; path=/; expires=Wed, 18-Oct-2006 03:47:09 GMT
Date: Tue, 17 Oct 2006 03:36:40 GMT
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Keep-Alive: timeout=15
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

GET /OA_HTML/cabo/styles/cache/oracle-desktop-2_2_18-en-ie-6-windows.css HTTP/1.1
Accept: */*
Referer: http://web.eselab.com/OA_HTML/AppsLocalLogin.jsp
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: web.eselab.com
Connection: Keep-Alive
Cookie: acecookie=R193696788
```

Network Configuration Examples

This section contains the network configurations for the Catalyst 6500 MSFC, ACE, and FWSM that supported the Oracle 11i application and database during testing.This section documents unrestricted security access control lists (ACLs). These lists should be modified prior to implementing in a production environment, creating specifc access control entry statments for acceptable traffic flows between clients and tiers. The ACE and FWSM each have this capability.

Catalyst 6500 MSFC

This section contains the network configurations for the Catalyst 6500 MSFC.

Primary Aggregation Switch

Allow the ACE and FWSM access to the relevant VLANs:

```
firewall multiple-vlan-interfaces
firewall module 8 vlan-group 3,20,77,146,220
svclc multiple-vlan-interfaces
svclc module 13 vlan-group 1,146,220,320
svclc vlan-group 1  5,13
svclc vlan-group 3  30,330
svclc vlan-group 20  20
svclc vlan-group 77  77
svclc vlan-group 146  146
svclc vlan-group 220  220
svclc vlan-group 320  320
```

Configure the inter-switch link (ISL) between aggregation switches. This link can carry fault tolerant and production VLANs or this traffic can be divided across multiple ISLs. The primary goal of the ISL is to provide path redundancy in the data center.

```
interface Port-channel6
 description <<** ISL between dc01agg Ten12/3 - 4  **>>
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,13,14,20,30,77,220,320,330
 switchport mode trunk
 no ip address
 logging event link-status
 logging event spanning-tree status
 logging event bundle-status
 logging event trunk-status
 load-interval 30
```

Use HSRP for high availability of the server's default gateway. This is the one-arm mode ACE SVI configuration:

```
interface Vlan5
 description <<** ACE OneArm VLAN **>>
 ip address 10.5.1.2 255.255.0.0
 no ip redirects
 no ip proxy-arp
 logging event link-status
 load-interval 30
 standby 1 ip 10.5.1.1
 standby 1 timers 1 3
 standby 1 priority 51
 standby 1 preempt delay minimum 120
 standby 1 name ace
!
```

The following example shows the ACE transparent mode SVI as the default gateway for the application servers:

```
interface Vlan320
 description <<** App Server DGW **>>
 ip address 10.20.1.2 255.255.0.0
 no ip redirects
 no ip proxy-arp
 ip route-cache flow
 logging event link-status
 load-interval 30
 standby 1 ip 10.20.1.1
 standby 1 timers 1 3
 standby 1 priority 51
 standby 1 preempt delay minimum 120
 standby 1 name app
!
interface Vlan330
 description <<** DB Server DGW **>>
 ip address 10.30.1.2 255.255.0.0
 no ip redirects
 no ip proxy-arp
 ip route-cache flow
 logging event link-status
 load-interval 30
 standby 1 ip 10.30.1.1
 standby 1 timers 1 3
 standby 1 priority 51
 standby 1 preempt delay minimum 120
 standby 1 name db
```

Secondary Aggregation Switch

The secondary aggregation switch configuration is nearly a mirror image of the primary aggregation switch, and provides a highly available and predictable Layer 2 and 3 environment, while simultaneously allowing the integration of services.

