Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 7 (98)/2001

Решения Hewlett-Packard для защиты информационных систем

КОРПОРАТИВНЫЕ СИСТЕМЫ

Решения Hewlett-Packard для защиты информационных систем

СОДЕРЖАНИЕ

Средства организации подсистем безопасности в корпоративных информационных системах

Современные компании все шире внедряют корпоративные информационные системы (КИС) в свою деятельность. Это позволяет повысить эффективность деятельности за счет использования более оперативной и полной информации внутри компании, а также открывает новые возможности для взаимодействия с потенциальными клиентами посредством общедоступных сетей и Интернет. Но вместе с преимуществами появляются и риски, связанные с опасностями взаимодействия с открытой и неконтролируемой внешней средой. Для снижения этих рисков необходимо уделять все большее внимание построению и сопровождению систем безопасности КИС.

Для построения системы безопасности необходимо четко представлять, что именно требует защиты и какими средствами эта защита будет осуществляться.

В информационной технологии Intranet ключевое место занимает Intranet — сервер, называемый также WWW — сервером.

WWW — сервер может рассматриваться как специфическая платформа для построения информационной системы. Архитектура WWW — сервера зависит от функциональной направленности информационной системы, которая будет строиться на его основе. Тем не менее можно выделить несколько типовых решений для WWW — серверов в рамках корпоративной информационной системы. Эти типовые решения называются моделями WWW — серверов. Выделим четыре базовые модели WWW — серверов:

- Информационный экран.
- Сервер документов.
- Внутренний информационный сервер.
- Внешний информационный сервер.

Информационный экран используется для решения задачи сегментации КИС в соответствии с организационной структурой. Информационный экран выполняет роль сервера подразделений или сервера рабочих групп, являясь одновременно шлюзом доступа к информационным ресурсам предприятия или организации. В то же время информационный экран предоставляет локальные сервисы для подразделения, такие как файловый сервис или сервис печати. Особенностью такого сервера является практически полное отсутствие на нем критичной информации — информационный экран содержит только ссылки на информационные ресурсы или приложения.

Сервер документов предназначен для хранения и обработки большого массива документов, в том числе нормативно-справочных, распорядительных, административных, технических и т.д. Специфика сервера — статические документы, предназначенные, в основном, для долговременного хранения. Формальные требования к структуре документов не специфицированы. Сервер документов представляет собой хранилище документов организации — как оперативное, так и долговременное. Такой сервер предоставляет универсальный доступ к размещенным на нем документам. Кроме того, он снабжен системами поиска и навигации в оперативном хранилище документов, а также средствами архивации документов. Доступ к документам осуществляется с рабочих мест, расположенных в локальной сети предприятия.

Внутренний информационный сервер предназначен для хранения и обработки информации, циркулирующей внутри организации или отдельных ее подразделений. Этот сервер используется как основной компонент единой системы централизованных коммуникаций внутри компании. Внутренний информационный сервер представляет собой основу корпоративной информационной системы организации и предоставляет следующие сервисы:

- Создание и публикация информационных ресурсов.
- Сервис поиска и навигации.
- Телеконференции.
- Интерфейс к прикладным системам, в том числе и к таким, которые не были специально разработаны для использования в среде WWW — сервера (такие системы называют унаследованными).

В зависимости от масштабов и структуры организации, внутренний информационный сервер может объединять несколько WWW — серверов подразделений. Такое структурирование информационного сервера целесообразно применять для больших организаций. Это позволяет оптимизировать информационные потоки между подразделениями. Кроме того, иерархическая организация информационного сервера делает его более управляемым. При этом хранилище информации остается структурно и логически единым. Специфика данной модели состоит в том, что информационная система ограничена рамками локальной сети организации.

В случае работы в рамках глобальных сетей общего или ограниченного доступа используется внешний информационный сервер. Внешний информационный сервер может быть создан для представительских (информация об организации и ее работах), технологических (абоненты получают доступ к техническим материалам, новым версиям программных систем и так далее), маркетинговых и других целей. Спецификой описанной модели является минимальная информация о пользователе, не-

обходимость работы в потенциально враждебной среде.

В этой связи возникает необходимость защиты WWW — серверов. Особенно это актуально для внутренних и внешних информационных серверов.

Для решения подобных задач необходим комплексный подход к защите информации в КИС. Примером такого подхода может быть решение по защите информации Praesidium компании HP.

Применение решений HP Praesidium по защите информации в автоматизированных системах

Типичная инфраструктура корпоративной АС

Типичная инфраструктура корпоративной АС (рис.1) включает зону Интернет, в которой находятся потенциальные клиенты и которая не является безопасной, демилитаризованную зону, в которой находятся доступные из Интернет Web-сервера, и защищенную зону Интранет, в которой циркулирует внутренняя информация.

Прежде всего, существует Интернет-зона, которая не считается надежной в плане безопасности от внешних атак. Предполагается, что из Интернет к определенным внутренним ресурсам компании обращаются потенциальные клиенты, партнеры из других компаний или поставщики Интернет-услуг.

DMZ (демилитаризованная зона) — это область, где небезопасная зона Интернет пересекается с защищенной внутренней сетью. Внешняя безопасность зоны DMZ обеспечивается работой межсетевых экранов (firewall) и фильтрующих маршрутизаторов.

Такие приложения, как общедоступные web-серверы и шлюзы электронной почты обычно устанавливаются именно в зоне DMZ.

В зоне Интранет находятся внутренние сервера, а также сервера приложений и баз данных. В этой зоне циркулирует внутренняя корпоративная информация, которая должна быть надежно защищена от несанкционированного доступа.

Рассмотрим схему защиты информации в корпоративной АС, используя комплексное решение Praesidium (рис. 2). Подобная схема может быть реализована в компаниях, занимающихся различными видами деятельности, в том числе и электронной торговлей.

Концепция внедрения комплексного решения Praesidium в АС

Для контроля демилитаризованной зоны рекомендуется использовать межсетевое экранирование, используя его как для контроля на границе Интернет и DMZ, так и на границе DMZ и Интранет. В этом случае Web-сервера, находящиеся в демилитаризованной зоне нуждаются в дополнительной защите, которую обеспечивает операционная система повышенной надежности Praesidium VirtualVault для Unix или Praesidium WebEnforcer для NT. Для повышения безопасности транзакций и контроля доступа к Web-серверам можно использовать Praesidium Authorization Server — сервер, предназначенный для централизованной проверки полномочий пользователя на запрашиваемый ресурс.

Решения по защите информации Praesidium

Семейство продуктов HP Praesidium, обеспечивающих безопасность информации, содержит решения для защиты различных уровней автоматизированной системы предприятия.

