Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 12 (199)/2009

Новый игрок на рынке ИТ

КОРПОРАТИВНЫЕ СИСТЕМЫ

Новый игрок на рынке ИТ

СОДЕРЖАНИЕ

В заключительном выпуске вы узнаете о решениях компании Huawei Symantec и компании «Инфосистемы Джет» в области информационной безопасности и строительства мобильных ЦОД.

Huawei Symantec Technologies — совместное предприятие, образованное в феврале 2008 года. В продуктовой линейке компании — три основных направления: системы хранения данных (SAN, NAS, унифицированные СХД, решения по виртуализации и др.), продукты для обеспечения сетевой безопасности (межсетевые экраны, системы анализа трафика, шлюзы безопасности и т.д.) и серверы, а также законченные комплексные решения (ЦОД, системы видеонаблюдения, специализированные отраслевые решения).

НОВОСТИ

Допуск к строительным работам

Компания «Инфосистемы Джет» получила Свидетельство о допуске к работам, которые оказывают влияние на безопасность объектов капитального строительства. Свидетельство подтверждает право осуществлять широкий перечень видов работ по строительству, реконструкции, капитальному ремонту, которые в соответствие с Приказом Минрегиона от 09.12.2008г. № 274 оказывают влияние на безопасность объектов капитального строительства.

Получение перечня допустимых работ является необходимым условием для всех компаний, осуществляющих строительную деятельность. Согласно Закону РФ от 22 июля 2008 года N 148-ФЗ «О внесении изменений в Градостроительный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» лицензии, выданные до 01.01.2009 г., будут действительны только до 01.01.2010 г. Регулирование строительной деятельности в области архитектурного проектирования, строительства, капитального ремонта и реконструкции, а также инженерных изысканий для строительства будут осуществлять саморегулируемые организации (СРО). Членам СРО будет выдаваться Свидетельство о допуске к определенным видам строительных работ, без которого осуществлять строительную деятельность с 1 января 2010 г. будет невозможно.

Свидетельство дает компании «Инфосистемы Джет» право осуществлять работы, в том числе, в области строительства ЦОД и прокладки кабельных систем в соответствии с новыми требованиями закона 148-ФЗ.

Oceanspace™ ISM Storage Management System – новые возможности по управлению системами хранения

Компания Huawei Symantec объявила в выходе нового программного продукта для управления системами хранения данных собственного производства Oceanspace™ ISM Storage Management System. Новая система позволяет производить поиск устройств в сети, контролировать возникновение неисправностей, удаленно настраивать системы хранения, управлять доступом, анализировать производительность устройств и сети. Система создана на основе технологии Java.

Стоит отметить, что новый программный продукт сочетает в себе простоту рабочего пространства с мощным функционалом по управлению СХД. Новый дисковый массив может быть введен в эксплуатацию в течение 5 минут благодаря встроенным в Oceanspace™ ISM мастерам первоначальной настройки. Система позволяет с легкостью переключаться между различными представлениями инфраструктуры хранения данных — от просмотра карты устройств до подробной статистики по производительности конкретного устройства с возможностью анализа узких мест. Система может контролировать до 128 устройств хранения.

Oceanspace™ ISM будет представлена в нескольких вариантах: версия для управления одиночными СХД (идет в комплекте с оборудованием), версия для управления корпоративной инфраструктурой, версия для управления облачными системами хранения, версия для организации и управления схемами защиты от сбоев. Присутствует возможность интеграции Oceanspace™ ISM с программными продуктами Storage Foundation и Scalable File System компании Symantec.

Oceanspace™ HDP3500 – новогодний подарок для малого и среднего бизнеса

Компания Huawei Symantec к новому году подготовила решение по резервному копированию данных Oceanspace™ HDP3500 для малого и среднего бизнеса. Данный продукт представляет собой удачную интеграцию дисковой системы хранения, сервера резервного копирования и программного продукта Symantec Backup Exec. Система интересна своей простотой и функциональностью. Oceanspace™ HDP3500 требует минимальной первоначальной настройки.

Система позволяет в автоматическом режиме производить резервное копирование по сети данных с серверов и рабочих станций под управлением операционных систем семейств Windows и Linux. Также, что немаловажно, поддерживается резервное копирование с платформ виртуализации от компаний Microsoft и VMware. В систему встроены модули для создания резервных копий данных таких программных продуктов, как SQL Server, Oracle, Exchange, Lotus Domino, DB2, Microsoft SharePoint, Windows Active Directory. Поддерживается шифрование хранимых данных по алгоритму AES.

Объем доступного пространства в стандартной конфигурации Oceanspace™ HDP3500 достигает 24ТБ, что достаточно для большинства компаний целевого сегмента. При необходимости дисковое пространство может быть расширено до 192 ТБ, что весьма неплохо для решения начального уровня.

Новый игрок на рынке сетевой безопасности

Александр Лопатин,
руководитель группы пресейл-инженеров Центра информационной безопасности, компания «Инфосистемы Джет»

Новый игрок на рынке сетевой безопасности

Появление новых брендов на рынке решений в области информационной безопасности далеко не редкость. Как правило, такие стартапы представляют инновационные продукты в узких рыночных и технологических нишах. Чаще всего судьба наиболее успешных из них — быть поглощенными одним из ведущих мировых вендоров, например, Cisco, IBM, Oracle или Symantec.

В этой связи образование компании Huawei Symantec — нового игрока рынка классических решений по сетевой безопасности — событие по-своему примечательное. Совместная активность гигантов рынков информационной безопасности — компании Symantec — и сетевых решений — компании Huawei — позволяет с уверенностью предположить, что бренд Huawei Symantec является изначально самоценным, и вероятность потери его самостоятельности невелика, по крайней мере, в ближайшей перспективе. Отчасти стремление Huawei и Symantec развивать новый самостоятельный бренд подтверждается мощным инвестиционным потоком: на сегодняшний день (спустя всего 2 года с момента своего создания) компанией образовано уже четыре научно-исследовательских центра (в Китае, США и Индии), а также учреждена специализированная лаборатория, занимающаяся вопросами защиты сетей и приложений.

Сегмент рынка сетевой безопасности крайне насыщен, между ведущими игроками идет жесткая конкурентная борьба. В этих условиях для того, чтобы новому бренду занять собственную рыночную нишу, предлагаемые продукты должны обладать, как минимум, богатым функционалом и привлекательными ценами. По заявлениям Huawei Symantec решения компании удовлетворяют обоим требованиям.

Компания «Инфосистемы Джет» обладает наиболее высокой компетенцией в России по решениям Huawei Symantec в области информационной безопасности. Давайте проведем экспертный анализ характеристик продуктов Huawei Symantec и посмотрим, насколько небезосновательны заявления вендора.

Комплексный подход к обеспечению сетевой безопасности

Компания Huawei Symantec предлагает собственную реализацию комплексного подхода к обеспечению безопасности базовой ИТ-инфраструктуры. Для оценки широты спектра решений вендора рассмотрим предлагаемые продукты с позиции лидеров рынка сетевой безопасности, например, компании Cisco, и их стратегии построения самозащищающейся сети (Cisco Self-Defending Network). Эта стратегия позволяет классифицировать всю продуктовую линейку по шести функциональным направлениям. Решения компании Huawei Symantec представлены в пяти таких направлениях.

