24.09.2004

Реализация IT-инфраструктуры корпорации/предприятия на базе программных продуктов компании Oracle. Анализ управления безопасностью (Oracle Identity Management Architecture и Oracle Database Security) для безопасной архитектуры Oracle и ее компонентов.

Базовые подходы и задачи

Все программное обеспечение компании Oracle, включая специализированные модули и опции реализующие безопасную инфраструктуру и управление, а также базовые компоненты платформы создавались таким образом, чтобы быть способными решать следующие задачи:

a) Быть максимально независимыми от аппаратной реализации глобальной инфраструктуры компании, и тем самым не ограничивать потребителя в выборе аппаратной платформы.
b) Обеспечивать максимальную гибкость в приспособлении к аппаратной платформе и в предоставлении необходимого безопасного уровня доступа не только к приложениям, но и, фактически, ресурсам самой системы, какими прежде всего являются компоненты сервера приложений, сервер базы данных с опциями и Oracle Grid Control, обеспечивая широчайший диапазон в создании совершенно различных программно-аппаратных систем (Подразумевается, что и сервера приложений, и сервера RDBMS, подключаемые к системе, являясь продуктами других компаний, могут интегрироваться в общую корпоративную инфраструктуру).
c) Управляться в условиях необходимости динамического перераспределения ресурсов между приложениями и компонентами системы, подчиняясь концепции Oracle Grid.

Все эти задачи потребовали проработки проблем безопасности фактически на всех уровнях системы: в клиентской части, на уровне MiddleTier, на уровне Data Layer. Помимо этого были разработаны подходы, конкретные имплементации и паттерны для создания и написания безопасных приложений, а также их интеграция в общую инфраструктуру компании.

Базовые положения и вводное рассмотрение вопросов, связанных с вопросами защиты корпоративной инфраструктуры можно найти в следующих руководствах компании:

1.) **Oracle® Database Advanced Security Administrator's Guide**
10*g* Release 1 (10.1) Part Number B10772-01
2.) **Oracle® Database Heterogeneous Connectivity Administrator's Guide**
10*g* Release 1 (10.1) Part Number B10764-01
3.) **Oracle® High Availability Architecture and Best Practices**
10*g* Release 1 (10.1) Part Number B10726-01
4.) **Oracle® Label Security Administrator's Guide**
10*g* Release 1 (10.1) Part Number B10774-01
5.) **Oracle® Database Net Services Administrator's Guide**
10*g* Release 1 (10.1) Part Number B10775-01
6.) **Oracle® Database Security Guide**
10*g* Release 1 (10.1) Part Number B10773-01
7.) **Oracle® Security Overview**
10*g* Release 1 (10.1) Part Number B10777-01
8.) **Oracle Workflow Administrator's Guide**
Release 2.6.3 Part Number B10283-02
9.) **Oracle® Enterprise Manager Advanced Configuration**
10*g* Release 1 (10.1) Part Number B12013-01
10.) **Oracle® Database Administrator's Guide**
10*g* Release 1 (10.1) Part Number B10739-01
11.) **Oracle® Database Platform Guide**
10*g* Release 1 (10.1) for Windows Part Number B10113-01
12.) **Oracle® Application Server 10*g* Concepts**
10*g* (9.0.4) Part No. B10375-01
13.) **Oracle® Application Server 10*g* Administrator's Guide**
10*g* (9.0.4) Part Number B10376-01
14.) **Oracle® Application Server 10*g* Advanced Topologies for Enterprise Deployments 10*g* (9.0.4)** Part No. B12115-01
15.) **Oracle® Application Server 10*g* Security Guide**
10*g* (9.0.4) Part No. B10377-01
16.) **Oracle HTTP Server Administrator's Guide**
10*g* (9.0.4) Part Number B10381-01
17.) **Oracle® Application Server 10*g* mod_plsql User's Guide**
10*g* (9.0.4) Part Number B10357-01
18.) **Oracle® Application Server Web Services Developer's Guide**
10*g* (9.0.4) Part No. B10447-01
19.) **Oracle® Application Developer's Guide – XML**
10*g* (9.0.4) Part Number B12099-01
20.) **Oracle® Application Server Containers for J2EE Security Guide**
10*g* (9.0.4) Part Number B10325-02
21.) **Oracle® Application Server Portal Configuration Guide**
10*g* (9.0.4) Part Number B10356-01
22.) **Oracle® Application Server Syndication Services Developer's and Administrator's Guide 10*g* (9.0.4)** Part No. B10667-01
23.) **Oracle Application Server Wireless Administrator's Guide**
10*g* (9.0.4) Part Number B10188-01

24.) **Oracle Application Server Web Cache Administrator's Guide 10*g* (9.0.4)** Part Number B10401-01
25.) **Oracle Application Server Reports Services Publishing Reports to the Web 10*g* (9.0.4)** Part Number B10314-01
26.) **Oracle® Application Server ProcessConnect User's Guide 10*g* (9.0.4)** Part Number B12121-01
27.) **Oracle® Identity Management Concepts and Deployment Planning Guide 10*g* (9.0.4) for Windows or UNIX** Part No. B10660-01
28.) **Oracle® Internet Directory Administrator's Guide 10*g* (9.0.4)** Part Number B12118-01
29.) **Oracle® Internet Directory Application Developer's Guide 10*g* (9.0.4)** Part Number B10461-01
30.) **Oracle® Application Server Single Sign-On Administrator's Guide 10*g* (9.0.4)** Part Number B10851-01
31.) **Oracle® Application Server Single Sign-On Application Developer's Guide 10*g* (9.0.4)** Part Number B10852-01
32.) **Oracle® Application Server Certificate Authority Administrator's Guide 10*g* (9.0.4)** Part Number B10663-01

Вся созданная система безопасности для IT инфраструктуры базируется на общем интегрированном подходе к решению задачи системной безопасности.

Методологический подход Oracle к проблеме обеспечения защиты.

Этот раздел представляет краткий обзор требований к защите данных и рассматривает полный спектр рисков защиты данных. В результате короткого анализа показывается матрица отношений рисков защиты к видам технологий доступных сейчас у Oracle, используемым для реальной защиты данных.
Существует три основных мифа, касающихся защиты информационных систем:

- Миф 1: Хакеры вызывают большинство нарушений безопасности.

  Фактически, 80% потерь данных вызвано сотрудниками организаций.

- Миф 2: Кодирование и криптование данных полностью обеспечивает защиту Ваших данных.

  Фактически, кодирование данных это только один из подходов к обеспечению защиты данных. Защита также требует контроля доступа, соблюдения целостности данных, высокой готовности системы, аудита, разделенного режима доступа к профилям пользователей и данным авторизации, и т.д.

- Миф 3: Системы сетевой защиты, аппаратные средства и файерволы обеспечивают полную защиту Ваших данных.