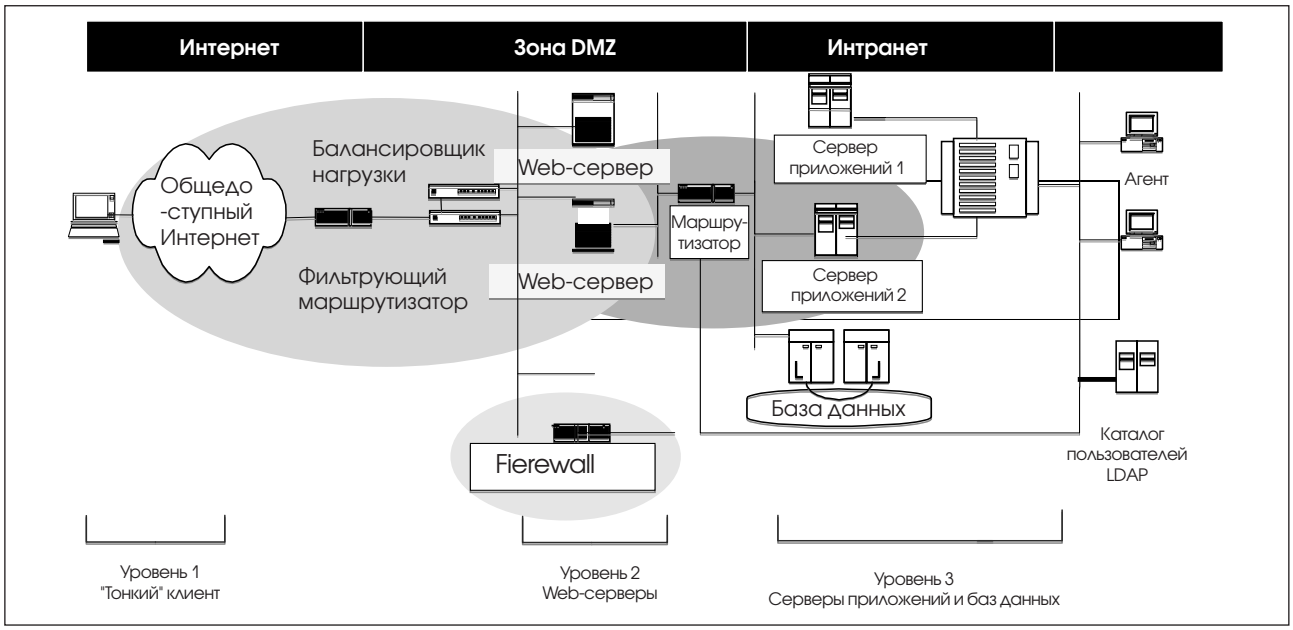

Рис. 1 Типичная инфраструктура корпоративной АС

Независимо от того, создает ли компания приложения на основе новейших web-технологий или только расширяет диапазон использования ранее разработанных приложений путем привлечения новых пользователей через локальные или глобальные сети, в компании возникает необходимость внедрить гибкие и эффективные решения по обеспечению безопасности, специально адаптированные к особенностям ее электронного бизнеса. В рамках этих требований, направленных на предоставление клиентам все более мощных решений по безопасности, HP предлагает семейство HP Praesidium.

В состав этого семейства входят:

- сервер авторизации Authorization Server;
- решение для защиты домена (DomainGuard);
- операционная система для защиты Web-серверов и приложений с помощью VirtualVault и WebEnforcer;
- обеспечение Extranet VPN;
- брандмауэр e-Firewall;
- система обеспечения безопасности транзакций и контроля доступа на основе открытых ключей Praesidium PKI.

Платформа для web-серверов VirtualVault

VirtualVault — это платформа для web-серверов, которая позволяет защитить критически важные Интернет-приложения за счет значительного сокращения количества уязвимостей, которыми могут воспользоваться злоумышленники (рис 3).

VirtualVault включает высоконадежную операционную систему, web-сервер (например, Netscape NES, Apache), а также разделенную на зоны рабочую среду, защищающую операционную систему, web-сервер, web-страницы и тексты интерфейсных программ, работающих на платформе web-серверов. VirtualVault также осуществляет мониторинг и создает отчеты обо всех попытках изменения системных файлов или файлов приложений.

При разработке системы VirtualVault учитывались три базовых принципа:

- минимализм;
- предельно жесткий контроль;
- непрерывный мониторинг.

Эта операционная система предоставляет только те сервисы, которые требуются для конкретного приложения, при этом отсутствует обладающий неограниченными полномочиями привилегированный пользователь или администратор, а выполнение каждого процесса разрешается только при наличии необходимого минимального набора прав доступа (и только на то короткое время, когда это действительно требуется). Все взаимодействия между web-сервером, операционной системой и интерфейсными приложениями происходят на уровне процессов и контролируются специальным механизмом, который создает раздельные виртуальные рабочие среды для повышения безопасности и надежности работы системы.

Аналогичным образом ограничивается доступ к web-страницам, системным файлам и файлам приложений.

Ниже представлен краткий список основных преимуществ операционной системы Virtual Vault:

- Web-сервер конфигурируется таким образом, что незащищенных мест становится значитель-

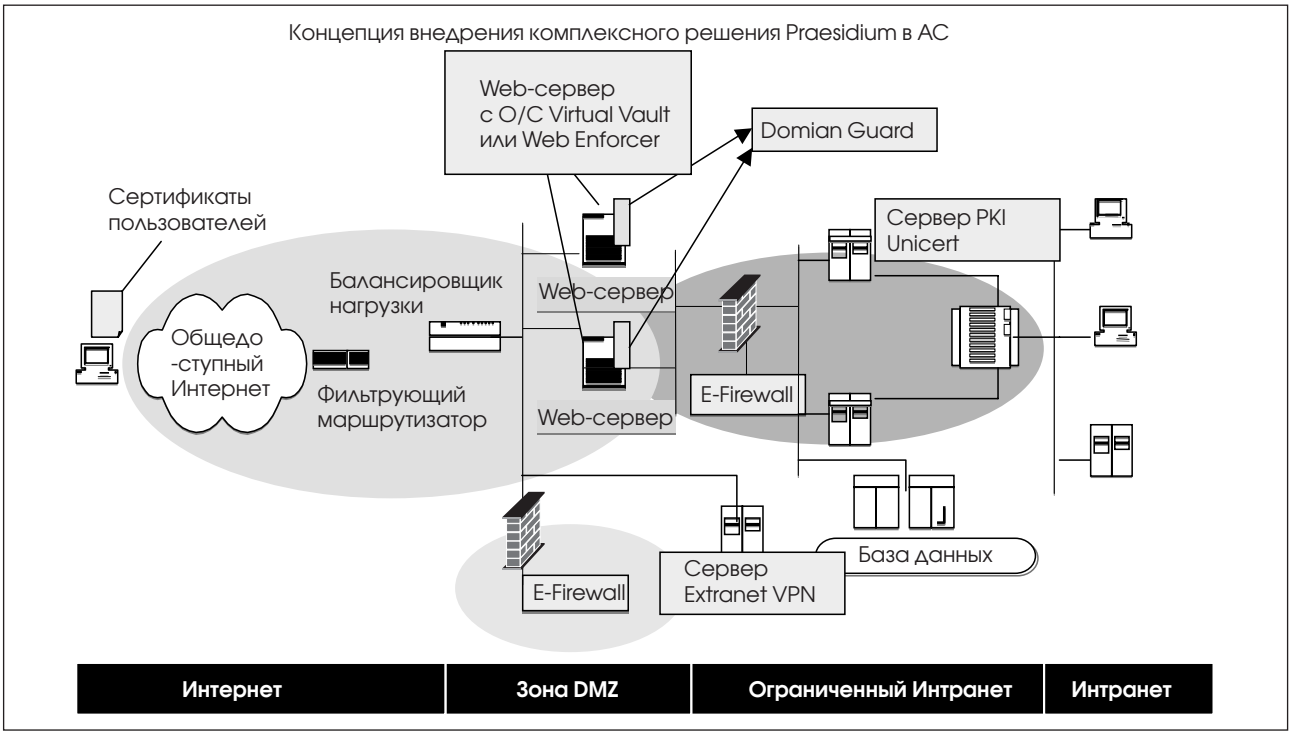

Рис. 2. Платформы и зоны применения комплексного решения в области безопасности информации Praesidium

но меньше, чем у ПО, установленного в режиме по умолчанию. ПО инсталлируется во внешней зоне для того, чтобы успешные атаки на web-сервер ограничивались только этой областью. Таким образом, внутренняя зона и внутренние ресурсы оказываются надежно защищенными от атак.