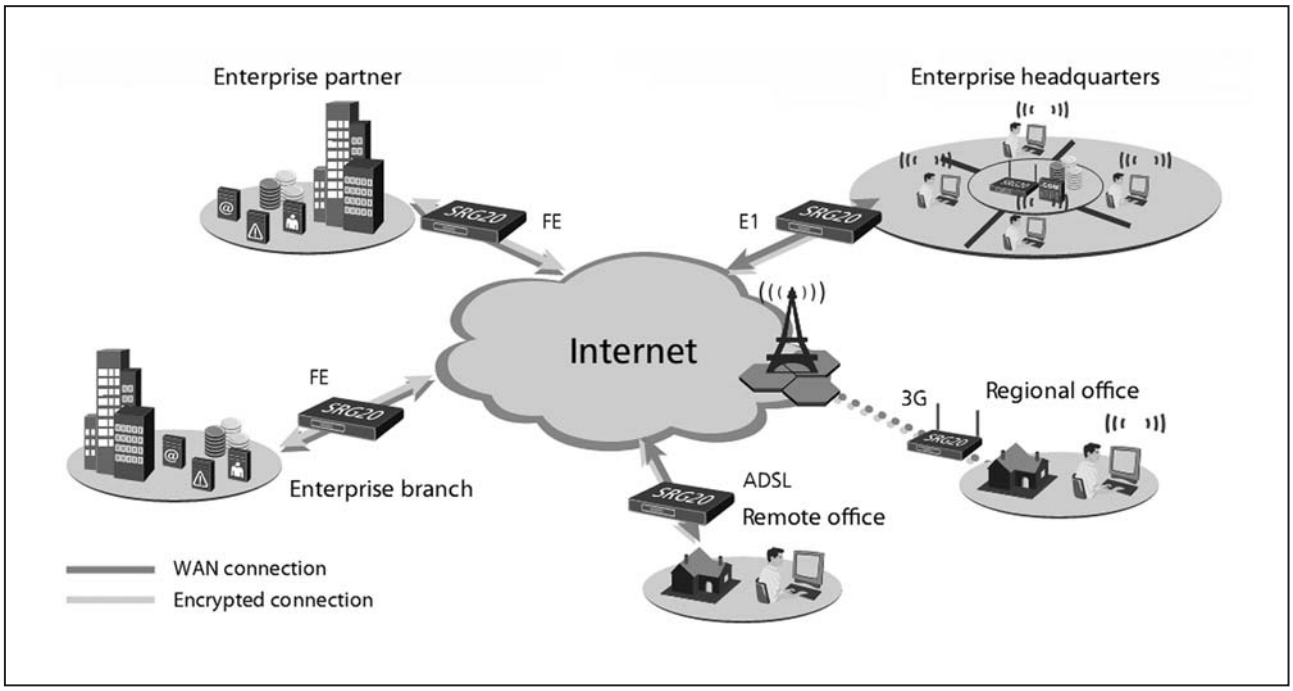

Рис. 1. Схема типовой сетевой инфраструктуры на базе решений Secoway SRG20

1. Защищенная сетевая платформа

В данной категории рассматриваются устройства, являющиеся основой при построении вычислительных сетей — маршрутизаторы, коммутаторы, точки беспроводного доступа и т.д. На данном направлении компания Huawei Symantec предлагает шлюзы безопасной маршрутизации Secoway SRG20. Решения серии SRG20 представляют собой комбинированные сетевые устройства, сочетающие в себе функции маршрутизации и коммутации с расширенными средствами обеспечения безопасности. По своим функциональным возможностям устройства Secoway SRG20 во многом схожи с маршрутизаторами Cisco ISR. Наряду со статической маршрутизацией, устройства SRG20 поддерживают протоколы динамической маршрутизации RIP, OSPF и BGP. Кроме того, устройствами поддерживается динамическая маршрутизация туннелей IPSec VPN. Производительность старших моделей линейки SRG20 достигает 500 тыс. пакетов в секунду (в режиме L3 forwarding), что сопоставимо с производительностью маршрутизаторов Cisco ISR серии 3800, позиционируемых в сегменте Large Branch — Medium Enterprise.

Решения серии SRG20 имеют следующие функции обеспечения безопасности:

- механизм контроля состояний (stateful inspection), предоставляющий защиту от DDoS-атак и атак на уровне приложений;
- интегрированный VPN-шлюз (IPSec VPN и SSL VPN);
- интегрированная система предотвращения вторжений;
- потоковый антивирус и антиспам (используются сигнатуры Symantec);
- функция URL-фильтрации;
- контроль трафика P2P и служб мгновенных сообщений.

Типовая схема построения распределенной сетевой инфраструктуры на базе устройств Secoway SRG20 представлена на рис. 1.

2. Сетевая безопасность

В этой категории рассматриваются выделенные защитные устройства: межсетевые экраны, средства построения VPN, системы предотвращения вторжений и т.д. На данном функциональном направлении компания Huawei Symantec представлена универсальными шлюзами безопасности Secoway USG (по функционалу устройства схожи с Cisco ASA), VPN-шлюзами SVN3000.

Универсальные шлюзы безопасности младшей серии (USG2000) объединяют в себе функции сетевого коммутатора, маршрутизатора, межсетевого экрана, шлюза VPN и беспроводной точки доступа. Такие решения могут использоваться для построения сетевой инфраструктуры компаний малого бизнеса, небольших филиалов крупных компаний.

Решения серии USG5000 обладают более высокой производительностью, что позволяет применять их в сетях средних и крупных пред-

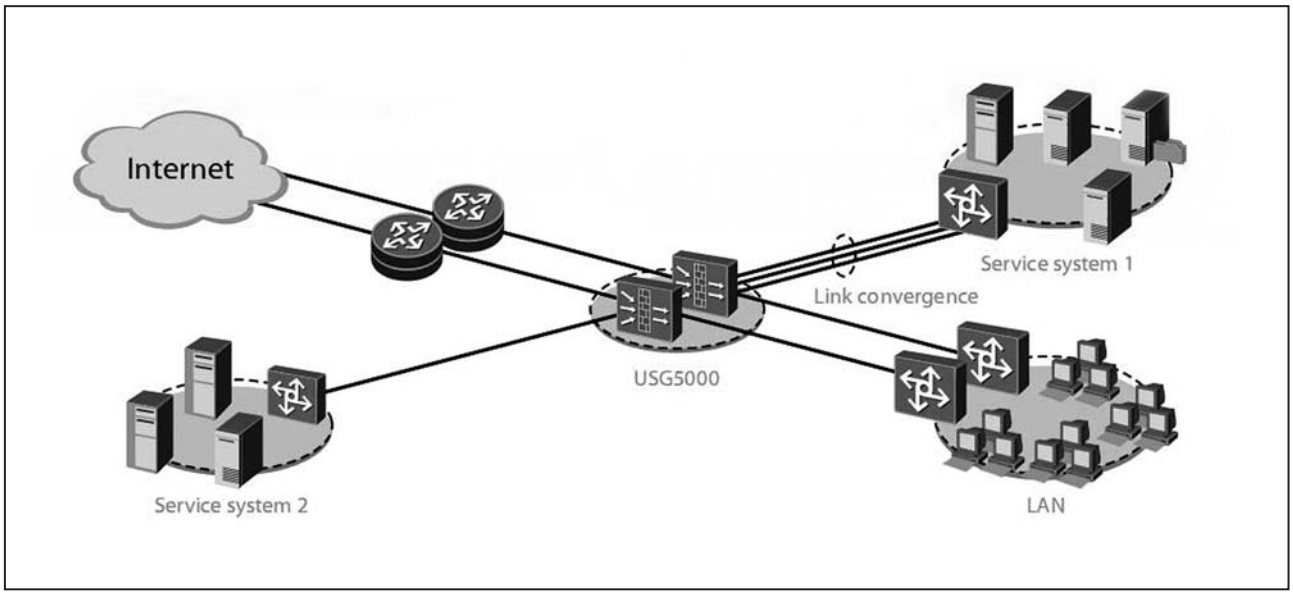

Рис. 2. Типовая схема использования устройств серии USG5000

приятий. Функционал позволяет организовывать отказоустойчивые сетевые решения с поддержкой резервирования и балансирования нагрузки. Типовая схема использования устройств серии USG5000 представлена на рис. 2.