```
firewall multiple-vlan-interfaces
firewall module 8 vlan-group 3,20,77,146,220
svclc multiple-vlan-interfaces
svclc module 13 vlan-group 1,146,220,320
svclc vlan-group 1  5,13
svclc vlan-group 3  30,330
svclc vlan-group 20  20
svclc vlan-group 77  77
svclc vlan-group 146  146
svclc vlan-group 220  220
svclc vlan-group 320  320
interface Port-channel6
 description <<** ISL between dc03agg Ten12/3 - 4  **>>
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 5,13,14,20,30,77,220,320,330
 switchport mode trunk
 no ip address
 logging event link-status
 logging event spanning-tree status
 logging event bundle-status
 logging event trunk-status
 load-interval 30
!
interface Vlan5
 description <<** ACE OneArm VLAN **>>
 ip address 10.5.1.3 255.255.0.0
 no ip redirects
 no ip proxy-arp
 logging event link-status
 load-interval 30
 standby 1 ip 10.5.1.1
 standby 1 timers 1 3
 standby 1 priority 50
 standby 1 preempt
 standby 1 name ace
!
interface Vlan320
 description <<** App Server DGW **>>
 ip address 10.20.1.3 255.255.0.0
 no ip redirects
 no ip proxy-arp
 logging event link-status
 load-interval 30
 standby 1 ip 10.20.1.1
 standby 1 timers 1 3
 standby 1 priority 50
 standby 1 preempt
 standby 1 name app
!
interface Vlan330
 description <<** DB Server DGW **>>
 ip address 10.30.1.3 255.255.0.0
 no ip redirects
 no ip proxy-arp
 logging event link-status
 load-interval 30
 standby 1 ip 10.30.1.1
 standby 1 timers 1 3
 standby 1 priority 50
 standby 1 preempt
 standby 1 name db
!
```

ACE Administrative Configuration

The following example shows the configuration for the ACE Admin server:

```
dc03-ace/Admin# show run
Generating configuration....


login timeout 0
hostname dc03-ace
boot system image:c6ace-t1k9-mz.3.0.0_A1_2.bin

resource-class onearm
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource conc-connections minimum 20.00 maximum equal-to-min
  limit-resource rate connection minimum 20.00 maximum equal-to-min
  limit-resource sticky minimum 20.00 maximum equal-to-min
resource-class transparent
```

```
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource conc-connections minimum 20.00 maximum equal-to-min
  limit-resource rate connection minimum 20.00 maximum equal-to-min
  limit-resource sticky minimum 20.00 maximum equal-to-min

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 REMOTE_ACCESS
  10 match protocol telnet any
  20 match protocol ssh any
  30 match protocol icmp any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
  class REMOTE_ACCESS
    permit

interface vlan 146
  description Management Address
  ip address 172.xx.xx.xx 255.255.254.0
  peer ip address 172.xx.xx.xx 255.255.254.0
  access-group input EVERYONE
  access-group output EVERYONE
  service-policy input REMOTE_MGMT_ALLOW_POLICY
  no shutdown

ft interface vlan 13
  ip address 13.13.13.1 255.255.255.0
  peer ip address 13.13.13.2 255.255.255.0
  no shutdown

ft peer 1
  heartbeat interval 200
  heartbeat count 10
  ft-interface vlan 13
ft group 1
  peer 1
  priority 150
  peer priority 110
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 172.26.146.1

context onearm
  description Context for 1-Arm Testing
  allocate-interface vlan 5
  member onearm
context transparent
  description Context for Transparent Testing
  allocate-interface vlan 220
  allocate-interface vlan 320
  member transparent

ft group 2
  peer 1
  priority 150
  peer priority 110
  associate-context onearm
  inservice
ft group 3
  peer 1
  priority 150
  peer priority 110
  associate-context transparent
  inservice
username admin password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/  role Admin domain
default-domain
username www password 5 $1$UZIiwUk7$QMVYN1JASaycabrHkhGcS/  role Admin domain
default-domain
```

ACE One-Arm Mode Configuration

The following example shows the configuration for one-arm mode:

```
ace/onearm# show run
Generating configuration....

logging enable
logging standby
logging buffered 6

crypto csr-params testparams
  country US
  state California
  locality SJ
  organization-name ESE-AS
  organization-unit Ch-US
  common-name web.eselab.com
  serial-number cisco123

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

probe http web
  port 8000
  interval 5
  faildetect 15
  passdetect interval 15
  receive 2
  expect status 200 200
  open 2

parameter-map type ssl sslparams
  cipher RSA_WITH_RC4_128_MD5
  version SSL3

rserver host node1
  ip address 10.20.1.101
  inservice
rserver host node2
  ip address 10.20.1.102
  inservice
rserver host node3
  ip address 10.20.1.103
  inservice

ssl-proxy service testssl
  key test.key
  cert testcert.pem
  ssl advanced-options sslparams

serverfarm host WEB
  probe web
  rserver node1 8000
```

```
    inservice
  rserver node2 8000
    inservice
  rserver node3 8000
    inservice