- В операционной системе VirtualVault (VVOS) нет привилегированного пользователя (root user), который мог бы использоваться злоумышленниками или их программами для атаки на внутренние ресурсы (напротив, в VirtualVault используется принцип наименьшего уровня привилегий). VVOS разбивает платформу на независимые подзоны, что позволяет защитить web-страницы и тексты интерфейсных приложений ОС от атак даже в том случае, если часть из них уже достигла своего результата. При использовании такой архитектуры приложений ОС VirtualVault перед выполнением приложения проводит проверку его текста и запускает на исполнение только в том случае, если он не был изменен. Если же в тексте приложения обнаружены изменения, выполняемые файлы могут быть возвращены в исходное, неизмененное состояние, после чего будет создан файл журнала контроля событий и ОС продолжит выполнение других приложений.
- VVOS регистрирует все случаи нарушения прав доступа в файле журнала контроля событий, который хранится в собственной высоконадежной зоне с наивысшим уровнем защиты. В случае попыток взлома средств безопасности система регистрации в режиме реального времени отправляет системному администратору сообщения, указывающие место и характеристики запрещенных действий.

Основные характеристики VirtualVault

WEB-безопасность	
Операционная система	• 50 различных и контролируемых привилегий ОС • Поддержка потоков и 64-битовой архитектуры
Сегментированная web-среда исполнения	• Защищенная виртуальная Java-машина • Защищенный шлюз Trusted Gateway Agent/Proxy
Интегрированный web-сервер	• Защищенный web-сервер.
Безопасность на стыке браузер — сервер	• Строгая аутентификация на основе SSL протокола • 40 и 128 — разрядное SSL — шифрование
Администрирование безопасности	
Администрирование на основе браузера	• Netscape Navigator и Internet Explorer
Мониторинг безопасности	• Аудит и аварийная сигнализация
Консоль управления	• Менеджер сетевых узлов HP OpenView (не входит)
Поддержка среды приложений	
Межплатформенная защита приложений	Интегрируемый модуль Praesidium Web Proxy (не входит)
Модули высокой доступности	• VVOS Mirror Disk (не входит), дисковый массив AutoRAID
Шлюзы приложений	• Традиционные CGI Scripts и Proxies
Шлюзы СУБД	• Стандартные SQL Scripts (напр., JDBC, ODBC)
Шлюзы сервера приложений	• Соответствующие фирменные сценарии (напр., NetDynamics)
Языки программирования для web	• HTML, Java Servlets, C/C++, Perl (CGI)
Качество web-услуг (HP webQoS)	• Выравнивание нагрузки между несколькими web-серверами • Управление пиковыми нагрузками • Защита от DoS атак.

Табл. 1. Основные характеристики VirtualVault

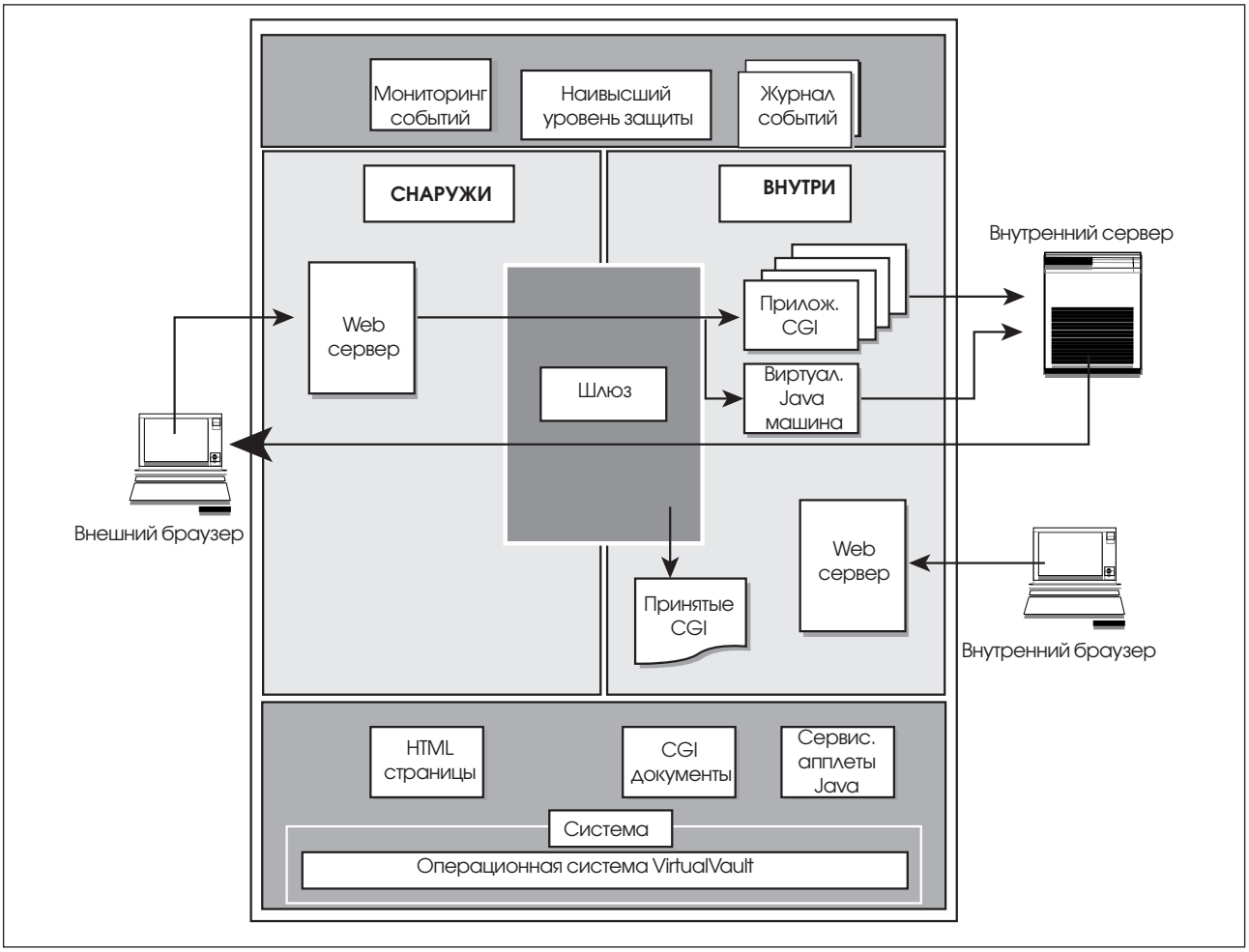

Рис. 3. Типичная рабочая web-среда, разделенная на зоны

Сегментирование данных

Сегментирование данных создает надежную «стену» между Интранет-приложениями и пользовательским интерфейсом, обслуживающим клиентов Интернет. Первоначально разработанная для защиты секретной информации технология сегментирования была адаптирована в VirtualVault для решения проблемы безопасности в коммерческих Интернет-проектах.

Сегментирование данных подразумевает классификацию всех файлов и программ на сервере по следующим категориям:

- Внутренние (например, базы данных, программы CGI, Java, серверы промежуточного ПО);
- Врешние (например, web-сервер, статические web-страницы).

ОС VirtualVault разграничивает доступ между этими категориями. Чтобы программа из одной области получила доступ в другую область, она должна обладать соответствующими привилегиями. Все коммуникации между Внутренней и Внешней областями контролируются с помощью технологии защищенных шлюзов VirtualVault. Защищенный шлюз защищает приложения, отнесенные к категории ВНУТРЕННИХ, от злонамеренных атак или ошибок, которые могли бы при отсутствии такой защиты нанести вред внутренним приложениям.

Все системные приложения хранятся в системной области с целью сохранения их целостности. Такое разделение защищает web-страницы от проникновения злоумышленников, выискивающих слабые места в защите или конфигурации. Защищенные web-страницы не могут быть переписаны или подвержены атаке с целью помещения непристойных и пропагандистских материалов.

Управление пиковыми нагрузками

Программа HP Web QoS добавляет к основной функциональности VirtualVault весьма важную функцию управления пиковыми нагрузками. Эта функция, непосредственно влияющая на качество услуг, предотвращает перегрузку сервера, минимизируя влияние неожиданных всплесков числа запросов и максимизируя объем завершенных транзакций. Управление пиковыми нагрузками гарантирует, что каждый находящийся в системе клиент будет обслужен.