  Фактически, 40% взломов в Интернет/Интранет системах происходят несмотря на систему сетевой защиты, находящуюся на том месте, где ей и положено быть.

В отличие от мифов, чтобы спроектировать реально работающее решение защиты, которое действительно защищает Ваши данные, вы должны определить необходимые требования к защите, уместные для вашей системы, и реально существующие угрозы для Ваших данных. Задача защиты данных является многомерной. В Интернет/Интранет-среде, риски потерь ценных и чувствительных данных стали больше, чем когда-либо прежде. На рис.1 представлена топология вычислительной среды, которую ваш план защиты данных должен обезопасить:

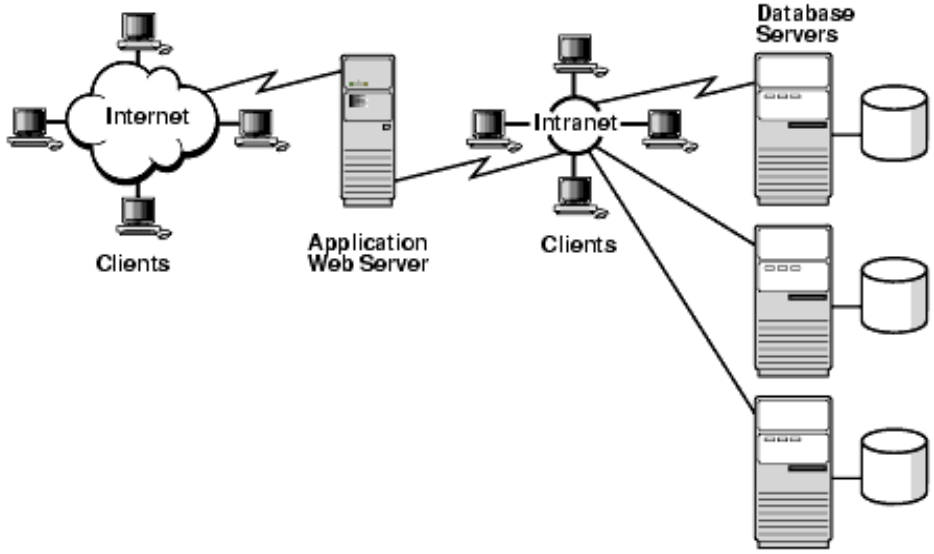


Рис. 1

Вы должны защитить базы данных и сервера приложений; Вы должны управлять и защитить права внутренних пользователей базы данных и пользователей приложений на серверах приложений; и Вы должны гарантировать конфиденциальность конечных клиентов, так как они обращаются к вашей базе данных и системе. С линейным увеличением пропускных способностей сетей и производительности систем в Интернет/Интранет угроза данным возрастает многократно. Чтобы защитить все элементы сложных вычислительных систем, вы должны обратиться к проблемам защиты во многих измерениях, как показано в Табл.1:

Измерение	Проблемы защиты
Физическое	Ваши компьютеры должны быть физически недоступны для несанкционированных пользователей.
Персональное	Люди, ответственные за администрирование системы и защиту данных, должны быть безусловно надежны.
Процедурное	Процедуры, используемые в операционном функционировании Вашей системы, должны гарантировать целостность и непротиворечивость данных. Удобное и сохранное обеспечение процедурного режима должно обеспечиваться самой системой.
Техническое	Память, доступ, манипуляции, и передача данных в системе должны базироваться на сохранной технологии, которая предписывает Вам специфические алгоритмы управления и распределения ресурсов в Вашей программно-аппаратной системе.

Табл. 1 Многомерность задачи безопасной IT-инфраструктуры

Решение проблемы только в техническом измерении, в чистом виде, к сожалению, не может обеспечить надежной защиты никакого программно-аппаратного комплекса, или компании. Любая технология должна гарантировать, как минимум три основных стандарта защиты для всех (!!!) компонентов системы:

- Конфиденциальность данных, состоящую из:
  1.) конфиденциальности связей компонентов системы и пользователей
  2.) безопасности общей памяти чувствительных данных (Как только секретные данные были введены, их целостность и конфиденциальность должны быть защищены в базах данных и серверах, где они постоянно находятся.
  3.) аутентификации пользователей

4.) дискретного гранулированного доступа к данным (сотруднику в отделе кадров возможно необходим доступ к данным о зарплате ряда сотрудников, но абсолютно не нужно видеть данные о зарплатах всех сотрудников компании)

- Целостность данных системы: Безопасная система гарантирует, что данные, которые она содержит, реальны и действительны. Целостность данных означает, что данные защищены от вычеркивания и искажения, как во время когда они постоянно находятся в пределах базы данных, так и, в то время когда они передаются по сети. Целостность данных включает несколько аспектов:
    1.) Системные и объектные привилегии доступа к прикладным таблицам и командам системы, организованные таким образом, что только зарегистрированные пользователи могут заменить данные.
    2.) Ссылочная целостность - способность поддерживать действительные взаимосвязи между значениями в базе данных, согласно правилам, которые были определены.
    3.) База данных должна быть защищена против вирусов, создаваемых, чтобы исказить данные, и любого несанкционированного доступа.
    4.) Сетевой траффик должен быть защищен от удаления, искажения, и, прослушивания.

- Высокая готовность системы: Безопасная система делает данные доступными к зарегистрированным пользователям, безотлагательно.

  К основным аспектам готовности системы относятся:

    1.) сопротивляемость системы к неправомерному воздействию и использованию ресурсов.
    2.) универсальность системы - Работа системы должна остаться адекватной к потреблению ресурсов, несмотря на число пользователей или процессов, требующих обслуживание.
    3.) гибкость системы - Администраторы должны иметь адекватное средство управления пользователями и ресурсами системы (желательно из общего виртуального и безопасного интерфейса, каким является, например, Oracle Grid Control).
    4.) нетрудоемкость в использовании и эксплуатации системы - реализация защиты непосредственно не должна уменьшить способность действительных пользователей осуществлять их работу и способность администраторов быстро и легко управлять системой.