Устройства серии USG9000 являются самыми производительными среди всей линейки USG. Они имеют модульную архитектуру, позволяющую на базе одного шасси использовать до 8 процессинговых модулей. Расширенные возможности по построению отказоустойчивого решения с высочайшей производительностью позволяют использовать устройства серии USG9000 для построения высокоскоростных сетей передачи данных операторов связи, для построения крупных центров обработки данных, а также в качестве основы при построении сетевой инфраструктуры крупных компаний.

Рассмотрим VPN-шлюзы Huawei Symantec. Устройство SVN3000 является классическим шлюзом для организации безопасного доступа по моделям Site-to-Site VPN (объединение в единую защищенную сеть нескольких распределенных филиалов одной организации) и Remote Access VPN (создание защищенного канала между сегментом корпоративной сети и одиночным пользователем). Модель Site-to-Site VPN реализована по технологии IPSec VPN, модель Remote Access VPN — по технологии SSL VPN, позволяющей удаленному сотруднику получить доступ к ресурсам корпоративной сети, используя только стандартный браузер операционной системы (т.е. без установки дополнительного ПО). Для аутентификации удаленных пользователей могут использоваться как встроенные механизмы (аутентификации по имени пользователя и паролю), так и внешние сервисы (RADIUS, LDAP, RSA SecurID, X.509 и др.). Кроме того, устройства SVN3000 поддерживают технологию виртуальных шлюзов VPN SSL (до 128 шлюзов). На рис. 3 представлена типовая схема применения продуктов серии SVN3000.

3. Доверенные оконечные устройства

Решение Secospace TSM является реализацией компаний Huawei Symantec технологии Network Access Control (NAC), позволяющей предоставлять доступ к информационным ресурсам только доверенным пользователям, использующим рабочие станции, конфигурации которых соответствуют требованиям политики безопасности компании.

Для получения доступа к ресурсам сети сначала пользователю требуется пройти процедуру аутентификации. Secospace TSM поддерживает аутентификацию на основе имени пользователя и пароля, MAC-адреса сетевого интерфейса рабочей станции и учетной записи LDAP. Затем в автоматическом режиме производится проверка соответствия конфигурации программно-технических средств рабочей станции пользователя требованиям политики безопасности. В случае успешного результата проверки пользователю предоставляется доступ к сетевым ресурсам, в противном случае — осуществляется блокировка и изоляция рабочей станции. На протяжении всего времени работы пользователя с защищенными сетевыми ресурсами ПО Secospace TSM

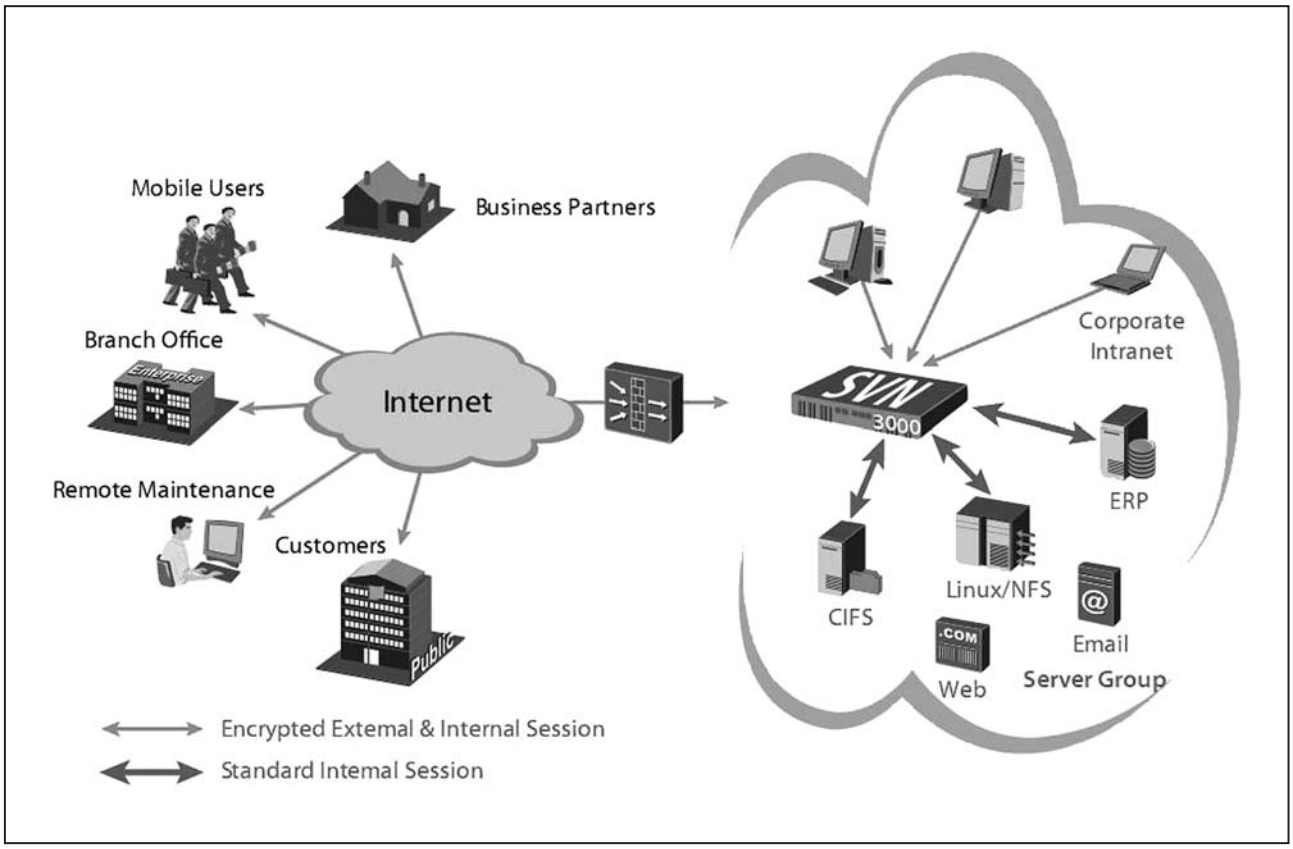

Рис. 3. Типовая схема применения устройств серии SVN3000

в прозрачном режиме осуществляет мониторинг действий пользователя, а также контроль изменений конфигураций программно-технических средств рабочей станции.

Secospace TSM состоит из следующих компонентов:

- Secospace Agent (SA) — клиентское ПО, функционирующее на рабочих станциях пользователей;
- Security Access Control Gateway (SACG) — аппаратный шлюз, контролирующий права доступа рабочих станций к сети;
- Secospace Manager (SM) — центральный программный компонент архитектуры Secospace TSM, обеспечивающий управление системой;
- Secospace Controller (SC) — программный компонент, обеспечивающий координацию модулей системы;
- Secospace Recover Server (SRC) — программный компонент, позволяющий приводить рабочие станции пользователей в соответствие требованиям политики безопасности.

На рис. 4 представлена типовая архитектура решения Secospace TSM.

4. Защита и контроль контента

В рамках стратегии Cisco Self-Defending Network в данной категории рассматриваются продукты для контроля и защиты электронной почты и веб-трафика. Среди продуктов Huawei Symantec отсутствуют выделенные решения класса Cisco IronPort, позволяющие решать подобные задачи, однако базовые функции антивирусной и антиспам проверок электронной почты, URL-фильтрации веб-трафика интегрированы в маршрутизаторы SRG20.