Новые пользователи не получают доступа к web-сайту, если они не смогут завершить свои транзакции соответствующим образом. Имея в своем распоряжении инструмент управления пиковыми

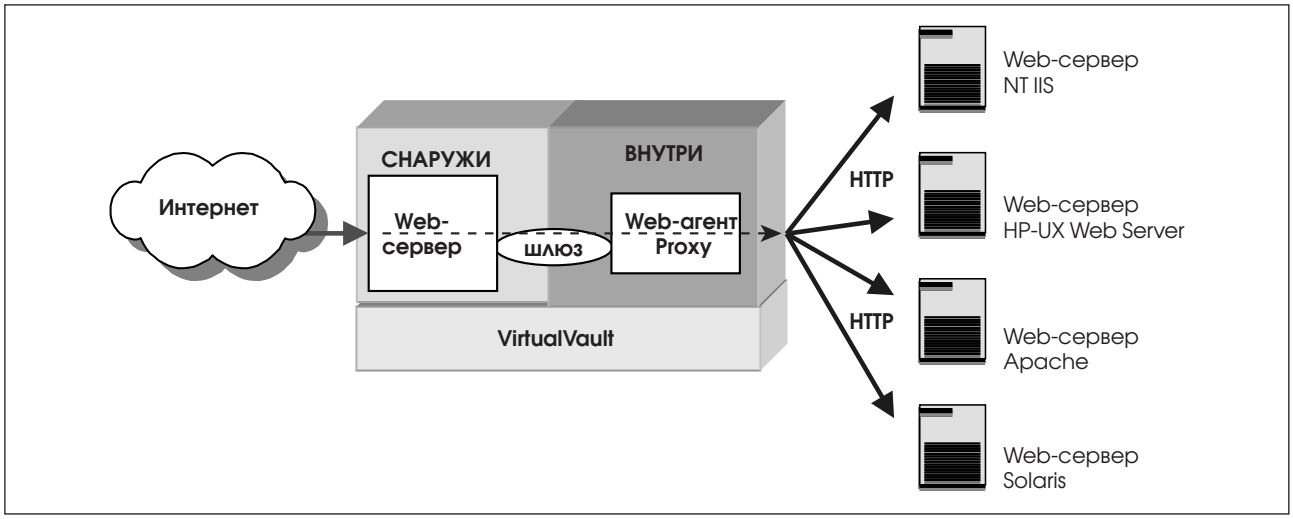

Рис. 4.

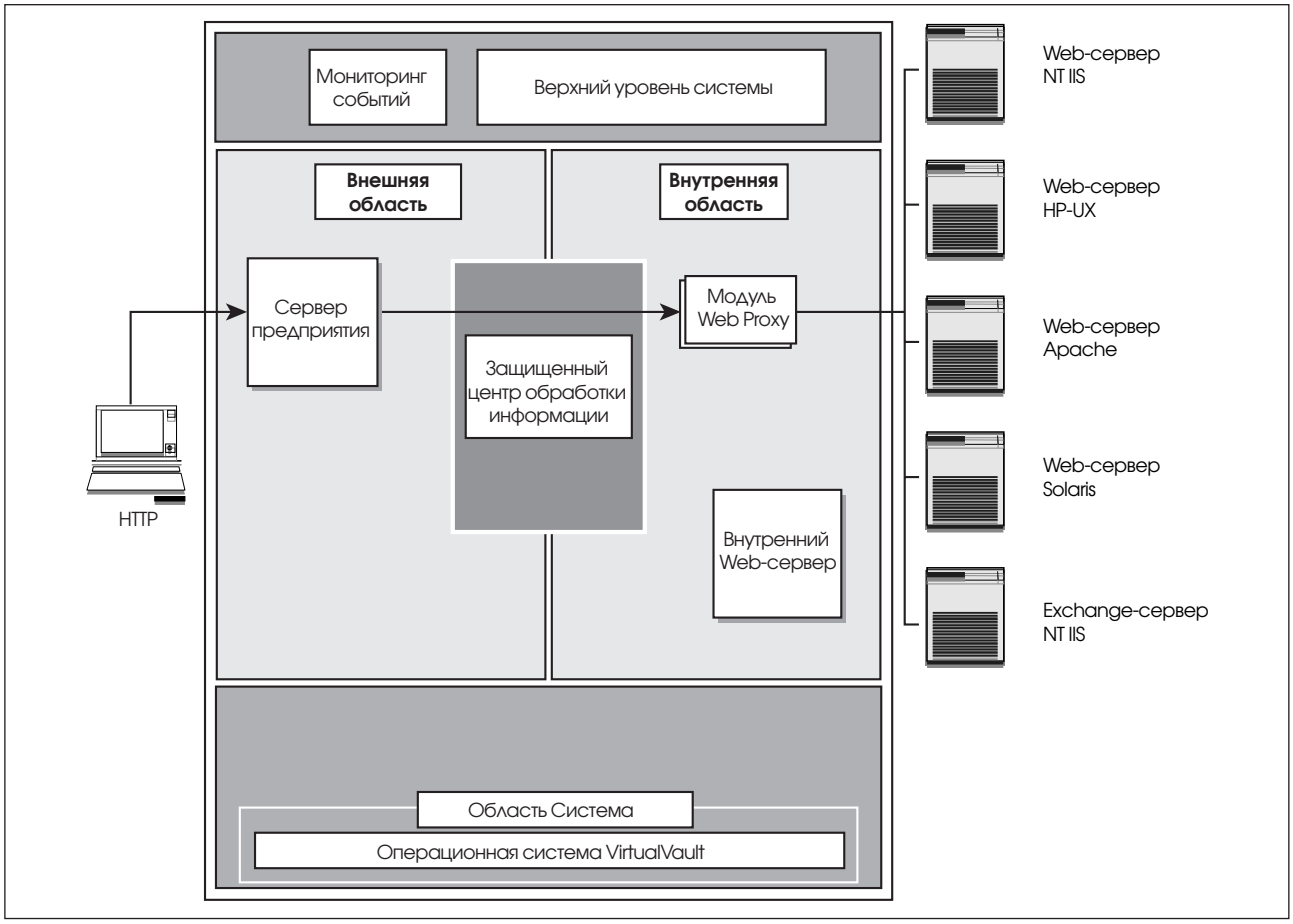

Рис. 5.

нагрузками, возможно настроить систему на работу в одном из следующих режимов:

- перенаправление новых запросов в другую систему, имеющую необходимые резервы производительности;
- задержание выполнения новых заданий на некоторый промежуток времени, пока не будут завершены текущие сеансы;
- отклонение новых запросов в условиях экстремальной нагрузки.

Результатом такого управления является общее улучшение функционирования сайта и получение конкурентных преимуществ за счет обеспечения более высокого качества услуг.

Защищенная виртуальная Java-машина

С помощью защищенной виртуальной Java-машины (JVM), работающей во ВНУТРЕННЕЙ области исполнения приложений, VirtualVault может защитить Java сервер, а также CGI Java-приложения.

VirtualVault переносит кроссплатформенную среду выполнения Java, являющуюся отраслевым стандартом, на безопасную платформу исполнения приложений. В случае традиционного web-сервера JVM была бы размещена в той же области исполнения, что и сам web-сервер, т.е. в области досягаемой из внешней сети, что подвергало бы JVM и Java приложения той же опасности, которой подвергается web-сервер.

Напротив, надежная web-серверная платформа VirtualVault помещает JVM и Java сервлеты во ВНУТРЕННЮЮ область исполнения приложений, которая отгорожена защищенным шлюзом и недоступна извне. Тем самым достигается гарантия того, что прямой доступ к JVM и сервлетам Java в принципе исключен, и эти программы надежно защищены от внешних атак и каких-либо изменений. VirtualVault поддерживает JDK CI.17.01 и JSDK 2.0.

Администрирование системой безопасности VirtualVault

VirtualVault использует интерфейс популярного web-браузера Netscape Navigator для решения задач администрирования, допуская удаленный доступ из Интранет. Административные задачи могут решаться после краткого обучения, а онлайновая справка и гипертекстовая (HTML) документация всегда имеется под рукой.