К наиболее серьезным рискам защиты данных относятся следующие:

- Вмешательство в данные и их искажение
- Удаленное прослушивание данных и их воровство
- Фальсификация идентификации пользователя
- Угрозы, связанные с аутентификацией пользователя паролем
- Несанкционированный доступ к таблицам и столбцам базы данных
- Несанкционированный доступ к рядам данных
- Отсутствие ответственности пользователей в то время, когда администратор не в состоянии полностью проконтролировать их действия
- Сложные требования управления пользователями в больших масштабируемых системах (В таких больших средах, большое количество пользователей и паролей делает Вашу систему уязвимой к ошибке и нападению. Вам нужно знать, кем пользователь действительно является – отследить его через все компоненты приложения - чтобы иметь надежную защиту. Эта проблема становится особенно комплексной в системах с промежуточными слоями (multitiers). Здесь, и в самых упакованных приложениях, типичная модель систем - это коннекция к RDBMS одним прикладным пользователем. Пользователь соединяется с приложением на основе прикладных файлов регистрации и на их основе обеспечивает полный доступ для каждого, без ревизии предоставленных привилегий. Эта модель подвергает ваши данные риску - особенно в Интранет, где ваш веб-сервер и сервер приложений зависят от системы сетевой защиты. Системы сетевой защиты обычно уязвимы к взломам. В случае Oracle безопасной IT инфраструктуры это не совсем так, поскольку всегда в паре с системой сетевой защиты используется инертный к взлому инвертированный прокси кэширующий WWW-сервер - Oracle WebCache).
- Сложности администрирования программно-аппаратных реализаций и множественных систем инфраструктур IT с существенно разнородной структурой, как программной, так и прежде всего аппаратной реализацией. Единая прикладная инсталляция инфраструктуры IT должна управляться неким централизованным способом (как это реализовано в Oracle Grid).

Базируясь на анализе работы компонентов платформы Oracle и анализа работы самой платформы была построена матрица, связывающая риски защиты, решения и технологии их реализующие, которая представлена в Табл. 2 Данная матрица явилась основанием для создания целого комплекса архитектурных решений, на базе которого реализуется (или адаптируется уже существующая) безопасная инфраструктура IT. Учитывая, практическое отсутствие в архитектуре дорогостоящих аппаратных реализаций средств защиты – данная безопасная инфраструра IT практически не имеет конкурентов на рынке, работающих в том же ценовом диапазоне.

Проблема	Решение	Технология Защиты	Программы и Особенности Oracle
Несанкционированные пользователи	Знание своих пользователей	Идентификация	Пароли, управление паролированием Oracle Advanced Security Option: Лексемы, интеллектуальные карточки, e-tokens, Kerberos. PKI: Свидетельства X.509, SSL-certificates, Oracle Wallets, digests
Несанкционированный доступ к данным	Ограничение доступа к данным Динамическая модификация запроса Ограничение доступа к рядам данным и столбцам Кодирование данных Привилегии предела	Контроль доступа Прецизионный контроль доступа Контроль доступа по метке Криптование данных Управление привилегиями доступа	Virtual Private Database, SSL-certificates, Oracle Wallets, Sinlge-Sign-On, digests. Virtual Private Database Oracle Label Security Роли, Привилегии Secure Application Roles

			Enterprise Roles
Прослушивание и сниффинг сети	Защита сети	Сетевое кодирование данных	Oracle Advanced Security Option: Кодирование Socket Secure Layers
Искажение и повреждение данных в сети	Защита сети	Целостность данных	Oracle Advanced Security: Вычисление контрольной суммы PKI: Вычисление контрольной суммы (как часть SSL)
Отказ в обслуживании	Управление доступом к ресурсам	Высокая готовность	Параметры Пользователя, RAC's, кэширование
Сложность управления пользователями в больших системах	Ограничьте число паролей	Single-Sign-On Single-Sign-On + +SSL SSL	Oracle Advanced Security Option: Kerberos, DCE, Enterprise User Security Single-Sign-On Server: Основанный на WWW Single Sign-On Oracle Certification Authority
Сложность в администрировании для больших систем	Централизация управления	Enterprise User Security Oracle Grid	Oracle Advanced Security Option, Служба Directory Integration Oracle Internet Directory
Отсутствие ответственности пользователей	Контролируйте действия пользователей	Ревизия и проведения аудита	Стандартный Аудит, Прецизионный Аудит.
Чрезмерно широкое обращение к данным	Динамическая модификация запроса	Прецизионный контроль доступа	Virtual Private Database

	запроса	доступа	Oracle Label Security
Слишком много учетных записей и пользователей	Централизуйте управление	Служба каталогов, другие LDAP-службы каталогов	Oracle Internet Directory
Взлом операционной системы	Криптование чувствительных данные	Stored Data Encryption	Кодирование данных

Табл. 2 Матрица рисков защиты и решений

Исходя из задач и используемых решений, формируется группа защиты безопасной IT инфраструктуры. Унифицированный состав группы приводится в таблице 3.

Человек	Ответственность
Пользователь	Ответственный за использование системы для законных целей, защиту чувствительных данных, к которым она имеет доступ, и управление ее паролей безопасно.
Администратор Базы данных	Ответственный за создание и управление пользователей базы данных, предоставление системных и объектных привилегий, и назначение локальных ролей пользователям.
Администратор Сервера приложений	Ответственный за поддержание сервера приложений, его целостности на уровне Web/Business приложений и Java Persistency
Администратор Операционной Системы	Ответственный за поддержание основной защиты операционной системы.
Сетевой Администратор	Ответственный за обеспечение защиты данных в передаче.

Прикладные Администраторы	Ответственный за развертывание приложений таким образом, так, чтобы гарантировать защиту.
Доверенный Прикладной Администратор	Ответственный за создание и управление пользователей доверенных приложений, и их связанных привилегий.
Руководитель Предприятия Службы безопасности	Ответственный за поддержание защиты каталога, и для осуществления централизованной защиты пользователя предприятия.

Табл.3 Группа, обеспечивающая безопасность системы.

Рассмотрим кратко, в самом общем виде, уровни корпоративной системы по отдельности, а затем концепцию интегрированной безопасной IT инфраструктуры на базе продуктов компании Oracle.

Уровень корпоративной системы – Data Layer (Уровень базы данных и его окружение).

К существующим техническим решениям на данном уровне относятся:

- Защита данных внутри базы данных.

Простейший пример, способность пользователя использовать действительное имя пользователя и пароль может использоваться в качестве первого уровня уполномочивания для пользователя, чтобы обратиться к базе данных или определенным таблицам базы данных. Базовые методы, которые обычно используются для управления системой и объектными привилегиями:

1. Использование Ролей, чтобы управлять Привилегиями
2. Использование Сохраненных Процедур, чтобы управлять Привилегиями
3. Использование Сетевых Средств, чтобы управлять Привилегиями
4. Использование Представлений, чтобы управлять Привилегиями

На рис. 2, для примера, показан механизм использования Ролей:

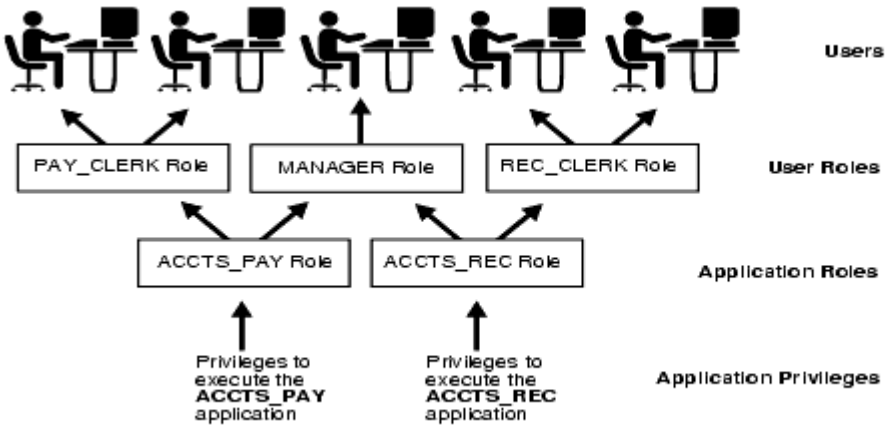


Рис.2

- Защита сетевого протокола и окружения базы.
- Аутентификация пользователей для доступа в базу данных.
- Использование и развертывание безопасного каталога.
- Администрирование уровня Enterprise User Security для доступа в базы данных.
- Аудит и мониторирование защиты системы для уровня Data Layer.
- Использование PKI (X.509), Virtual Private Database, Oracle Advanced Security Option, Oracle Label Security на уровне Data Layer.

За неимением возможности остановиться здесь более подробно на всех этих вопросах, лишь заметитм, что уровень проработки вопросов, связанных с безопасностью самой RDBMS и службы директорий, включая механизмы репликаций, кластеризации, кодирования, криптования данных, java security в базе данных, расширенных механизмов безопасности для Oracle RDBMS и его компонентов, а также Oracle Internet Directory разработан настолько гибко и хорошо, что представляется возможность настроить продукты на уровне Data Layer практически под любые нужды безопасной IT корпоративной системы.

Уровень корпоративной системы – MiddleTier (Уровень промежуточного слоя и приложений на нем работающих, реализация иерархических демилитаризованных зон, зон ограниченного доступа и систем сетевой защиты).

Общая архитектурная рекомендация - использовать известную и общепринятую Internet-Firewall-DMZ-Firewall-Intranet архитектуру, показанную на Рис. 3

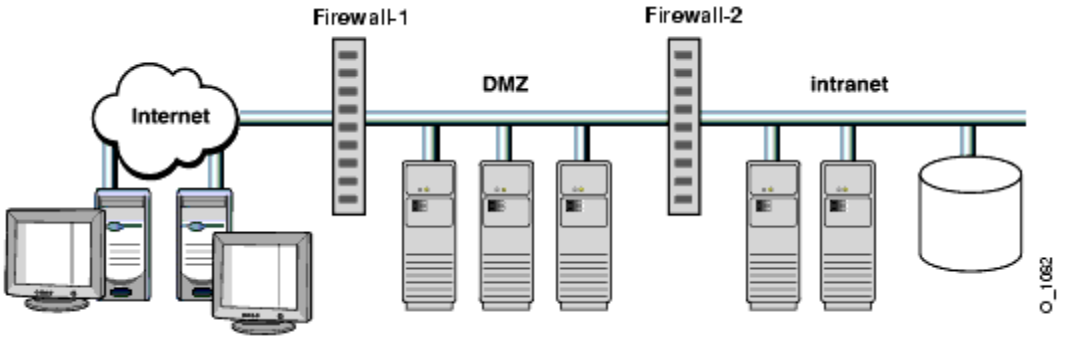


Рис.3

В архитектуре OAS 10G, ДЕМИЛИТАРИЗОВАННАЯ ЗОНА включает все зоны между Интернетом и внутренней сетью (множественность DMZ). Эти зоны отделены системами друг от друга системами сетевой защиты. На Рис. 4 представлена схема реальной имплементации среднего слоя (middletier) и data layer обеспечивающая безопасную инфраструктуру предприятия на основе платформы Oracle. В данной схеме мы рекомендуем, чтобы ваши зоны ДЕМИЛИТАРИЗОВАННОЙ ЗОНЫ удовлетворяли следующим критериям:

- Весь входящий траффик HTTP/HTTPS должен быть обработан WWW-серверами в зоне ДЕМИЛИТАРИЗОВАННОЙ ЗОНЫ, соединенной с Интернетом (или областью размещения клиентов). Поскольку прокси HTTP/HTTPS не полностью процессируют все запросы и не являются реальной защитой против атак типа cross-site scripting, directory traversal и ряда других атак, это означает, что все серверы HTTP/HTTPS должны постоянно находиться в этой зоне, которая названа Web Server Tier зоной. Если прямой доступ к службе директорий (Oracle Internet Directory) требуется от Интернет-клиентов (или от внешних к DMZ-зонам клиентов), то сервера службы директорий должны постоянно находиться в ДЕМИЛИТАРИЗОВАННОЙ ЗОНЕ тоже (в этом случае они реплицируются стандартным образом между DMZ-зонами).

- Сервера, на которых работают WWW- серверы не должны иметь прямого доступа к внутренней сети, если это возможно. WWW-сервера – это как минимум риск для вторжения из-за их сложности (включая и все прокси), потому что они первыми обрабатывают входящие сообщения, и, потому, что хакеры стремятся концентрировать усилия на этих серверах. В результате, мы рекомендуем применить дополнительную зону J2EE Business Logic DMZ, где OC4J (Oracle Containers for Java) только посылает запросы во внутреннюю зону. Здесь входящие сообщения сначала обрабатываются в зоне WWW-серверов, а затем пересылаются через

использование протокола AJP в зону J2EE для обработки. Процессы OC4J, возможно, тогда вызывают деловые базы данных во внутренней сети, использующей SQL*Net.

- Мы рекомендуем, чтобы процессоры, доступные от Интернета не были бы прикрепленными ко внутренней сети. Это обеспечивает сдерживание вторжения во времени. Сервера службы директорий нужно разместить в зоне DMZ Инфраструктуры, если они непосредственно не требуются для доступа к ним из Интернет. Приложения, которые обращаются к деловой базе данных, используя mod_plsql (Oracle AS Portal, например) в WWW-Сервере требуют прямой доступ к внутренней сети от серверов http/https. В данном случае, J2EE система сетевой защиты исключена, потому что требуется обращение к деловым данным, и система сетевой защиты должна быть сформирована, чтобы позволить использование траффика SQL*Net. В данных конфигурациях целесообразно выделять портал и кластера на его основе в отдельную DMZ. Исходя из смысла защиты системы, приемлемо для исходящего из внутренней сети траффика достижение всех внешних зон, исключая зону Internet (или область внешних клиентов) Это правило может использоваться для размещения всех компонентов. Например, для запуска Параллельного Механизма распараллеливания запросов к страницам Портала Oracle AS 10G, как сервлетный процесс на OC4J.
- При использовании Oracle Grid Control для больших конфигураций размещение его возможно производить в DMZ инфраструктуры, или других зонах, исключая зону Web Tier DMZ.
- Сама концепция реализации безопасной инфраструктуры IT компании Oracle подразумевает возможность использования элементов и компонент третьих рекомендуемых фирм-производителей (firewall'ы, аппаратные балансировщики, аппаратные акселераторы SSL, и т.д.) и, в смысле совместимости, не является такой закрытой, как продукты некоторых других компаний, что представляется предпочтительным в ее использовании для компаний, имеющих достаточно большой аппаратный парк, особенно учитывая, что платформа Oracle может работать на различных операционных системах.
- Взаимная синхронизация работы компонентов на уровне MiddleTier обеспечивается за счет размещения X.509 сертификатов и приватных ключей в контейнерах формата PKCS#12 (Oracle Wallets) по компонентам и генерации запросов на сертификаты согласно спецификации PKCS#10.