sticky ip-netmask 255.255.255.255 address source sticky-src-ip
  timeout 10
  replicate sticky
  serverfarm WEB
sticky http-cookie acecookie sticky-cookie-insert
  cookie insert
  replicate sticky
  serverfarm WEB

class-map match-all ACL
  2 match access-list EVERYONE
class-map match-all VIP-APP-100
  2 match virtual-address 10.99.10.100 tcp eq 9000
class-map match-all VIP-SSL-99
  2 match virtual-address 10.99.10.99 tcp eq https
class-map match-all VIP-WEB-99
  2 match virtual-address 10.99.10.99 tcp eq www
class-map type management match-any remote-mgmt
  10 match protocol ssh any
  20 match protocol telnet any
  30 match protocol icmp any
  40 match protocol http any
  50 match protocol https any
class-map match-any server-initiated
  2 match source-address 10.20.0.0 255.255.0.0
class-map match-any test
  2 match virtual-address 0.0.0.0 0.0.0.0 any

policy-map type management first-match remote-access
  class remote-mgmt
    permit
policy-map type loadbalance first-match vip-pol-99
  class class-default
    sticky-serverfarm sticky-cookie-insert
policy-map type loadbalance first-match vip-pol-SSL-99
  class class-default
    sticky-serverfarm sticky-src-ip
policy-map multi-match lb-vip
  class VIP-WEB-99
    loadbalance vip inservice
    loadbalance policy vip-pol-99
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 5
  class VIP-SSL-99
    loadbalance vip inservice
    loadbalance policy vip-pol-SSL-99
    loadbalance vip icmp-reply
    ssl-proxy server testssl
policy-map multi-match server-side
  class server-initiated
    nat dynamic 1 vlan 5

interface vlan 5
  ip address 10.5.1.4 255.255.255.0
  alias 10.5.1.6 255.255.255.0
  peer ip address 10.5.1.5 255.255.255.0
  access-group input EVERYONE
  nat-pool 1 10.5.1.10 10.5.1.20 netmask 255.255.255.0 pat
  service-policy input remote-access
  service-policy input lb-vip
  service-policy input server-side
  no shutdown

ip route 0.0.0.0 0.0.0.0 10.5.1.1
```

ACE Transparent Mode Configuration

The following example shows the configuration for ACE transparent mode:

```
dc03-ace/transparent# show run
Generating configuration....

logging enable
logging standby
logging buffered 6

crypto csr-params testparams
  country US
  state California
  locality SJ
  organization-name ESE-AS
  organization-unit Ch-US
  common-name web.eselab.com
  serial-number cisco123
access-list BPDU ethertype permit bpdu

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

probe http web
  port 8000
  interval 5
  faildetect 15
  passdetect interval 15
  receive 2
  expect status 200 200
  open 2

parameter-map type ssl sslparams
  cipher RSA_WITH_RC4_128_MD5
  version SSL3

rserver host node1
  ip address 10.20.1.101
  inservice
rserver host node2
  ip address 10.20.1.102
  inservice
rserver host node3
  ip address 10.20.1.103
  inservice

ssl-proxy service testssl
  ssl advanced-options sslparams

serverfarm host WEB
  probe web
  rserver node1 8000
    inservice
  rserver node2 8000
```

```
    inservice
  rserver node3 8000
    inservice

sticky ip-netmask 255.255.255.255 address source sticky-src-ip
  timeout 10
  replicate sticky
  serverfarm WEB
sticky http-cookie acecookie sticky-cookie-insert
  cookie insert
  replicate sticky
  serverfarm WEB

class-map match-all ACL
  2 match access-list EVERYONE
class-map match-all AppVIP
  description class-map for appltop loadbalancing
  10 match virtual-address 10.20.100.100 tcp eq www
class-map type management match-any remote-mgmt
  10 match protocol ssh any
  20 match protocol telnet any
  30 match protocol icmp any
  40 match protocol http any
  50 match protocol https any
class-map match-all server-initiated
  description NAT Server Initiated Connections to the VIP
  2 match source-address 10.20.0.0 255.255.0.0
  3 match destination-address 10.20.100.100 255.255.255.255

policy-map type management first-match remote-access
  class remote-mgmt
    permit
policy-map type loadbalance first-match VIP-POL-100
  class class-default
    sticky-serverfarm sticky-cookie-insert
policy-map multi-match SLB_WEB
  class server-initiated
    nat dynamic 1 vlan 220
  class AppVIP
    loadbalance vip inservice
    loadbalance policy VIP-POL-100
    loadbalance vip icmp-reply