Большую помощь администраторам оказывают предусмотренные в системе сеансы аудита с аварийной сигнализацией, во время которых проводятся проверки всех ключевых элементов, связанных с безопасностью системы. Программы, не имеющие соответствующих полномочий, не могут получить доступ к аудиторским отчетам. Кроме того, все параметры аудиторских сеансов и аварийной сигнализации VirtualVault могут быть сконфигурированы для работы с продуктом OpenView.

Виртуальный шлюз Vault Proxy

Для web-приложений, работающих только на платформах, отличных от HP-UX, или требующих быстрого выхода на рынок, портфель HP Praesidium предлагает решение VirtualVault Proxy (рис. 4). Оно позволяет установить любое работающее по протоколу HTTP приложение во внутренней зоне системы Virtual Vault.

В этом случае пользователям не придется обращаться к незащищенным web-приложениям напрямую; вместо этого доступ к ним будет осуществляться через шлюз VirtualVault, который используется в качестве агента для передачи запроса внутренним web-приложениям.

Модуль Praesidium Web Proxy дает возможность интегрировать приложения, работающие на различных платформах, в среду выполнения Virtual Vault.

Платформонезависимая защита приложений с помощью модуля Praesidium Web Proxy

Модуль Web Proxy придает платформе VirtualVault дополнительную гибкость, высокую доступность, масштабируемость и легкость использования. Это промежуточное ПО связывает пользовательский интерфейс VirtualVault с серверными приложениями, работающими под AIX, HP-UX, NT и Solaris, или с любым другим сервером, работающим на основе Web.

Поддержка конфигураций HP 9000

Минимальные требования к аппаратному обеспечению, необходимому для работы платформы VirtualVault и соответствующих защищенных приложений, зависит, в первую очередь, от уровня услуг, который ожидается от конкретного бизнес-приложения. Для типовой опытной установки системы, масштаб которой находится где-то между средним и большим, достаточно сервера предприятия HP 9000 серии N 4000.

VirtualVault работает также на некоторых серверах предприятия HP 9000 классов A-, D-, E-, K-, L-, N- и R. Для обеспечения высокой доступности VirtualVault поддерживает Зеркальный диск MirrorDisk/VVOS и дисковый массив AutoRAID. Конфигурации с несколькими web-серверами возможны на основе использования собственного модуля Praesidium Web Proxy системы VirtualVault — инструмента выравнивания нагрузки HP webQoS, и продукта от компании Cisco — Cisco LocalDirector. Платформы Workstation не поддерживаются.

Web Enforcer – Защита Web-серверов для платформы для NT

Система WebEnforcer для NT, входящая в портфель HP Praesidium, предназначена для защиты среды web-серверов, работающих под Windows NT, осуществления непрерывного мониторинга и обеспечения безопасности работы приложений электронного бизнеса. Решение HP Praesidium WebEnforcer призвано защищать самые важные компоненты NT-платформы web-серверов и обладает возможностями по автоматическому устранению известных уязвимых мест в системах защиты и внедрению более эффективных методов контроля за согласованностью настроек в системе защиты.

WebEnforcer — это решение в области безопасности электронного бизнеса, обеспечивающее комплексную защиту основных элементов среды web-серверов для Windows NT, включая сервер Windows NT, web-сервер сервиса IIS, сервер транзакций, сервер индексов, браузер Internet Explorer и компоненты контроля доступа к данным.

WebEnforcer решает известные проблемы уязвимости, установленной в режиме по умолчанию ОС Windows NT, которые могут выражаться в потере важных данных, несанкционированном до-

ступе к информации, злонамеренном изменении содержимого web-сайта и отказе от обслуживания зарегистрированных клиентов.

WebEnforcer автоматически распознает уязвимые точки, устраняет их, а также осуществляет непрерывный мониторинг, расширяющий и усиливающий стандартные функции защиты. WebEnforcer деактивирует системные службы и подсистемы, потенциально являющиеся слабым звеном системы защиты, контролирует полномочия модели DCOM и удаленный доступ к системному реестру. Кроме того, это решение фиксирует значения параметров настройки системного реестра, распределяет пользовательские полномочия, а также защищает файлы и папки данных.

Администратор может задавать периодичность сканирования системы с целью поиска и устранения новых уязвимых мест в защите, возникших в результате изменения конфигурационных настроек ПО или несанкционированных проникновений.

Обновление версии HP SecurityUpdate гарантирует, что решение WebEnforcer будет включать все новые обнаруженные уязвимые места для взлома системы.

В ПО WebEnforcer включен целый ряд различных функций и инструментов, направленных на упрощение процесса конфигурирования и обслуживания системы защиты платформы web-серверов. Интерфейс пользователя WebEnforcer в стиле стандартных Windows-приложений, подробные мастера и обширная диалоговая справочная система обеспечивают гибкость и простоту использования даже для пользователей, не имеющих достаточного опыта работы в области защиты информации.

Поскольку установка WebEnforcer не требует каких-либо изменений в настройке операционной системы, инсталляция продукта и его интеграция с используемыми приложениями и процессами не вызовет никаких затруднений. В зависимости от конкретных требований к безопасности и совместимости, возможно применить один из четырех предварительно установленных профилей конфигурации или настроить их в соответствии с собственными требованиями. Есть также возможность отмены произведенных конфигурационных изменений и возврат к предыдущим настройкам.

Решение HP Praesidium WebEnforcer, благодаря автоматизации процесса настройки системы защиты, позволяет профессионалам в сфере ИТ сэкономить время на конфигурирование системы защиты вручную.

Безопасность транзакций

Сервер авторизации Authorization Server

Authorization Server — является масштабируемым сервером проверки доступа к различным клиент-серверным приложениям.

Очень часто в компаниях возникает проблема идентификации и авторизации пользователей и приложений, а также централизованного администрирования прав доступа к различным сетевым ресурсам в рамках единой корпоративной модели информационной безопасности. Для решения данных задач был создан HP Praesidium Authorization Server. Данный продукт является масштабируемым сервером проверки доступа к различным клиент-серверным приложениям. Он обеспечивает централизованную авторизацию пользователей по ролевому принципу. В рамках определенных бизнес ролей и присвоенных им бизнес правил, которыми можно описать практически любой процесс, обеспечивается не только централизованная проверка полномочий на запрашиваемый пользователем ресурс одного или нескольких приложений, но и проверка действий (передача данных), которые пользователь пытается произвести. Проверка производится через специальный авторизационный программный модуль, который интегрируется в приложения. Имеется API для встраивания данных модулей в пользовательские приложения, которые в результате смогут использовать данную схему авторизации. Сервер имеет единую интуитивно понятную систему администрирования, которая позволяет очень быстро регулировать доступ большого числа пользователей к множественным информационным ресурсам. Одним из недостатков продукта Authorization Server является то, что он в данный момент работает только под управлением операционной системы HP-UX 10.20.

Администратор безопасности порталов Экстранет DomainGuard Enterprise

Продукт DomainGuard Enterprise семейства HP Praesidium позволяет компаниям легко и быстро развертывать Экстранет-приложения и обеспечивает для них надежную защиту.

Для того, чтобы разработка web-приложений на базе продуктов Microsoft для создания систем работы с партнерами и внешними клиентами выполнялась как можно проще и в кратчайшие сроки, специалисты используют самые разнообразные инструменты. Однако, построение таких систем существенно осложняет процесс разработки схем защиты и организации доступа пользователей для таких web-приложений, а также управление этим процессом для нескольких приложений, особенно учитывая постоянно возрастающее число пользователей.

DomainGuard — это программное обеспечение для управления защитой портала сети Экстра-

нет. DomainGuard гарантирует, что пользователям будет предоставляться доступ только к той информации, которая им действительно необходима и которую им разрешено просматривать. Введя пароль всего один раз при входе в систему, пользователи смогут без проблем работать со многими приложениями.