Помимо общих топологических схем, реально существуют оптимизированные варианты реализаций безопасной инфраструктуры для конкретных типов сервисов и приложений на промежуточном слое.

Например, на рис. 5 представлена схема для системы генерации отчетов Oracle Reports.

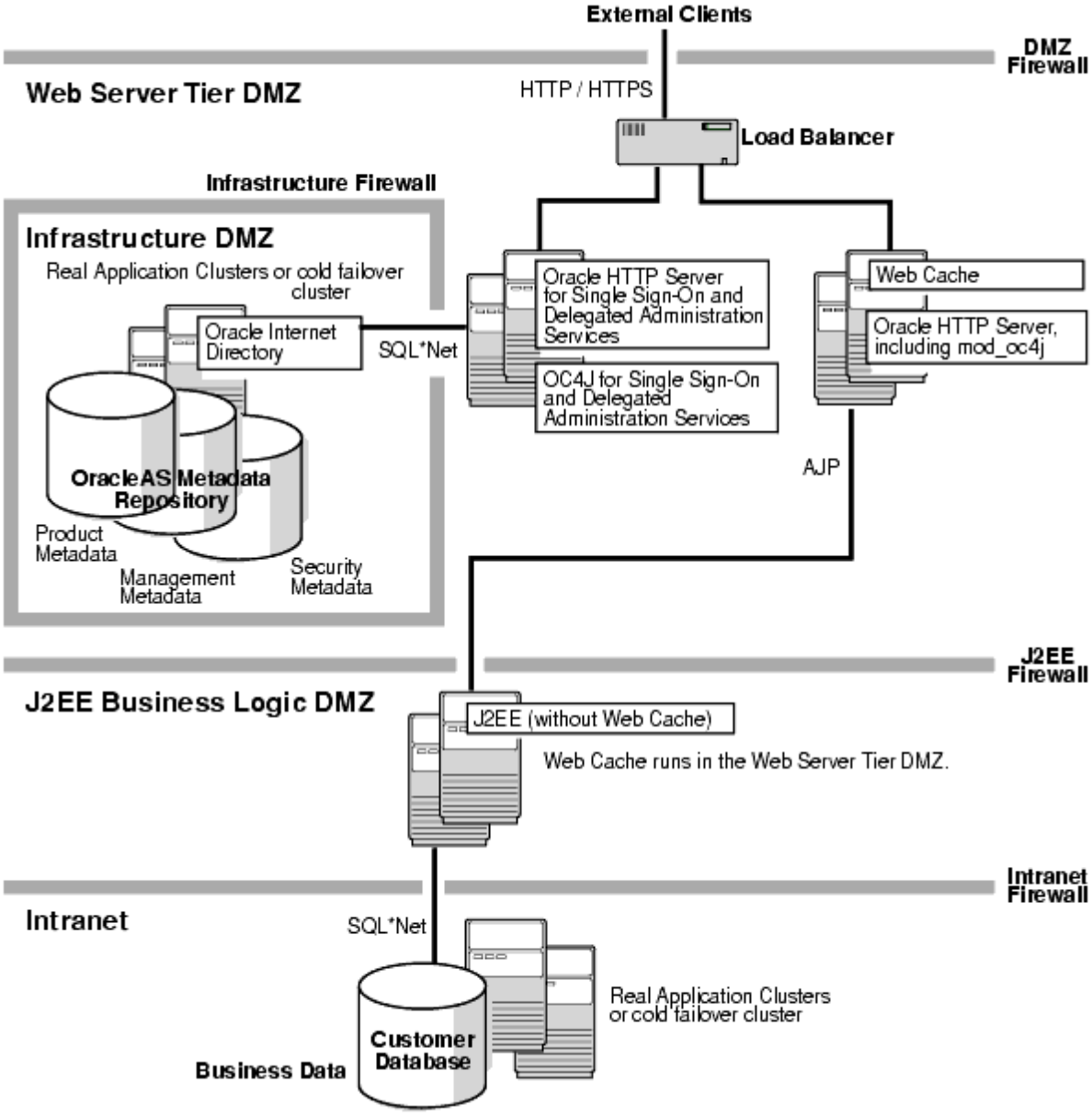


Рис. 4

Уровень корпоративной системы – ClientTier (Тонкие и толстые клиенты).

С точки зрения рассмотрения защиты системы, веб-броузеры – это компоненты, которыми IT инфраструктура может управлять менее всего и имеет минимальное количество элементов управления. Выполняя электронную

витрину Веб, например, чаще всего мы не можем управлять броузерами, которые используют клиенты. Броузер клиента тем не менее воздействует на защиту вашей системы, и должен быть принят во внимание. Чтобы безопасно осуществлять транзакции Веб, Ваше приложение должно поддерживать определенные протоколы и технологии защиты, в том числе http/https, LDAP, SSL, x.509 сертификаты, и Java. По умолчанию, информация, посланная взад и вперед к веб-навигатору, передается в открытую; любой промежуточный сайт может читать данные и потенциально изменить их в середине передачи информации. Веб-навигаторы и серверы решают эту проблему при использовании Secure Sockets Layer - протокол, чтобы кодировать передачи http (обращаются как HTTP/SSL или https). Это гарантирует защиту данных, передаваемых между клиентом к серверу. Однако, потому что доступные веб-навигаторы не отправляются с клиентскими свидетельствами, большинство передач HTTP/SSL удостоверено только в одном направлении, от сервера к клиенту; клиент не удостоверяет себя серверу. В случае Oracle OAS 10G доступна взаимная идентификация. Oracle OAS 10G может поддерживать и аппаратные акселераторы SSL.
Поскольку протокол http не поддерживает сессии, много приложений электронной коммерции используют cookies, чтобы запомнить данные сессии для индивидуальных клиентов. Эти cookies передаются как cleartext; это означает, что они могут быть прерваны третьей стороной. Для этого, мудро для приложения кодировать или затемнить информацию, которая запомнена в cookies. Сообразно корпоративной политике Oracle Corporation, веб-навигаторы сертифицируются для использования с платформой. В случае использования толстых (rich, thick) клиентов (для примера, через Web Services, SOA/SODA и т.д.) количество элементов управления может быть большим, и слабая связанность компонентов системы может существенно уменьшиться. Достаточно перспективным с точки зрения безопасности толстых клиентов видится использование eToken устройств, позволяющих на аппаратном уровне разрешить вопросы разграничения прав доступа.