interface vlan 220
  description South Side Server VLAN
  bridge-group 1
  access-group input BPDU
  access-group input EVERYONE
  nat-pool 1 10.20.254.250 10.20.254.254 netmask 255.255.255.0 pat
  service-policy input remote-access
  service-policy input SLB_WEB
  no shutdown
interface vlan 320
  description North Side ACE VLAN
  bridge-group 1
  access-group input BPDU
  access-group input EVERYONE
  service-policy input remote-access
  service-policy input SLB_WEB
  no shutdown

interface bvi 1
  ip address 10.20.1.5 255.255.0.0
  alias 10.20.1.7 255.255.0.0
  peer ip address 10.20.1.6 255.255.0.0
  no shutdown

ip route 0.0.0.0 0.0.0.0 10.20.1.1
```

FWSM Administrative Configuration (Admin Context)

The following example shows the configuration for the FWSM:

```
FWSM(config)# show run
: Saved
:
FWSM Version 3.1(1) <system>
!
resource acl-partition 12
hostname FWSM
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
!
interface Vlan20
 description APPL_TOP VLAN
!
interface Vlan30
 description DATABASE VLAN
!
interface Vlan77
 description LAN/STATE Failover Interface
!
interface Vlan146
 description MGMT VLAN
!
interface Vlan220
 description APPL_TOP Bridge VLAN
!
interface Vlan330
 description DATABASE Bridge VLAN
!
passwd 2KFQnbNIdI.2KYOU encrypted
class default
  limit-resource ASDM 5
  limit-resource IPSec 5
  limit-resource Mac-addresses 65535
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource All 0
!

ftp mode passive
pager lines 30
failover
failover lan unit secondary
failover lan interface fover Vlan77
failover polltime unit msec 500 holdtime 3
failover polltime interface 3
failover interface-policy 1%
failover replication http
failover link fover Vlan77
failover interface ip fover 10.77.1.1 255.255.0.0 standby 10.77.1.2
asdm history enable
arp timeout 14400
username admin password e1z89R3cZe9Kt6Ib encrypted
console timeout 0
```

```
admin-context admin
context admin
  allocate-interface Vlan146 int1
  config-url disk:/admin.cfg
!

context appltop
  description <<** Bridge VLAN 220 - 20 (11i APPL_TOP)  **>>
  allocate-interface Vlan20
  allocate-interface Vlan220
  config-url disk:/tp220-20.cfg
!

context db
  description <<** Bridge VLAN 330 - 30 (11i DB)  **>>
  allocate-interface Vlan30
  allocate-interface Vlan330
  config-url disk:/tp330-30.cfg
!

prompt hostname context
Cryptochecksum:2f7216a14c3b94aeb334b38cf19e7b9b
: end
```

FWSM Transparent Mode Configuration (Database Context)

The following example shows the configuration for the FWSM in transparent mode:

```
FWSM/db(config)# show run
: Saved
:
FWSM Version 3.1(1) <context>
!
firewall transparent
hostname db
domain-name eselab.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan30
 nameif inside
 bridge-group 1
 security-level 100
!
interface Vlan330
 nameif outside
 bridge-group 1
 security-level 0
!
interface BVI1
 ip address 10.30.1.4 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list outside extended permit ip any any log
access-list inside extended permit ip any any log
access-list BPDU ethertype permit bpdu
pager lines 35
logging enable
logging timestamp
logging buffered informational
logging trap informational
logging asdm informational
logging queue 0
logging device-id hostname
mtu outside 1500
mtu inside 1500
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400
access-group BPDU in interface outside
access-group outside in interface outside
access-group BPDU in interface inside
access-group inside in interface inside
route outside 0.0.0.0 0.0.0.0 10.30.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 360
ssh timeout 5
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect smtp
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect sqlnet
!
service-policy global_policy global
Cryptochecksum:c74e5affba450ceb83052cf618bf7996
: end
```

FWSM Transparent Mode Configuration (APPL_TOP Context)

The following example shows the configuration for the FWSM APPL_TOP context:

```
FWSM/appltop(config)# show run
: Saved
:
FWSM Version 3.1(1) <context>
!
firewall transparent
hostname appltop
domain-name eselab.com
enable password 2KFQnbNIdI.2KYOU encrypted
```