DomainGuard предоставляет следующие функциональные возможности:

- аутентификация;
- единая точка авторизации (Single sign-on);
- контроль доступа;
- администрирование.

Используя решение DomainGuard Enterprise, компании могут удовлетворить свои потребности, связанные с комплексным обеспечением электронной безопасности, не внося изменений в базовые приложения. Решение DomainGuard Enterprise позволяет разработчикам сосредоточить свои усилия на формировании бизнес-логики, а администраторам систем безопасности — решать вопросы по управлению безопасностью в сети Экстранет. С помощью DomainGuard Enterprise пользователю предоставляется доступ к определенному ресурсу на web-сервере, к конкретному приложению или даже к некоторой учетной информации в рамках приложения. Впрочем, функции решения DomainGuard Enterprise не ограничиваются обеспечением безопасности для отдельных модулей. DomainGuard Enterprise предоставляет целую инфраструктуру для развертывания Экстранет-приложений, масштабируемую и несложную в использовании и администрировании.

Решение DomainGuard Enterprise сочетает в себе следующие основные функции защиты:

- аутентификация;
- единовременная регистрация в системе по механизму Single Sign-On;
- авторизация;
- администрирование.

В дополнение к возможности Single Sign-On, процесс проверки полномочий на доступ к отдельным модулям на web-серверах Microsoft IIS/NT упрощается благодаря использованию графического интерфейса. А управление доступом на основе ролей и соответствующих им правил еще больше сокращает затраты на администрирование. Для того, чтобы процесс развертывания не занимал много времени, клиентам предоставляются специальные шаблоны.

Основные преимущества:

- Снижение затрат на администрирование, благодаря централизованному управлению защитой для нескольких web-приложений;
- Использование существующей web-инфраструктуры, например, IIS и LDAP;
- Сокращение времени подготовки за счет несложной интеграции системы безопасности в существующие или новые web-приложения;
- Уменьшение затрат на разработку благодаря применению имеющихся ресурсов и знаний в инструментах разработки для сред NT.

Обеспечение безопасности

Безопасность обеспечивается благодаря контролю доступа к web-объектам, возможности задания различных уровней доступа для разных web-объектов (например: web-страницы, ASP, Java-приложения, CGI-сценариии и т. д.).

В системе DomainGuard производится репликация данных о политиках по нескольким web-серверам для поддержки балансирования нагрузки и преодоления сбоев и единовременная регистрация пользователей в web-среде. Благодаря этой возможности пользователи могут переходить от одного приложения к другому, не вводя каждый раз пароль, а зарегистрировавшись в системе только один раз.

Администрирование системы защиты

Система контроля доступа на основе ролей, возможность определения полномочий через группы, делегируемое администрирование и контроль за web-контентом — позволяет расширить возможности администрирования. Кроме того, использование единообразного GUI-интерфейса, работающего на базе Web-браузера, и доступа к каталогу LDAP упрощает управление системой DomainGuard.

Среда приложений

DomainGuard поддерживает такие инструменты, как Microsoft Management Console.

Пользователи могут и дальше разрабатывать приложения, используя Visual InterDev, а затем интегрировать их в механизм защиты DomainGuard.

Легкая адаптация при расширении компании и добавлении дополнительных пользователей обеспечивает высокую масштабируемость системы.

Наличие настраиваемых схем для аутентификации пользователей и API для аутентификации. Интерфейс API (или процедура прерывания аутентификации) может запросить дополнительную информацию перед тем, как полностью подтвердить подлинность пользователя.

Особенностями DomainGuard являются:

- Совместимость с консолью управления Microsoft Management Console и интерфейсом программирования приложений COM.
- Экономия затрат на администрирование благодаря управлению доступом на основе ролей и распределенных полномочий.

- Возможность использования учетных записей пользователей и групп пользователей из существующих корпоративных каталогов LDAP.

Эта система также выполняет централизованный контроль доступа и аутентификации на основе ролей для всех web-объектов, находящихся на нескольких web-серверах Microsoft IIS/NT, что позволяет компаниям внедрять и организовывать управление защищенными приложениями Экстранет быстро, просто и с минимальными затратами. Данное решение также можно установить на сервере Virtual Vault Proxy с целью контроля доступа, аутентификации и полномочий на внутренних web-серверах, находящихся внутри зоны безопасности Virtual Vault.

Инфраструктура открытых ключей (PKI)

Несмотря на наличие многих позитивных факторов, продвигающих новые идеи Интернет-бизнеса, проблемы безопасности все еще остаются основным препятствием для их успешной реализации. Однако, сейчас новые виды систем безопасности позволяют компаниям преодолевать эти ограничения и применять в Интернет новейшие подходы к организации бизнеса и предоставлению электронных услуг. Эксперты в этой области и руководители компаний единодушны в том, что в число наиболее эффективных технологий обеспечения безопасности входит инфраструктура открытых ключей (PKI). Использование технологии PKI позволило компаниям совершенно иначе использовать Интернет: теперь они могут предоставлять дифференцированные и безопасные электронные услуги, а также снизить текущие эксплуатационные расходы. С помощью PKI компании могут:

- безопасно выполнять важные транзакции в интерактивном режиме;
- обеспечивать безопасность конфиденциальной связи через Интернет;
- защищать порталы Экстранет и Интранет, используя строгую проверку подлинности пользователей на основе сертификатов.

Инфраструктура открытых ключей (PKI) является комбинацией аппаратных и программных продуктов, политик и процедур. Она является основным звеном защиты, необходимым для функционирования электронного бизнеса, и позволяет удаленным пользователям безопасно обмениваться информацией с помощью цепочки доверительных отношений. Инфраструктура PKI основывается на цифровых идентификаторах, называемых «цифровыми сертификатами», которые действуют подобно электронным паспортам, связывающим индивидуальный секретный ключ пользователя с его открытым ключом.

Согласно прогнозу ведущей английской аналитической компании Datamonitor, в течение следующих нескольких лет на рынке систем безопасности услуги по внедрению PKI продемонстрируют очень высокие темпы роста. Одной из причин является большой потенциал, используемый PKI. Инфраструктура PKI необходима компаниям для безопасной передачи документов и ведения бизнеса, требующего максимально защищенного доступа к данным через Интернет — как внутри предприятия, так и в сетях Экстранет. Глобальным компаниям и интерактивным магазинам инфраструктура PKI требуется для безопасного проведения операций электронного бизнеса.

Для эффективной реализации защищенных приложений поставщики новых электронных услуг должны удостовериться в подлинности сторон, находящихся в режиме онлайн, обеспечить неприкосновенность отправляемых через Интернет данных и конфиденциальность хранения информации, а также подтвердить успешное выполнение транзакции. Пользователям требуется снижение риска и обеспечение надежности — возможности однозначно и достоверно связать электронный идентификатор личности с уникальным физическим лицом.

PKI предоставляет инфраструктуру безопасности, позволяющую реализовать эти критически важные функции и обеспечить для компаний требуемый уровень надежности. PKI проверяет подлинность сторон, поддерживает целостность данных, а также обеспечивает конфиденциальность и достоверность передачи информации. Таким образом, PKI обеспечивает такой уровень безопасности, который необходим незнакомым друг с другом пользователям для обмена информацией и безопасного выполнения транзакций через Web. PKI защищает web-приложения, электронную почту, передачу файлов, сообщения и другие средства коммуникации и ведения интерактивного бизнеса.

Система управления Инфраструктурой открытых ключей Praesidium PKI

Решение Public Key Infrastructure (Инфраструктура открытых ключей), базируется на системе UniCERT компании Baltimore. Решение HP PKI предоставляет компаниям все необходимое для внедрения усовершенствованной Инфраструктуры открытых ключей, предоставляющей возможность защиты широкого спектра приложений электронного бизнеса.

Компания Baltimore Technologies является ведущим в мире разработчиком Инфраструктуры открытых ключей и технологий электронной безопасности. Семейство продуктов HP также создавалось для защиты и обеспечения нормального функционирования электронного бизнеса во всем мире.