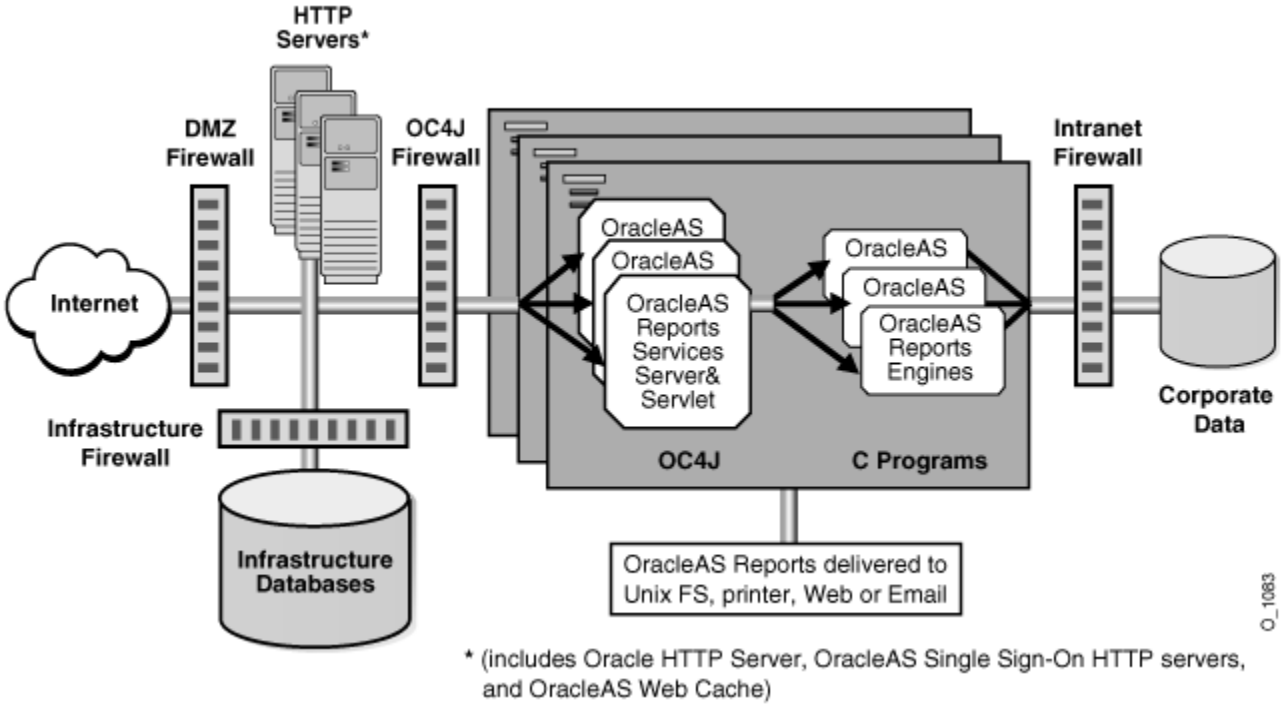


Рис. 5

Концепция интегрированной безопасной IT-инфраструктуры предприятия на базе платформы Oracle.

Рассмотрев основные механизмы реализации безопасности на различных уровнях в современной платформе Oracle, постараемся увидеть каким образом все это интегрируется в общую безопасную IT-инфраструктуру. Все различные уровни работы IT инфраструктуры интегрируются в единое целое на основе двух основных концепций:

- Identity Management Architecture – системе управления тождественностью (идентичностью) объектов в распределенной IT инфраструктуре.
- Oracle Grid – системе контроля, мониторинга и управления IT инфраструктурой в условиях динамического перераспределения ресурсов между ее компонентами.

Управление тождественностью - это процесс, при котором различные компоненты в административной системе управляют жизненным циклом сетевых объектов в IT инфраструктуре. Жизненный цикл сетевых объектов включает в себя создание учетной записи об объекте, приостановку использования учетной записи, модификацию, назначение на нее привилегий, и вычеркивание учетной записи. Сетевыми управляемыми объектами могут

являться устройства, процессы, приложения, или что-либо еще, взаимодействующее с сетевым окружением. Используя Identity Management System, предприятие может:

- Сократить затраты на администрирование через централизованное управление учетными записями и автоматизацию задач
- Ускорить прикладное развертывание, предоставляя новые приложениям возможность усилить существующую IT-инфраструктуру
- Улучшить опыт использования IT-инфраструктуры, разрешая быстрый доступ к новым сетевым управляемым объектам
- Улучшите защиту пользовательских паролей за счет централизации хранения учетных записей в целях улучшения централизованного управления распределенными приложениями и другими сетевыми управляемыми объектами.

На Рис. 6 представлены базовые компоненты Oracle Identity Management System.

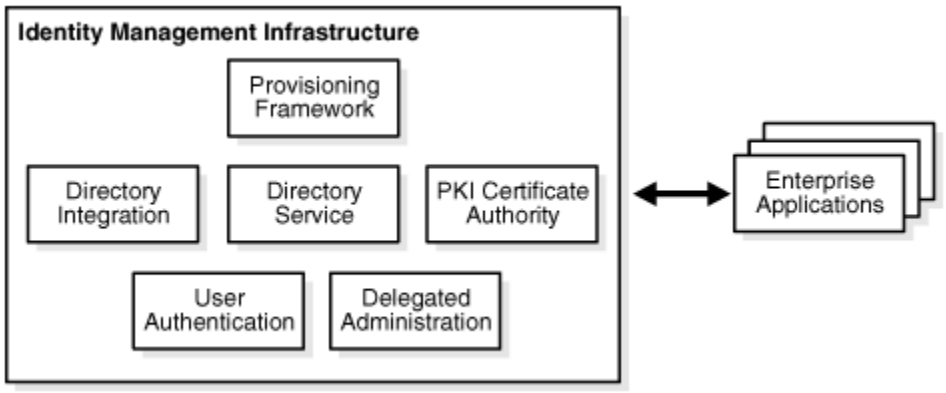


Рис.6

Oracle Identity Management инфраструктура включает в себя следующие компоненты:

- Oracle Internet Directory: Масштабируемая LDAP V3-совместимая служба директорий симплементированая на базе Oracle9i/10g Database Server
- Oracle Directory Integration and Provisioning: Компонент Oracle Internet Directory, которая предоставляет возможность:
    1. Синхронизовать данные между Oracle Internet Directory и другими подключенными службами директорий
    2. Посылать уведомления к приложениям для отражения состояния статуса пользователей или информации
    3. Разрабатывать и подгружать Ваши собственные агенты для подключения других служб директорий.