В этой категории Huawei Symantec позиционирует существенно более функциональные и производительные решения серии Secoway SIG 9800, предназначенные, в первую очередь, для сетей операторов связи. Решения построены на основе модульной платформы высокой доступности (>99,9999%). Платформа позволяет использовать до 32 многоядерных процессоров, обеспечивающих максимальную полосу пропускания 80 Гб/с. В Secoway SIG 9800 используется технология DPI (Deep Packet Inspection), позволяющая контролировать, помимо веб- и почтового трафика, передачу данных в пиринговых сетях (P2P), VoIP-телефонию, потоковое мультимедиа, трафик сервисов мгновенных сообщений, трафик игровых

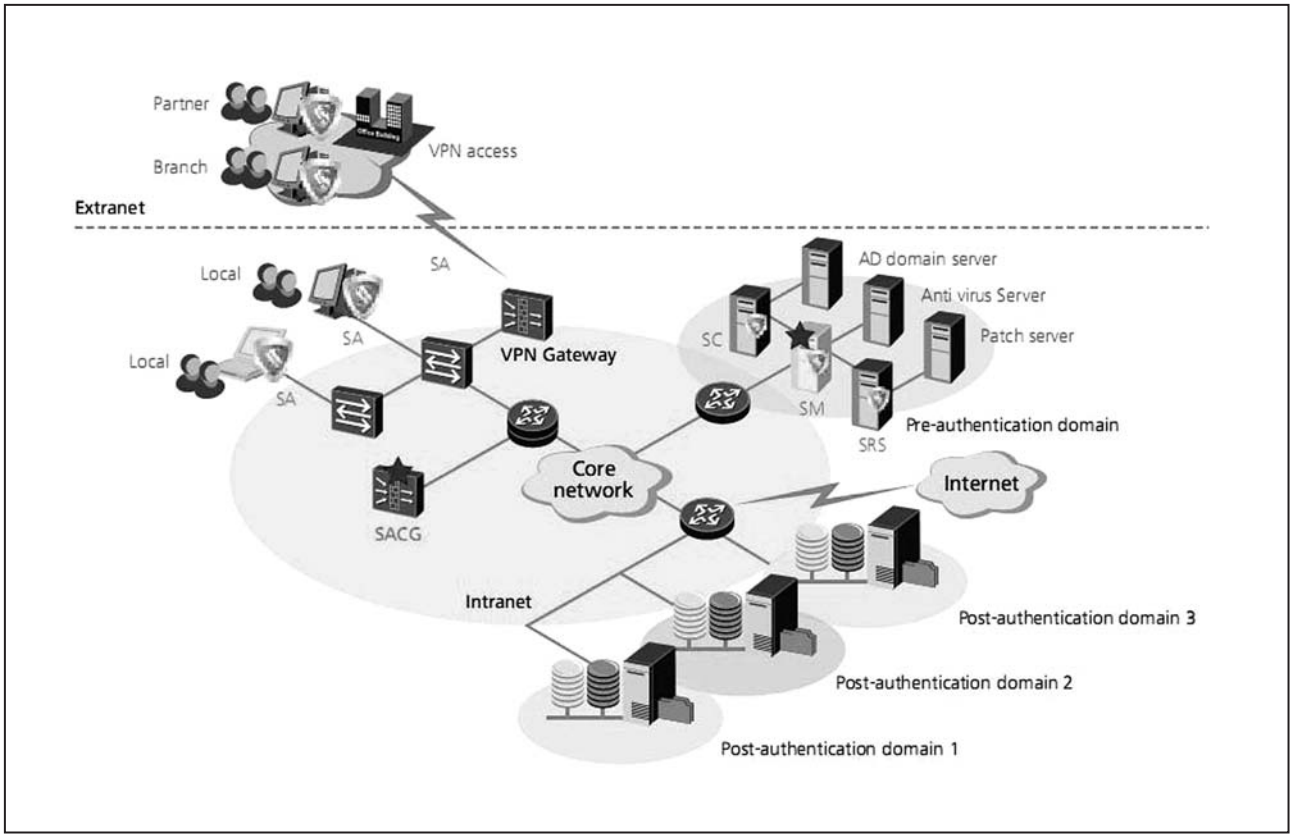

Рис. 4. Архитектура решения Secospace TSM

приложений и т.д. Данное решение предоставляет механизм управления полосой пропускания на основе гибко настраиваемых политик в привязке к конкретным пользователям, приложениям, целевым URL и времени. Необходимо отметить, что Secoway SIG 9800 позволяет обнаруживать и успешно бороться с трафиком сетевых червей, ботнет-сетей, спамом. Более того, на базе устройств этой серии возможно реализовать защиту от DDoS-атак.

5. Защита приложений

В данной категории рассматриваются решения класса Application Firewall, однако среди продукции Huawei Symantec они не представлены.

6. Управление, контроль соответствия, идентификация

В этой категории вендором представлено решение по мониторингу событий безопасности Secoway eLog. Продукт позволяет централизованно собирать и анализировать протоколы работы сетевых устройств Huawei Symantec, а также других устройств, использующих стандартный протокол Syslog. Решение поддерживает стандартные для такого класса продуктов функции:

- выдача оповещений в случае обнаружения инцидентов безопасности;
- предоставление доступа пользователям системы на основе ролевой модели;
- поддержка распределенной архитектуры;
- генерация отчетности.

Организация защищенного документооборота

Компания Huawei Symantec имеет в своем активе продукт, который нельзя отнести к какой-либо из вышеперечисленных категорий — Secospace Document Security Management (DSM). Это решение позволяет организовать защищенный документооборот не только в рамках контролируемого периметра компании, но и за его пределами (при обмене документами с партнерами, клиентами, удаленными сотрудниками). Продукты со схожим функционалом имеются у компаний Oracle (Oracle Information Rights Management) и Microsoft (Microsoft Rights Management Services).

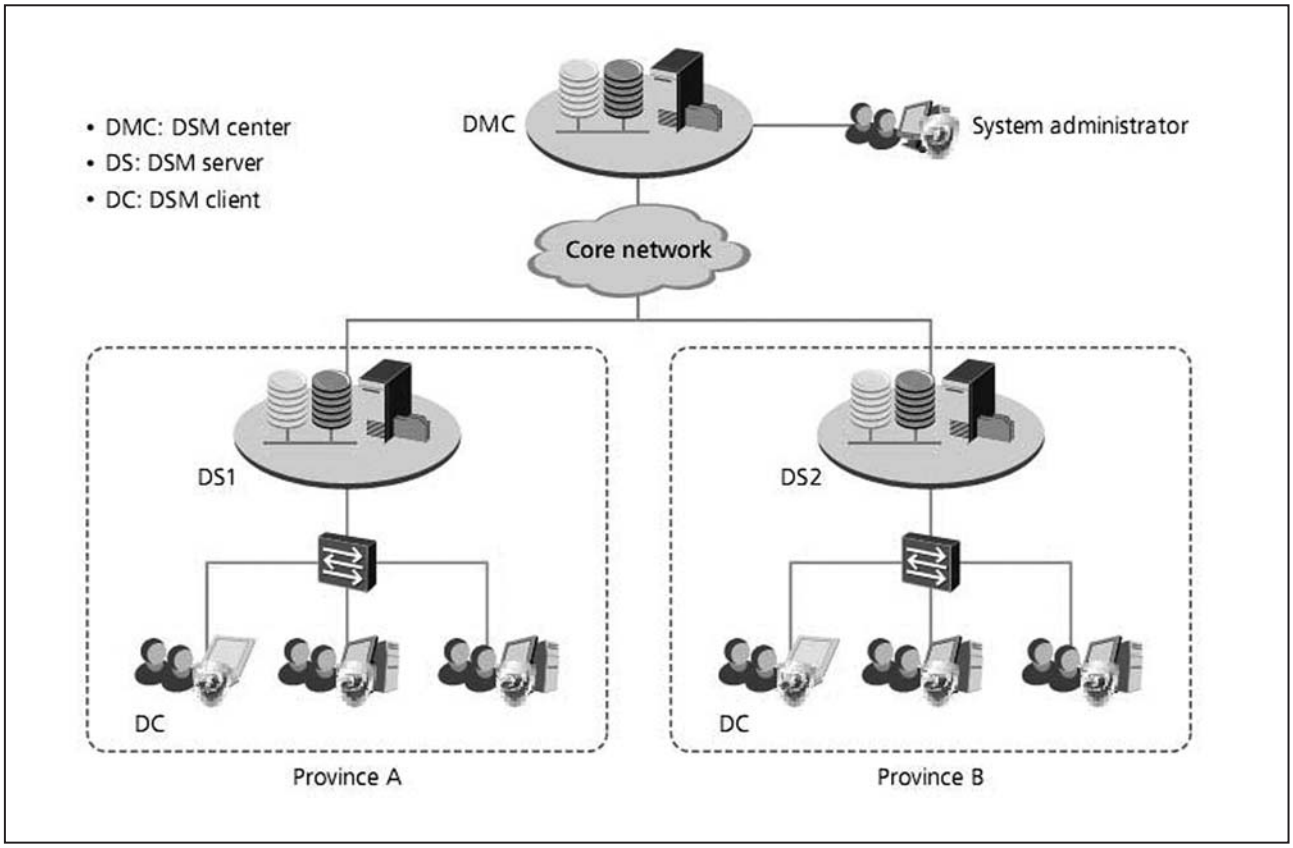

Рис. 5. Типовая архитектура решения Secospace DSM

Продукт Secospace DSM состоит из следующих компонентов:

- DSM management center — ПО верхнего уровня архитектуры Secospace DSM, отвечающее за координацию всех компонент системы, управление правами пользователей и управление инцидентами;
- DSM server — ПО, обеспечивающее аутентификацию и авторизацию пользователей, хранение ключей шифрования, мониторинг и аудит действий пользователей;
- DSM client — ПО, функционирующее на рабочих станциях пользователей, обеспечивающее процесс прозрачного шифрования и контроль доступа к документам.

Типовая архитектура решения представлена рис. 5.

Механизм работы этого решения следующий. При создании документа (в формате MS Office, pdf, jpg, gif) его содержимое зашифровывается, к документу прикрепляется метка, содержащая информацию о правах доступа, сроках действия этих прав и других атрибутах безопасности. При открытии такого документа клиентское ПО (DSM Client), функционирующее на рабочей станции пользователя, обращается к серверу Secospace DSM для подтверждения прав доступа и обмена ключевой информацией, после чего происходит расшифрование содержимого документа. При закрытии документ снова зашифровывается. Основным преимуществом такого подхода является то, что документ всегда хранится в зашифрованном виде, а это существенно снижает риск раскрытия конфиденциальной информации злоумышленником при перехвате файла, хищении носителей информации и ноутбуков.

Особенности продуктов Huawei Symantec

Пытаясь определить главную особенность продукции Huawei Symantec, в первую очередь, необходимо отметить более высокую производительность решений компании по сравнению с аналогичными решениями конкурентов, причем этот факт справедлив как для продуктов уровня SOHO и SMB, так и для продуктов уровня Enterprise.

Например, универсальные шлюзы безопасности серии Secoway USG5000 обладают пропускной способность до 8 Гб/с, имеют возможность обрабатывать до 2 млн. одновременных соединений и до 150 тыс. новых соединений в секунду, таким образом, позволяя защитить сетевую инфраструктуру, в том числе, и от DDoS-атак уровня Mpps (например, лавинные атаки SYN, UDP, ICMP, DNS), эти показатели соответствуют уровню старших моделей Cisco ASA серии 5580. При этом максимальное количество одновременных VPN-туннелей USG5000 составляет 20 тыс., и это вдвое превосходит возможности устройств Cisco ASA 5580. А топовое решение Huawei Symantec серии Secoway USG9300, строящееся по модульной архитектуре, позволяет добиться поистине беспрецедентной производительности: пропускная способность до 80 Гб/с, количество одновременных соединений до 32 млн. и до 2 млн. новых соединений в секунду.

Необходимо отметить, что зачастую многие решения компании помимо основного функционала обладают рядом особенностей. В частности, в том же шлюзе безопасности Secoway USG5000 реализован механизм защиты трафика GTP (GPRS Tunneling Protocol), этот функционал весьма востребован в сетях передачи данных телекоммуникационных компаний. Кроме того, шлюзы этой серии обладают функцией идентификации и управления трафиком P2P, позволяющей эффективно ограничивать такой трафик, тем самым гарантируя ширину полезной полосы пропускания каналов, также обладают возможностью фильтрации URL, функционалом IPS.

Маршрутизаторы серии SRG20 обладают расширенными возможностями работы с беспроводными сетями: наряду со стандартной поддержкой сетей Wi-Fi имеется возможность работы в сотовых сетях второго (GSM/GPRS/EDGE) и третьего поколений (HSDPA/WCDMA). К сожалению, в связи с небольшим уровнем проникновения сетей 3G на территории РФ, в настоящее время данный функционал является именно интересной особенностью, а не техническим преимуществом.

Компания Huawei Symantec является во многом технологическим последователем своих материнских компаний. В частности, в шлюзах безопасной маршрутизации используются антивирусные сигнатуры и антиспам-алгоритмы компании Symantec. Аппаратная составляющая продуктов Huawei Symantec основывается на платформах компании Huawei, хорошо зарекомендовавших себя в телекоммуникационной отрасли, благодаря высокой отказоустойчивости и резервированию критичных узлов.

Подводя итоги

Если говорить о продуктах компании Huawei Symantec в области информационной безопасности в целом, необходимо отметить широту спектра решений как с точки зрения функционала (универсальные шлюзы безопасности, VPN-шлюзы, шлюзы безопасной маршрутизации, решения по управлению безопасностью терминалов, решения по обеспечению защищенного документооборота), так и с точки зрения целевого потребителя (решения для малого, среднего и крупного бизнеса).

Очевидно, что компания Huawei Symantec представила рынку решения, обладающие высокой производительностью, интересными функциональными особенностями и демократичными ценами. Можно с уверенностью сказать, что такое сочетание характеристик способно привлечь внимание потенциального потребителя, особенно в условиях сложившейся экономической обстановки.

Huawei Symantec USG Unified Threat Management – гарант Вашей безопасности в 1U исполнении

Иван Перов,
Huawei Symantec

Сеть-полезна или опасна?

Какое-то время тому назад, обратившись к специалисту по сетям передачи данных, независимо от того, является он представителем крупного вендора, специализирующегося на производстве сетевого оборудования, или администратором небольшой корпоративной или домовой сети, с вопросом о том, что же такое сетевая безопасность, вы наверняка получили бы в качестве ответа (и в результате длительных графических представлений на листе бумаги) некую схему, пеструю от кружочков и ромбиков, облачков и «кирпичных стенок», а также соединительных линий различного вида между ними, где каждая из фигурок являла бы собой фаервол с антивирусом, коммутатор с маршрутизатором или какой-либо еще сетевой элемент... Но в целом, это был бы ответ на ваш вопрос, а именно: базовая концепция защищенной сети передачи данных.

Действительно, уже довольно давно необходимость защиты сетевых ресурсов, не только осуществляющих взаимодействие с Internet, но и потенциально открытых для различных атак, исходящих из других локаций в виде самых разных вредоносных программ и процессов, стала явной. В эволюции развития сетевого взаимодействия с применением различных технологий связи и протоколов, а также с ростом необходимости для различных бизнес-структур иметь возможность удаленного взаимодействия по сети, точка входа в корпоративную сеть стала также и точкой проникновения внутрь инфраструктуры большого количества вирусов и атак, направленных на самые разные элементы сети. Подобные интервенции могут преследовать самые различные цели: от понижения эффективности работы сети через DoS/DDoS-атаки и до попыток завладения конфиденциальной информацией, иногда приводящих к серьезным последствиям, таким как потеря средств, деловой репутации и интеллектуальной собственности. Все чаще атаки извне стали носить характер направленных, т.е. нацеленных на конкретные узлы и ресурсы, в целях не только хищения информации, но и нарушения работоспособности этих узлов, подмены или нарушения структуры данных. Нужно иметь в виду, что вопреки очень популярной точке зрения о «внешнем» характере большинства атак, большая часть вредоносных действий, как ни странно, исходит изнутри самой сети. По некоторым данным, от 60% до 80% всех деструктивных активностей, фиксируемых в современных корпоративных сетях передачи данных в последние годы, порождается внутри самих сетей.