Центральной идеей в концепции электронной безопасности является система управления сертификатами UniCERT. Эта система необходима для расширения возможностей электронной торговли, поскольку она предоставляет комплексное

решение по обеспечению безопасности, устанавливая надежные взаимоотношения всех форм электронного бизнеса и средства управления ими.

UniCERT — это система управления сертификатами на основе определенных политик. Функция редактирования политик безопасности Secure Policy Editor в сочетании с централизованным управлением позволяет компании определять политики доступа в рамках инфраструктуры открытых ключей (PKI).

Редактор Secure Policy Editor и централизованное управление обеспечивают гибкость, направленную на удовлетворение постоянно изменяющихся потребностей компании.

Система UniCERT поддерживает следующие стандарты и алгоритмы:

- Сертификаты стандартов X.509 v3 и CRL v2 (списки аннулированных сертификатов).
- Протоколы DAP, LDAP v2, v3.
- Сообщения PKIX.
- Агент системы каталогов DSA.
- ECDSA.
- PKCS#1 Стандарт шифрования RSA.
- PKCS#5 Стандарт шифрования на основе паролей.
- PKCS#7 Стандарт синтаксиса зашифрованных сообщений.
- PKCS#8 Стандарт синтаксиса информации с конфиденциальным ключом.
- PKCS#9 Выборочные виды атрибутов.
- PKCS#10 Запрос на сертификацию RSA.
- PKCS#11 Смарт-карты и маркеры.
- PKCS#12 Передача ключей.

Так как система Certification Authority (CA) является центральным звеном систем защиты, необходимо, чтобы она обладала высоким уровнем безопасности. Ведь если она уязвима для внешних или внутренних атак, риску подвергается вся инфраструктура открытых ключей. Система CA должна соответствовать следующим требованиям:

- Защищенность конфиденциальных ключей шифрования.
- Защищенность от атак извне, направленных на генерирование ложных сертификатов.
- Отказоустойчивость в случае перебоев с электропитанием, разрыва коммуникационных цепей, неправильного функционирования отдельных модулей.
- Индивидуальная отчетность операторов систем Certification Authority (CA) и Registration Authority (RA).

Обширный набор встроенных в UniCERT внутренних средств разработки гарантирует согласованность, постоянную доступность и высокую конфиденциальность информации. UniCERT PKI можно защитить с помощью контроля доступа на основе смарт-карт, обмена сообщениями с аутентификацией и аппаратных модулей обеспечения безопасности (HSM).

Секретные ключи систем CA и RA, а также их операторы защищены полнофункциональным шифрованием. Все данные, используемые в системах CA и RA, хранятся в базе данных, что облегчает их зеркальное копирование, восстановление, а также выполнение других распространенных операций, направленных на снижение риска потери информации в непредвиденных ситуациях. Любые факты взаимодействия между модулями UniCERT и записи в журнале имеют цифровую подпись и определенную степень защиты, что позволяет на их основе воссоздать реальную цепь событий, которую можно проверить и проконтролировать, но невозможно сфальсифицировать. Система UniCERT также предназначена для восстановления работоспособности в случае системных отказов и сбоев при обмене информацией.

Система UniCERT предоставляет следующие функции защиты:

- Поддержка широкого спектра аппаратных модулей HSM в системе CA для генерации конфиденциального ключа, безопасного хранения данных и подписи сертификата.
- Смарт-карты для безопасного хранения данных, контроля доступа и распределения ключей/сертификатов по всем важнейшим точкам инфраструктуры открытых ключей.
- Использование PKIX-сообщений для организации коммуникации между модулями.
- Полнофункциональное шифрование и цифровая подпись.
- Присвоение каждому сообщению и журналу регистрации сообщений уникального идентификационного номера.
- Все данные, ведущиеся в системах CA и RA, хранятся в базе данных Oracle. Использование этой широко распространенной БД существенно упрощает зеркальное копирование и восстановление данных, а также выполнение многих других операций, направленных на снижение риска потери информации в непредвиденных ситуациях, независимо от системы UniCERT.
- Возможность безопасной архивации пользовательских ключей шифрования, для того чтобы их можно было восстановить при необходимости восстановления зашифрованных данных.
- UniCERT принята на сертификацию в соответствии со стандартом ITSEC E3.
- Оборудование для шифрования.
- Восстановление данных.
- Архивирование с кодированием.

- Инструментальные средства защиты для разработчиков, которые могут использоваться в любом приложении.

Защита сети

Средства для организации виртуальных частных сетей VPN

Продукт Extranet VPN обеспечивает безопасность обмена информацией между удаленными пользователями и внутренней сетью компании благодаря аутентификации и шифрованию информации, передаваемой через Интернет. Решение Extranet VPN предоставляет компаниям возможность безопасно и экономически эффективно выполнять транзакции и передавать конфиденциальную информацию через Интернет клиентам, стратегическим партнерам и собственным сотрудникам.

Сети Экстранет с архитектурой «клиент/сервер» обеспечивают подключение отдельных пользователей к внутренним данным и приложениям компании, в отличие от схемы включения в сеть всех структур. Благодаря модели «клиент/сервер» Экстранет обеспечивает целостную безопасность, а не только возможность шифрования, а также позволяет осуществлять сложное управление пользователями и политиками. Сети Экстранет с архитектурой «клиент/сервер» предназначены для таких компаний, которым необходимо сформировать модель индивидуального учета сотрудников, сохранив при этом контроль над тем, кому и к каким ресурсам открыт совместный доступ. С другой стороны, в сетях Экстранет, построенных на модели LAN-to-LAN, наоборот, доминирует принцип доступа к ресурсам «все или ничего». В сетях Экстранет «клиент/сервер» производится четкая аутентификация каждого отдельного пользователя (а не только его IP-адреса), а доступ к конкретным ресурсам предоставляется в соответствии с подробным профилем пользователя. Шифрование является частью базовой инфраструктуры, поэтому аутентификация, контроль доступа и управление — это черты, характерные для любых реализаций модели клиент/сервер.

Модель клиент/сервер можно внедрять как в сетях Экстранет с поддержкой web, в которых в качестве клиента выступает браузер, так и в полнофункциональных сетях Экстранет, где применяется специализированное клиентское ПО.

Сети Экстранет, работающие на основе web, идеально подходят для обмена информацией. Подход, заключающийся в том, чтобы вся информация компании была доступна через браузер, приобретает все большую популярность, однако, для компаний, которые хотят использовать существующие системы, такой подход до сих пор представляет серьезную техническую проблему. Установка браузера в качестве интерфейсного приложения устаревшей системы или системы собственной разработки решает эту проблему только частично. Многие используемые в компаниях приложения поставляются со специализированными интерфейсами, обеспечивающими значительно более высокий уровень гибкости и скорости, чем написанные для них трансляторы в формат HTML, что ограничивает функциональность и возможности работы в диалоговом режиме. Кроме того, многие компании не всегда готовы обучать своих сотрудников для работы с новыми системами.

Если компании не ограничены условием использования установленных приложений и заинтересованы лишь в средстве распределения информации, создание сети Экстранет на основе web будет вполне логичным началом. Многие компании приступают к использованию Экстранет с рассылки информации только через web, постепенно внедряя полнофункциональные приложения «клиент/сервер».

Решение Extranet VPN предназначено для компаний, которым требуется многофункциональная сеть Экстранет, которая могла бы быть гладко интегрирована во все существующие системы. Функциональные возможности Extranet VPN не ограничены протоколом HTTP, а включают шлюзы между web-сервером и сервером приложений, прямой доступ к системам ERP, устаревшим системам и прочим приложениям, преобразование которых в формат web затруднительно. Кроме того, в основу этого решения заложена совместимость с новыми объектно-ориентированными web-технологиями, которые в будущем могут стать повсеместно принятым стандартом.