- Oracle Delegated Administration Services: Компонента Oracle Internet Directory, которая обеспечивает доверительное администрирование содержимого в службе директорий для пользователей и администраторов приложений.
- Oracle Application Server Single Sign-On (OracleAS Single Sign-On): Обеспечивает Single Sign-On доступ к компонентам Oracle IT инфраструктуры и сторонним Web-приложениям.
- Oracle Application Server Certificate Authority (OCA): создает, отменяет, возобновляет, и издает свидетельства X.509v3 , чтобы поддерживать PKI-основанные сильные аутентификационные методы в рамках Oracle Identity Management System и безопасной IT-инфраструктуре.
- Много различных типов приложений, как-то Oracle E-Business Suite и Oracle Collaboration Suite, могут использовать Oracle Identity Management инфраструктуру, как показано на Рис. 7

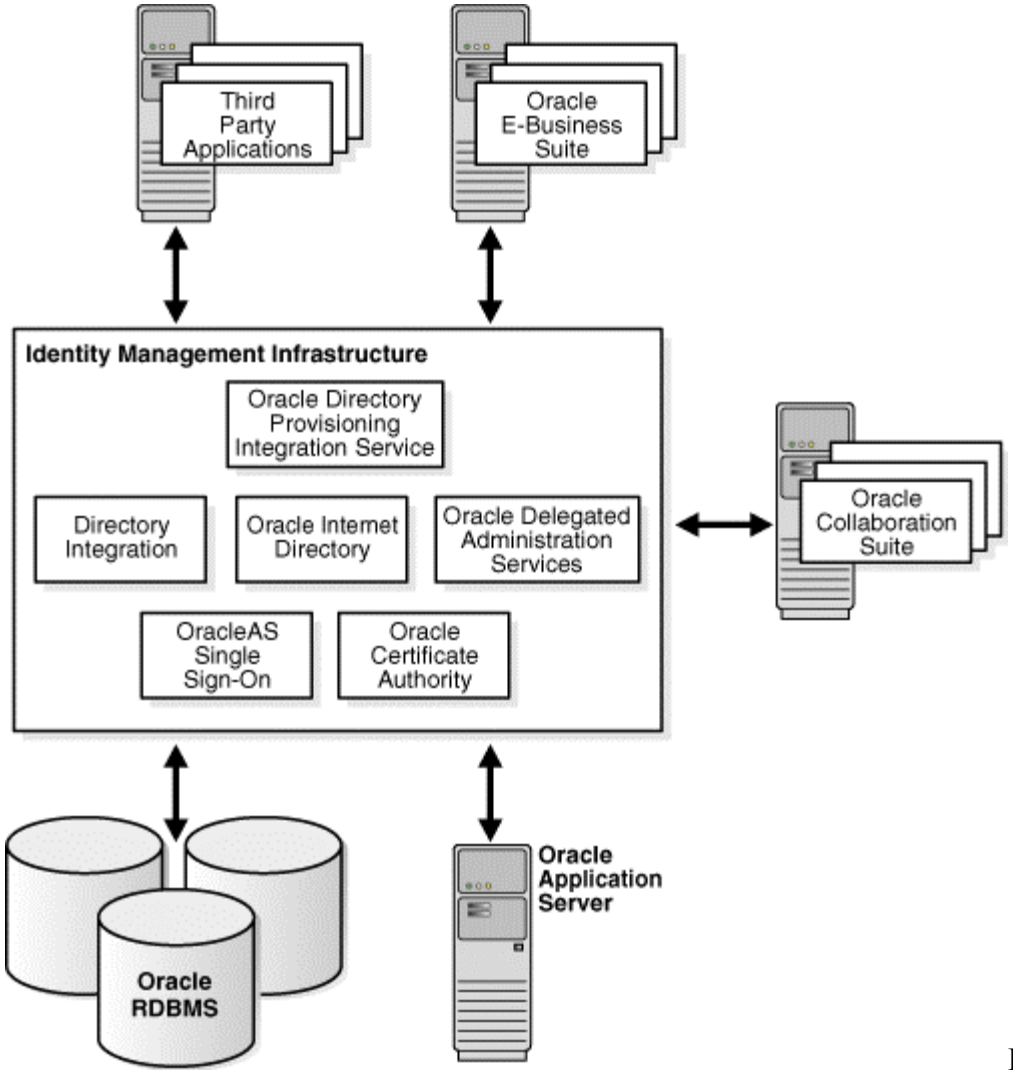