```
names
!
interface Vlan220
 nameif outside
 bridge-group 1
 security-level 0
!
interface Vlan20
 nameif inside
 bridge-group 1
 security-level 100
!
interface BVI1
 ip address 10.20.1.4 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list outside extended permit ip any any log
access-list inside extended permit ip any any log
access-list BPDU ethertype permit bpdu
pager lines 24
logging enable
logging timestamp
logging buffered informational
logging trap informational
logging asdm informational
logging queue 0
logging device-id hostname
mtu outside 1500
mtu inside 1500
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400
access-group BPDU in interface outside
access-group outside in interface outside
access-group BPDU in interface inside
access-group inside in interface inside
route outside 0.0.0.0 0.0.0.0 10.20.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect smtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
Cryptochecksum:822088e52ddf41626a20bf206a13b80c
: end
```

Appendix

Table 1 lists the default port values for the Oracle E-Business Suite 11i 10.5.2 used for testing. These port values can be referenced to create security policies on both the ACE and the FWSM.

Table 1 Default Port Values for Oracle 11i Environment

Description	Port Values
Database port	1521
RPC port	1626
Reports port	7000
Web listener port	8000
OProcMgr port	8100
Web PLSQL port	8200
Servlet port	8800
Forms listener port	9000
Metrics server data port	9100
JTF fulfillment server port	9200
Map Viewer Servlet port	9800
OEM web utility port	10000
VisBroker OrbServer Agent port	10100
MSCA server port	10200
MSCA dispatcher port	10300
Java object cache port	12345
OACORE servlet port	16000–16009
Discoverer servlet port	17000–17009
Forms servlet port	18000–18009
XMLSVCS servlet port	19000–19009

Note For more information about the terms listed in Table 1, refer to the following URLs:
www.oracle.com
www.cisco.com

References

This section provides additional references.

- See the ACE documentation at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/ace/ace_301/index.htm
- See the FWSM documentation at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/fwsm/index.htm
- Oracle Metalink document ID 233428.1: "Sharing the Application Tier File System in Oracle Applications 11i."
- Oracle Metalink document ID 217368.1: "Advanced Configurations and Topologies for Enterprise Deployments of E-Business Suite 11i"
- Oracle Metalink document ID 233428.1: "Using Forms Listener Servlet with Oracle Applications 11i"
- Oracle Applications 11i (11.5.10.2) Documentation Library: http://download-east.oracle.com/docs/cd/B25516_08/current/html/docset.html

Glossary

Table 2 provides some of the key terms that are used in this document

Table 2 Glossary

Term	Definition
Cisco Application Control Engine (ACE)	The Cisco Application Control Engine is a module within the Catalyst 6500 Series switch that allows applications resources to be distributed and managed via logical groups within a given physical platform. The ACE also provides high levels of Layer 4-7 performance (16 Gpbs and 345,000 connections per second) to optimize application performance and provide scalability. For more information on the ACE service module refer to the following URL: http://www.cisco.com/en/US/products/ps6906/index.html
Cisco Firewall Services Module (FWSM)	The Cisco Firewall Services Module (FWSM) is a high-speed, integrated firewall module for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers, and provides the fastest firewall data rates in the industry: 5-Gbps throughput, 100,000 CPS, and 1M concurrent connections. Up to four FWSMs can be installed in a single chassis, providing scalability to 20 Gbps per chassis. For more information on the FWSM service module refer to the following URL: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html
Forms listener servlet	A Java servlet that allows Oracle Forms applications to run over HTTP and HTTPS connections.
MSFC Forms Server	Multilayer Switch Feature Card for the Catalyst 6500 platform. The forms server hosts the Oracle Applications forms and associated runtime engine that support the professional interface.
Service	A group of processes running on a single machine that provides a particular function, such as an HTTP service.
Tier	A grouping of services, potentially across physical machines. A tier represents a logical grouping and can be represented by multiple network segments (subnets) with a particular application running (on multiple physical machines) deployed in each subnet, or multiple applications can be merged into a single network segment.
Transparent Mode	Term describing a network device that is bridging traffic between two different Layer 2 segments.
Transparent Network Substrate (TNS)	TNS provides connectivity between the Oracle application layer and the Oracle database layer. This is commonly referred to as the SQL*Net protocol. The default port value is 1521.
Web server	Oracle HTTP server powered by Apache.