Представьте себе, какой исчерпывающей информацией о внутренней топологии сети и логическом расположении систем хранения важной корпоративной информации могут обладать некоторые сотрудники конкретной организации, и какой потенциальный вред это может повлечь. Также большой вред может быть причинен сотрудниками неумышленно, в силу неправомерного использования тех или иных программ, паролей, внешних устройств и т.д., не заблокированных и используемых внутри организации по причине отсутствия эффективных механизмов и политик предотвращения их развертывания и нанесения ими ущерба ресурсам компании. Несанкционированный доступ сотрудников ко многим внешним ресурсам, таким как Bit Torrent'ы, YouTube и др., может существенно повлиять на производительность сети.

От разрозненной конкуренции – к унифицированным решениям!

Таким образом, понимая потенциальные риски, опасность и необходимость контроля за внутренними ресурсами, уже сейчас большая часть коммерческих и государственных организаций, иных структур, а также частных лиц, вне зависимости от географического положения, внедряют в своих сетях и на своих рабочих станциях самые различные механизмы защиты от атак, вирусов, а также несанкционированного использования своих ресурсов. Однако исторически развитие того или иного функционала в продуктах (программных или аппаратных) конкретных вендоров носило, как правило, довольно узкую направленность. В результате этого обстоятельства компании, предпринимающие попытки защитить свою сеть, учитывая весь комплекс предлагаемых средств и решений, необходимый для выполнения большей части задач по предупреждению, выявлению и предотвращению атак, а также восстановлению сети в результате совершенных атак, часто сталкиваются с рядом технических, бюджетных, административных и прочих препятствий. Мультивендорные решения могут оказаться чрезвычайно негибкими, дорогими и избыточными. С технической точки зрения очень нередки случаи программных и аппаратных несовместимостей различных продуктов, в силу отличных друг от друга способов реализации того или иного функционала различными вендорами. Следует также отметить, что с ростом сетевой инфраструктуры организаций, внедрением новых сервисов, и, так или иначе, усложнением внутренней структуры, также растут требования к автоматизации управления этими сервисами, в том числе и системами защиты.

В силу описанных выше обстоятельств, учитывая современные требования рынка, многие производители решений в области сетевой безопасности пришли к пониманию необходимости не только унификации некоторых протоколов и стандартов, но и разработки инновационных программно-аппаратных решений, основной концепцией которых являлась бы максимально возможная интеграция основного функционала различных элементов, выполняющих те или иные задачи обеспечения сетевой безопасности на базе одной платформы. Именно эти тенденции привели к появлению UTM, Unified Threat Management, определенного не очень точно, но, с точки зрения большинства вендоров, способного объединить в себе большую часть функций основных систем безопасности, используемых в современных сетях передачи данных, таких как фаервол, антивирус, механизмы AAA, а также Intrusion Detection/Prevention system (IDS/IPS).

UTM Huawei Symantec – богатый функционал в 1U устройстве

Решение UTM компании Huawei Symantec — это результат большой работы, проделанной в области разработок программного и аппаратного комплекса, оптимизации механизмов взаимодействия большого количества элементов, интегрированных на одну платформу, несущую функционал фаервола, IDS/IPS-систем, систем фильтрации различных типов траффика, спам-фильтров, антивирусов и включающую возможность эффективного дифференцирования и управления траффиком конечных пользователей на базе одной платформы, управляемой одной операционной системой.

UTM — это реализованный на базе фаерволов USG-серий 2000 и 5000 и включающий в себя, помимо базового функционала фаервола (простые и расширенные аксесс-листы, функция NAT/NAPT, поддержка до 12 настраиваемых и преднастроенных зон, поддержка статической и динамической маршрутизации RIP, OSPF, технологии VLAN, протоколов PPP, PPPoE, HDLC, функции DHCP, QoS), также ряд функций, позволяющих гибко управлять сетевым трафиком, обеспечивая максимально эффективные способы сетевой защиты.

Фаерволы USG 2000-й и 5000-й серий могут работать в режимах Routing, Transparent и Composite, тем самым адаптируясь под требования конкретной сети. Помимо прочих функций фаервола, также поддерживаются функции:

- Blacklisting;
- MAC-IP binding;
- FIFO, PQ, CQ, WFQ, CQC, CBWFQ, WRED, CAR;
- L2TP, GRE, IPSec, SSL VPN;
- ограничение на количество соединений по IP;
- статистика проходящего трафика и атак;
- отслеживание и ограничение трафика типа P2P;
- огранричение по скорости для доступа к ресурсам типа YouTube, BitTorrents;
- механизмы AAA (RADIUS, HWTACACS);
- IDS/IPS;

- фильтрация e-mail посредством Real-time Blackhole list (RBL).

Возможность распознавания и анализа протоколов уровня приложений позволяет устройству фильтровать весь нежелательный трафик внутри сети, например, ограничивать использование сотрудниками ресурсов развлекательного толка.

Устройства UTM поддерживают протокол VRRP, применение которого позволит обеспечить резервирование по схеме Active-Standby, что существенно повысит отказоустойчивость сети.

Высокочастотный процессор, выполненный в соответствии с современными стандартами, обеспечивает высокую производительность, что крайне важно для быстрой обработки трафика, в соотвествии с настроенными политиками, в том числе и для обработки заголовков уровня приложений. База данных сигнатур позволяет оперативно отслеживать вирусы и имеет возможность обновления.

Механизмы защиты от DoS/DDoS-аттак позволяют защитить сеть от таких неприятностей, как SYN flood, ICMP flood,UDP flood, Fraggle, Smurf, WinNuke, IP Spoofing, ARP spoofing, ARP flood. Фаерволы Huawei Symantec могут управляться как через GUI, так и через CLI операционной системы VRP локально консолью или удаленно по Telnet или SSH. Серия USG5000 поддерживает протокол GTP, таким образом появляется возможность использования этих устройств в PS Core сотового оператора на Gn- и Gp-интерфейсах. Данная линейка оборудования Huawei Symantec позволяет осуществить конфигурации до 4 Gigabit Ethernet + 10 Fast Ethernet портов для серии USG 2000 и вплоть до 8 Gigabit Ethernet портов для серии USG 5000. Также поддерживаются 3G интерфейсные платы, платы ADSL2+ и E1/CE1. Данные платформы представляют собой 1U решения, что существенно экономит место в стойке, а революционно низкое потребление электроэнергии (~35 Вт для USG2000 и ~100 Вт для USG5000) делает данные устройства лидерами по экономичности в своем классе.

Продукты UTM компании Huawei Symantec ориентированы на представителей крупного и среднего (USG5000) и среднего-малого (USG2000) бизнеса. Возможность гибкой конфигурации программного обеспечения и плотности портов позволяет максимально удовлетворить потребности заказчика.

Нужно отметить, что компания Huawei Symantec придерживается гуманистической концепции, вследствии чего использует для своего оборудования антирадиационные материалы, отвечающие электромагнитным стандартам и уменьшающие электромагнитную радиацию, создавая для заказчиков здоровую и благоприятную рабочую обстановку.

ЦОД в отдельно взятом контейнере

Алексей Панкратов,
Huawei Symantec

Современные бизнес-задачи становятся все более требовательны к ИТ-инфраструктуре, на которой они решаются. Надежным ядром такой ИТ-системы в настоящее время, как правило, является центр обработки данных (ЦОД). Так ли необходимо тратить время и деньги на строительство традиционного ЦОД?

Согласно сложившейся терминологии, ЦОД – специализированное здание (площадка) для размещения серверного и коммуникационного оборудования и подключения к каналам сети Интернет. Таким образом, в классическом понимании ЦОД это то, что строится «на века» и допускает только лишь замену собственно оборудования на более современное без каких-либо значительных архитектурных изменений. Обычно ЦОД размещается в отдельном здании или занимает его часть. Такие ЦОДы отличаются использованием отработанных технологий, но требуют значительных затрат по времени на строительство. Однако, если потребуется сменить месторасположение ЦОДа (например, вследствие переезда компании), то приходится снова вкладываться в строительство новой площадки и терпеть убытки от непредоставления услуг.