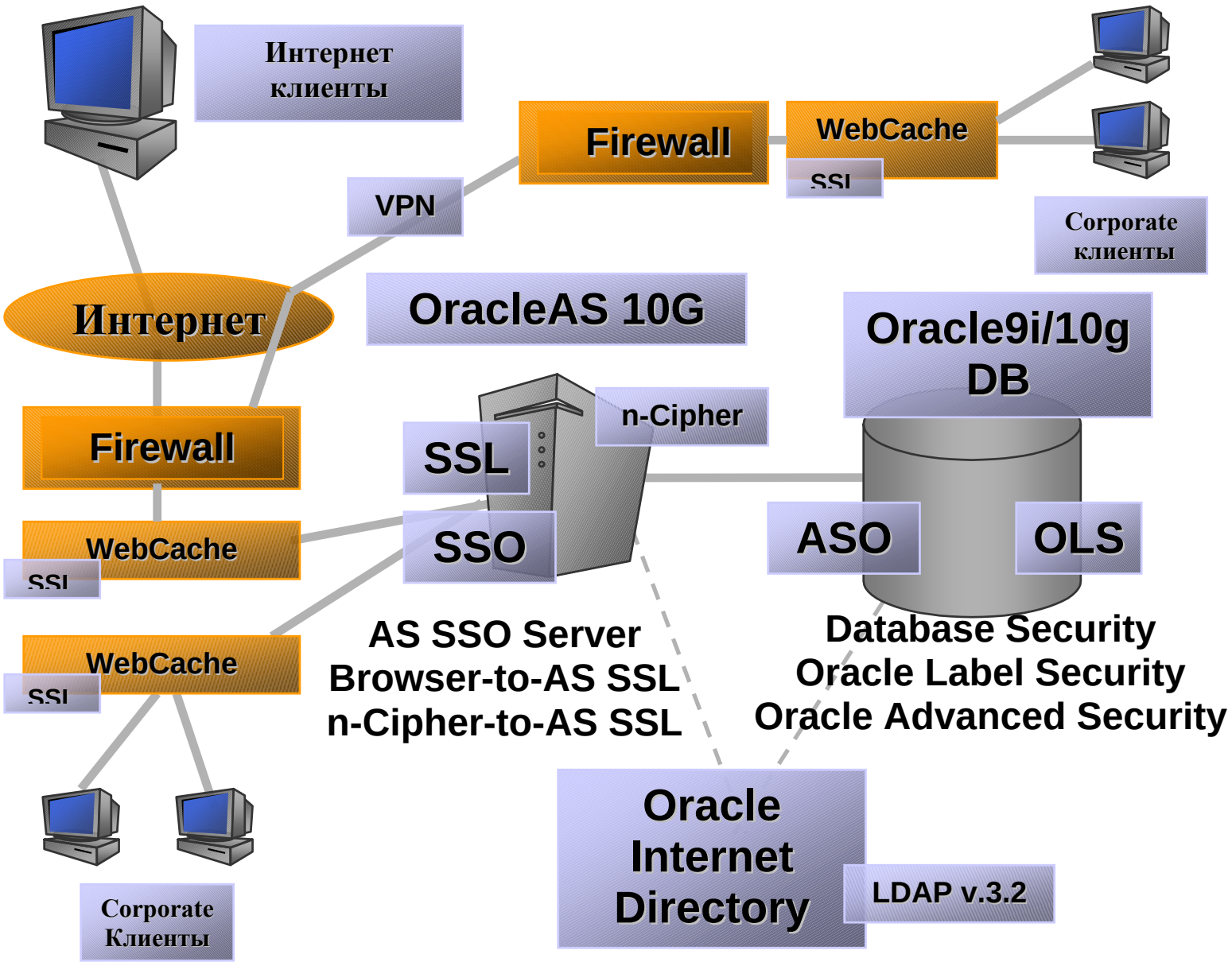
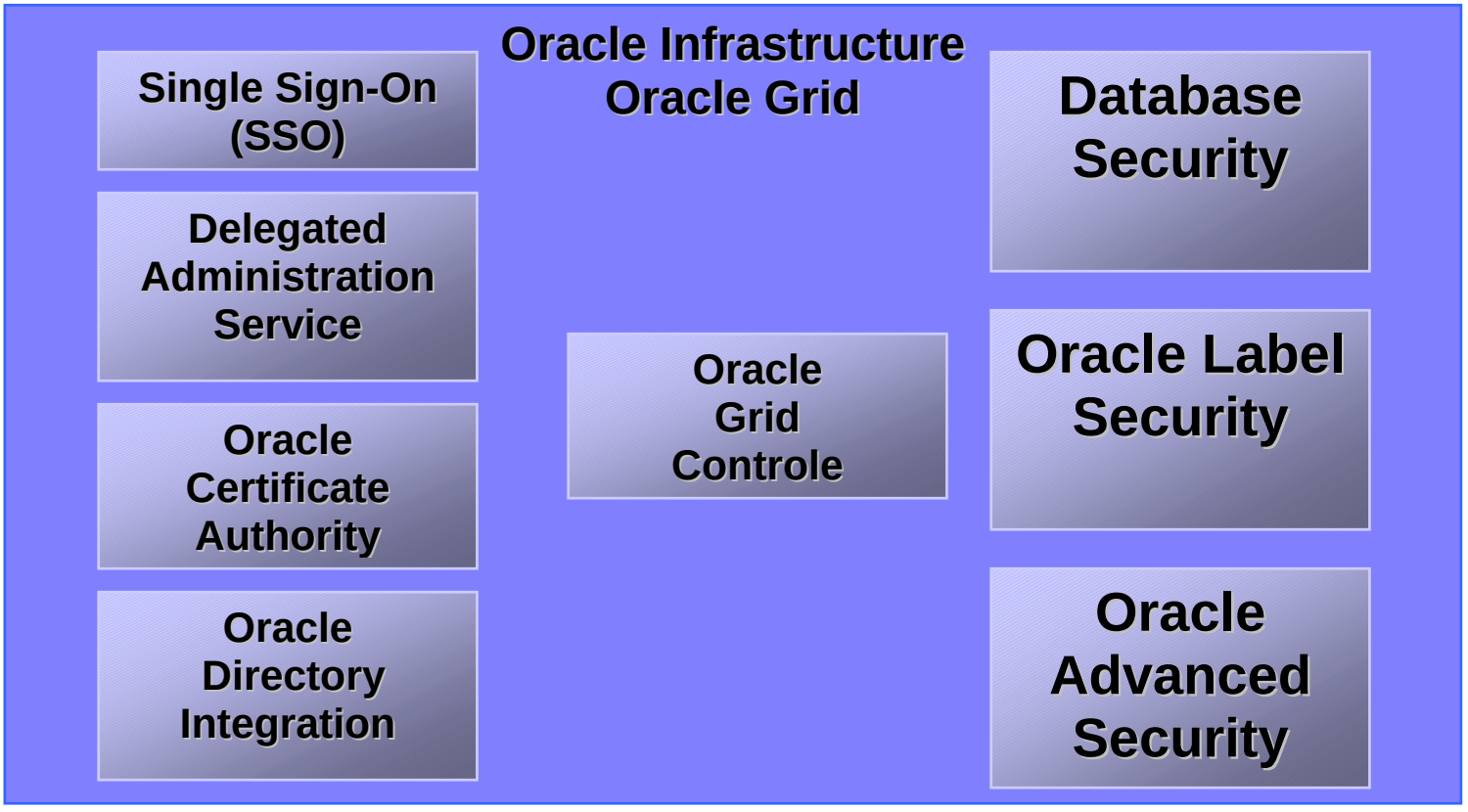


Рис. 7

На цветной вкладке (смотри ниже) приведен схематический анализ общей концепции реализации Oracle IT безопасной инфраструктуры.

Отдел технического консалтинга 24.09.2004
Oracle CIS, Russia, Moscow


Интернет клиенты
Firewall
WebCache
SSL
VPN
Corporate клиенты
Интернет
OracleAS 10G
Oracle9i/10g DB
Firewall
n-Cipher
SSL
SSO
WebCache
SSL
ASO
OLS
AS SSO Server
Browser-to-AS SSL
n-Cipher-to-AS SSL
Database Security
Oracle Label Security
Oracle Advanced Security
WebCache
SSL
Oracle Internet Directory
LDAP v.3.2
Corporate Клиенты


Oracle Infrastructure
Oracle Grid
Single Sign-On (SSO)
Delegated Administration Service
Oracle Certificate Authority
Oracle Directory Integration
Oracle Grid Controle
Database Security
Oracle Label Security
Oracle Advanced Security