Система обнаружения вторжений ids/9000

Система обнаружения несанкционированного доступа IDS/9000 фокусируется на защите операционной среды HP-UX 11.x и используется для обнаружения проникновений в сетевой периметр. Рекомендуется использование системы IDS/9000 для защиты операционных систем важных серверов от проникновения или повреждения.

Предположим на сервере HP 9000 имеется какая-то система безопасности, защищающая ключевые места операционной системы, уязвимые для атаки через Интернет. Кроме того, во внутренней сети предприятия разработаны и внедрены дополнительные системы и элементы системы безопасности. Но как оценить насколько эффективна построенная защита?

Данная система обнаружения вторжений позволяет сообщать о проникновении в операционную среду HP-UX 11.x и выявлять подозрительные действия, которые могут нанести вред наиболее критичным компонентам Информационной ин-

фраструктуры — операционной системе и приложениям.

Внутреннее наблюдение

Система обнаружения вторжений дополняет другие установленные системы безопасности.

Если брандмауэры рассматривать как забор с калиткой, позволяющей пропускать персонал, наделенный соответствующими полномочиями, система обнаружения будет выступать в роли устройств внешнего видеонаблюдения и охранной сигнализации, которая включается, когда злоумышленник перелез через забор или выломал дверь калитки и теперь намеревается захватить центральный пульт управления. То есть когда основная угроза уже проникла внутрь и готовится из засады поразить жизненно важную систему.

Схема обнаружения несанкционированного доступа

Прежние методы регистрации несанкционированных действий были основаны на почерках атак. Однако, как и в случае с почерком письма, почерков атак может быть столько, сколько индивидуальностей среди злоумышленников. По некоторым оценкам на сегодняшний день зарегистрировано около 300 различных почерков атак. Это требует выполнения большого объема работы, нацеленной на поддержание актуального статуса информации о потенциальных почерках. Кроме того, это означает, что новые типы атак могут нанести серьезный вред до того, как соответствующие почерки атак будут идентифицированы, включены в каталог и занесены в файл почерков на автоматическое распознавание.

Компании HP удалось реализовать новый подход. Функции защиты выполняют схемы обнаружения HP, которые фокусируют внимание на областях уязвимостей. Именно такие области злоумышленники пытаются атаковать. Когда регистрируется событие, определенное в профиле, оно передается приложению корреляционного анализа, которое определяет, имеет ли место попытка проникновения. Технология корреляционного анализа — это еще одно изобретение HP. Этот уникальный комплексный подход к обнаружению несанкционированного доступа позволяет распознавать самые современные сценарии атак, а также некоторые будущие, еще не изобретенные способы. В систему может быть добавлено несколько различных систем обнаружения подозрительной активности, однако, максимальная степень защиты достигается в случае использования эксклюзивной системы обнаружения и системы распознавания несанкционированных действий.

Список уязвимостей

Ниже перечислены основные операции, которые могут обнаруживаться системой IDS/9000 и по которым могут генерироваться сообщения и предупреждения:

- Действия опасные для системы
  - несанкционированный доступ;
  - изменение ресурсов пользователей;
  - заражение вирусами;
  - изменение прав доступа;
  - запуск троянского коня;
  - использование прав супер-пользователя.
- ОС HP-UX
  - состояние процессов;
  - переполнение буфера;
  - нестандартное поведение демон-приложения;
  - попытки подбора пароля;
  - необычные состояния системы.
- Безопасность пользователей
  - ошибки регистрации пользователей в системе;
  - неудачные попытки получения полномочий супер-пользователя;
  - модификация пользователем А файлов пользователя В.
- Файлы
  - видоизменение файлов, помеченных как «только для чтения»;
  - модификация дозаписываемых файлов;
  - создание супер пользователем файла с разрешением на запись любым пользователям;
  - создание файлов «setuid»;
  - модификация и удаление файлов.

Распознавание проникновений и система предупреждений в реальном времени

Несанкционированный доступ определяется сразу, после того как предпринята соответствующая попытка, затем происходит генерация предупреждающих сообщений. Сообщения появляются в системе просмотра предупреждений, отображаясь в ней разными цветами в соответствии с тремя степенями опасности. В предупреждающих сообщениях атакующий идентифицируется по имени пользователя или IP-адресу. Такая идентификация удобна для определения ответных действий на основе политик безопасности. Предупреждающие сообщения заносятся также в журнал, который может быть изучен в системе просмотра предупреждений или сохранен в архивных целях.

Автоматизация ответных действий

Каждое предупреждение может инициировать выполнение определенных команд ОС HP-UX, которые могут использоваться и в других системах.

Например, может инициироваться отправка сообщения по электронной почте или на пейджер. Эти команды могут модифицировать календарные планы проведения контрольных проверок на немедленный запуск специальных приложений в системах управления безопасностью, общего управления предприятием или других прикладных программ. Инициируемые предупреждениями команды могут осуществлять коммуникацию с любым устройством, прикладной программой или процессом ОС HP-UX для инициирования требуемых ответных действий.

Функции управления

Графический интерфейс системы управления, дает возможность пользователю добавлять различные сервера и рабочие станции, а также группировать их. Например, могут быть созданы группы серверов для общего наблюдения, помеченные как «Серверы приложений» или «Серверы баз данных». После этого выбор, например, группы серверов приложений позволит осуществлять детализированный мониторинг или запускать специализированный календарный план контрольных проверок именно для этой группы серверов.

Календарные планы контрольных проверок, активные для каждой хост-системы, задаются с помощью графического интерфейса системного управления. Сочетание нескольких схем обнаружения образует группу наблюдения. Группы наблюдения могут выбираться из стратегических соображений по защите определенных хостов, таких как серверы приложений. Календарные планы контрольных проверок представляют собой группы наблюдения или шаблоны действий, привязанные к определенному времени выполнения. Календарные планы контрольных проверок удобны для запуска, остановки или модификации системы обнаружения несанкционированного доступа на основе операционной деятельности хоста. Например, для хоста, проходящего техническое обслуживание, может быть активирован календарный план контрольных проверок техобслуживания с временным прекращением выполнения схем обнаружения. Календарные планы контрольных проверок могут быть разработаны для операций резервного копирования, тестирования и техобслуживания. Календарные планы контрольных проверок могут относиться к специально помеченной группе серверов, например, серверам приложений или к отдельным хостам.

Инсталляция в режиме по умолчанию

Инсталляция системы IDS/9000 в режиме «по умолчанию» позволяет начать выявление фактов несанкционированного доступа, так как в систему встроены предварительно спланированные схемы обнаружения, группы наблюдения, календарные планы контрольных проверок и обработка предупреждающих сообщений. Кроме базовых функций существует возможность подстройки системы в соответствии с конкретными требованиями безопасности операционной среды.

Мониторинг источников данных

Система IDS/9000 позволяет анализировать контрольные данные ядра, которые генерируются внутренним компонентом ОС. Сюда относится анализ системных вызовов, включая входные и выходные параметры.

Мониторингу также подвергаются файлы системных журналов, поскольку содержат информацию о входе/выходе пользователей из системы, выполненных пользователями командах, отчеты от приложений-демонов сетевых сервисов, а также статистические записи передачи файлов по протоколам HTTP и FTP.

Весь обмен информацией, происходящий внутри системы IDS/9000, надежно защищен на базе использования протокола защищенных сокетов Secure Socket.

Layer (SSL). Протокол SSL обеспечивает также защиту системы обмена сообщениями клиент/сервер.

Области применения продуктов по обеспечению электронной безопасности HP

Применение решений по безопасности Praesidium и системы обнаружения вторжений IDS/9000 возможно в различных компаниях и отраслях бизнеса, на их основе можно построить безопасную систему электронной торговли, эффективно управлять корпоративными автоматизированными системами государственных и частных предприятий и организаций. В подтверждение этого продукты HP Praesidium установлены в более чем 110 учреждениях и предприятиях в разных странах.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Антонов А.Н. *(silver@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su
http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555