Кроме прочего, в последние годы все более остро встают вопросы нехватки площадей, дефицита и дороговизны электроэнергии, а также эффективности охлаждения.

Разработаны и успешно применяются методы для частичного или полного решения указанных проблем. Использование «зеленых» технологий позволяет снизить энергопотребление серверного и телекоммуникационного оборудования. Проектирование «горячих» и «холодных» коридоров повышает эффективность системы охлаждения. Аналогично существуют подходы для решения проблемы нехватки площадей: мобильные ЦОД.

Мобильный ЦОД – это продукт интеграции в стандартном транспортном контейнере всех элементов центра обработки данных. Контейнер уже включает в себя стойки с оборудованием, систему кондиционирования, пожаротушения, СКС и другие необходимые компоненты, хотя часть из них (например, внешние модули кондиционера или источник питания) могут располагаться отдельно снаружи. Место установки может быть выбрано не только в специально оборудованном помещении, но и на улице, позволяя, тем самым, ощутимо экономить на арендной плате. Благодаря компактной установке всех систем внутри контейнера уменьшается объем охлаждаемого пространства, что в свою очередь приводит к повышению эффективности системы кондиционирования и дополнительной экономии электроэнергии.

Еще одним очевидным преимуществом такого ЦОД является, как ни странно, его мобильность и время развертывания. Порой бывает необходимо разместить «кусочек» ЦОДа на удаленной площадке, подключить электричество и линии данных и в максимально короткие сроки получить полностью функционирующий Дата-центр. Такого рода задачи особенно часто возникают у телекоммуникационных и топливных компаний. Строить обычный центр обработки данных в таком случае никто не будет и мобильный ЦОД видится оптимальным решением. Кроме быстроты развертывания, немаловажным оказывается время свертывания и готовности к транспортировке (как в уже упомянутом случае переезда компании).

Другой нишей, в которой мобильный ЦОД является оптимальным решением, являются задачи плавного расширения и наращивания имеющегося Дата-центра. Рассмотрим следующую ситуацию: имеется некий классический ЦОД. Со временем, в условиях повышающихся ИТ-тре-

бований, владелец принимает решение построить еще один. Однако время не ждет, и потребности растут и, вполне возможно, начинают превышать возможности имеющегося ЦОДа, а новый еще не готов. В результате приходится говорить об упущенной прибыли. И вот новый ЦОД построен, все ИТ-потребности удовлетворены и созданы резервы (площади и электрические мощности) для дальнейшего роста. Но роста нет — разразился экономический кризис, сроки окупаемости увеличились, что теперь делать с избытком ресурсов? В данной ситуации вместо строительства традиционного Дата-центра наилучшим выходом было бы использование контейнерного ЦОДа для оперативного наращивания ресурсов небольшими ступеньками. Справедливости ради отметим, что контейнерные ЦОД не являются полноценной заменой классическим, и, рано или поздно, строить традиционый Дата-центр все равно придется.

В связи с упомянутым кризисом компании замораживают или вовсе отказываются от строительства ЦОД из-за довольно высоких капитальных затрат, в этом случае мобильный центр обработки данных им вполне по карману и может стать подходящим решением «здесь и сейчас».

Рис. 1. Транспортировка контейнера автотранспортом

Одним из важнейших направлений развития компании Huawei Symantec является предоставление законченных комплексных решений. Среди них особое место занимает мобильный ЦОД (см. рис. 1), в котором основной упор сделан на максимальной законченности и самодостаточности решения. В типовом решении для достижения минимальных сроков развертывания было решено отказаться от использования внешних модулей и разместить все необходимые компоненты внутри контейнера. В качестве системы охлаждения используется прецизионное кондиционирование, все блоки которого (включая испари-

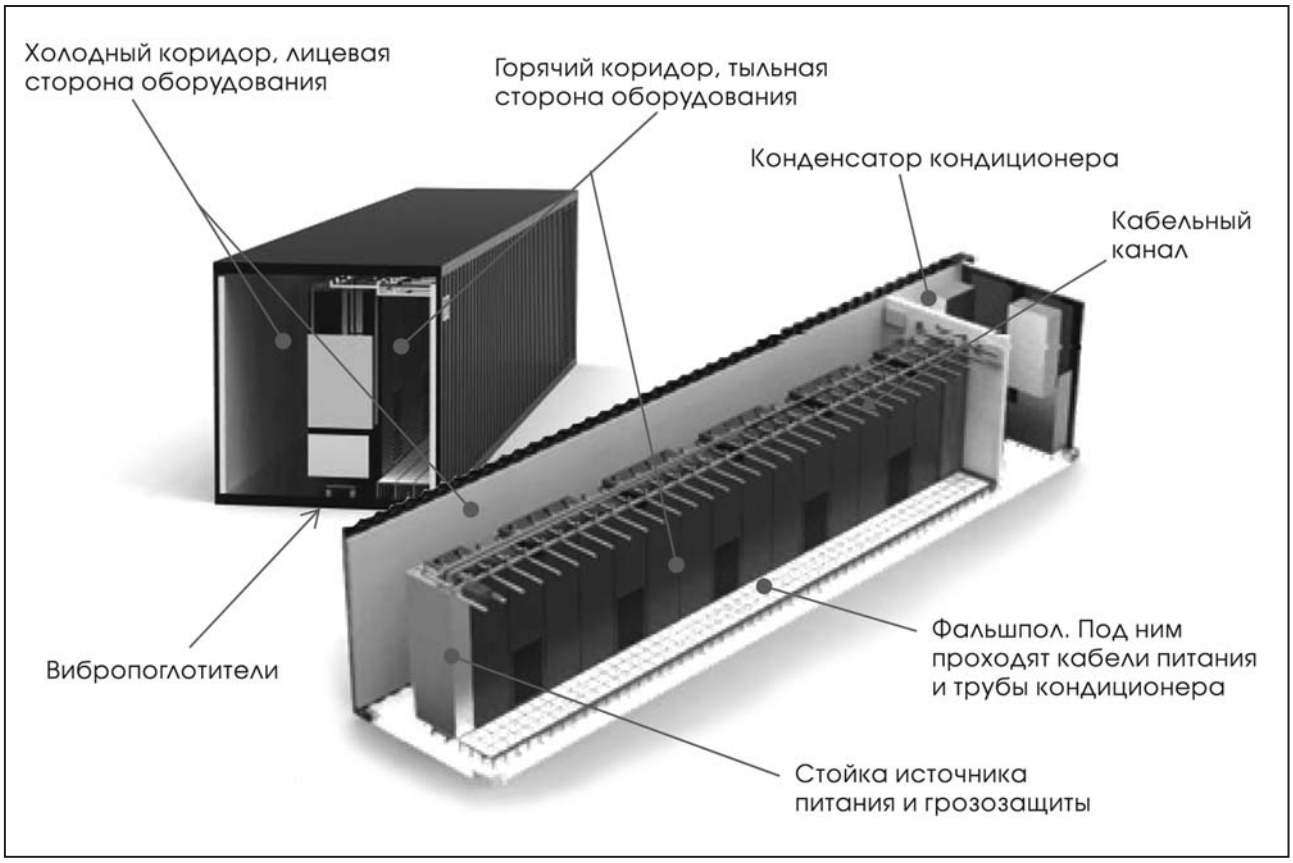

Рис. 2. Основные элементы контейнерного ЦОД

тели) размещены внутри контейнера, что невозможно при использовании водяного охлаждения.

Основными характеристиками типового решения мобильного ЦОД от компании Huawei Symantec являются:

- контейнер 40 футов, 10 стоек глубиной 800 мм;
- ввод питания: 380 В, до 350 А, 3 фазы + N + G, два независимых ввода;
- ввод данных:
  - 10 разъемов RG45;
  - 5 пар оптических разъемов (опционально);
- система газового пожаротушения;
- система прецизионного кондиционирования;
- две камеры видеонаблюдения;
- исполнение NEMA 3R, IP44;
- рабочая температура: от -35С до +45С;
- влажность от 30% до 80%;
- штабелирование до 3 этажей.

Несмотря на ограниченность пространства, стойки с оборудованием и кондиционеры расположены в ряд и образуют горячий и холодный коридор, что соответствует требованиям стандарта TIA-942 (см. рис. 2).

Чтобы обеспечить высокий уровень готовности к транспортировке, для крепления стоек применяются вибропоглотители, что позволяет не извлекать оборудование на время перевозки контейнера и тем самым значительно сократить время свертывания/развертывания.

Для ряда заказчиков наиболее интересным вариантом использования контейнера является размещение в труднодоступных, удаленных местах прямо на улице. В этом случае для предотвращения попадания в основное помещение пыли, влаги, снега и воздействия других неблагоприятных факторов организуется промежуточный входной тамбур. Если же необходима инсталляция «глубокого» оборудования, то при соответствующей перекомпоновке внутреннего пространства возможно размещение стоек глубиной 1000 мм.

Таким образом, контейнер может быть кастомизирован под любые требования заказчика. Гибкая ценовая политика компании в отношении контейнерных ЦОД делает это решение привлекательным не только для крупных, но и для небольших компаний.

Экспертное мнение

Вячеслав Карасев,
инженер-проектировщик отдела инженерных систем Центра сетевых решений, компания «Инфосистемы Джет»

Все большее количество зарубежных производителей приходит на рынок модульных центров обработки данных (ЦОД в контейнере, МЦОД) со своими продуктами. Идея уже перестала быть новой и ЦОД в контейнере воспринимается сейчас как полноценное, проработанное решение. Несмотря на то, что количество реализаций невелико, многие производители, стараясь не терять возможные рынки, разрабатывают все новые и новые решения в этой области. МЦОД обрастают громадным количеством патентов, что связано с новизной решений. Сейчас это большое поле для экспериментов. И, несмотря на их внешнюю схожесть (внешне — это все тот же морской контейнер), производители стараются предложить что-то новое для потребителя: новые эксплуатационные характеристики, разные уровни готовности решений, различные технические характеристики. Приходя на этот рынок, каждый новый игрок получает небольшое преимущество, т.к. может оценивать востребованность тех или иных предлагаемых вариантов, необходимость разработки новых, ориентируясь на уже созданные решения. Это совсем не означает, что каждый новый разработчик полностью копирует существующие продукты. Предлагаемые МЦОД очень разнообразны по внутренней инженерной инфраструктуре. Новые решения модульных ЦОД — это симбиоз уже реализованных ранее решений и уникальных, разработанных в рамках данного конкретного проекта. Является ли процесс изменений в МЦОД эволюционным? Наверное, нет. Процесс изменений, происходящий сейчас, — это поиск решений, способных заинтересовать потенциальных покупателей МЦОД. То, насколько востребованным будет предлагаемый вариант центра обработки данных, в конечном итоге определяет целесообразность его разработки и правильность принятых решений.

Основными характеристиками, которые отличают один МЦОД от другого, сейчас являются:

- форм-фактор используемого контейнера;
- показатель мощности на стойку с вычислительным оборудованием;
- количество стоек;
- глубина стоек;
- наличие обслуживающей инженерной инфраструктуры в предлагаемом решении (законченность решения).

Прочие характеристики являются второстепенными и характеризуют МЦОД со стороны удобства эксплуатации и наличия дополнительных опций:

- расположение стоек;
- организация внутреннего пространства контейнера;
- наличие интегрированной системы мониторинга, наличие единого интерфейса мониторинга;
- степень резервирования обслуживающих инженерных систем;
- наличие доп. опций в виде тамбуров-шлюзов, предустановленной структурированной кабельной системы и т.д.

Свое решение в этой области предложила компания Huawei Symantec — D-Box.

Приведенный рабочий вариант МЦОД D-Box представляет собой сорокофутовый морской контейнер. Контейнер предназначен для размещения 10 телекоммуникационных стоек глубиной 800 мм. Особенностью данного решения является то, что в состав оборудования инженерных систем входит полностью готовая к эксплуатации система кондиционирования. Внешние блоки кондиционеров размещаются в одной из торцевых частей контейнера. Часть контейнера с разме-

щенными в ней внешними блоками кондиционеров изолирована от пространства, предназначенного для размещения стоек. Внутренние блоки кондиционеров установлены в ряду со стойками. Общее количество внутренних блоков — 5 шт., производительность по холоду — 12,5 кВт на блок. С учетом необходимости резервирования оборудования системы получается 50 кВт на контейнер или 5 кВт на стойку в среднем. Организация воздушных потоков для охлаждения — спереди стоек назад (т.е. спереди стоек расположен холодный коридор, сзади — горячий). При построении системы кондиционирования использовано оборудование компании Emerson.

В составе решения не поставляется оборудование ИБП, предназначенное для организации бесперебойного электроснабжения вычислительного оборудования. С учетом того, что сеть электроснабжения для стоек и системы кондиционирования является общей, подвод «чистого» питания к контейнеру был бы не целесообразным (т.к. пусковые токи двигателей кондиционеров существенно ухудшали бы характеристики подаваемого питания). Поскольку возможности по теплоотводу со стойки для данного варианта решения невысоки (5 кВт в среднем), наиболее логичной является установка стоечных ИБП (ИБП 19-дюймового монтажа). Устанавливая ИБП в стойки, заказчик сможет самостоятельно определять степень резервирования ИБП, требуемое время автономной работы на аккумуляторах, отдавать предпочтение любому производителю. Ограничивающим фактором в выборе решений по бесперебойному электроснабжению и оборудованию ИБП является только ограниченное пространство контейнера. В одной из стоек установлен ИБП 2U, предназначенный для электроснабжения оборудования системы мониторинга контейнера.

Данная конфигурация контейнера не предусматривает заводской установки структурированной кабельной системы. Установка СКС в контейнер возможна после разработки эскизного проекта размещения активного сетевого оборудования, планов по масштабированию СКС и выбора производителя для построения системы.

Телекоммуникационные стойки (42U) крепятся к полу и потолку контейнера с использованием вибропоглотителей. Стойки расположены в один ряд. В отличие от решений других производителей, стойки в данной версии контейнера D-Box от Huawei Symantec не перемещаются, т.о. ширина холодного и горячего коридоров является фиксированной. Фиксированная ширина холодного коридора и глубина стоек накладывает определенные ограничения на использование «глубокого» вычислительного оборудования, что, собственно, и определяет область использования контейнера.

К числу прочих инженерных систем, которыми оснащен данный тип контейнера, относятся:

- система мониторинга, в составе:
  - 2-х датчиков температуры/влажности;
  - 2-х датчиков дыма;
  - 4-х датчиков открывания двери;
  - 3-х датчиков подтопления/протечки;
  - датчика потери электроснабжения;
- система газового пожаротушения;
- система видеонаблюдения (две камеры);
- система освещения.

Производитель заявляет возможность функционирования комплекса при внешних температурах от — 34 С до + 45 С, что делает возможной установку данного решения без внешних защитных сооружений на большей европейской части России. В качестве опции существует возможность перепланировки внутреннего пространства контейнера с целью выделения тамбура-шлюза, предназначенного для дополнительной защиты входа в контейнер. Количество установленных стоек при этом сокращается.

Адаптированность решения к зимним температурам, заводская готовность системы кондиционирования и отсутствие необходимости выделения площадей под обслуживающее оборудование выгодно отличают контейнер D-Box от большинства решений, предложенных другими производителями. Требуемую плотность монтажа вычислительного оборудования каждый заказчик определяет для себя индивидуально, в зависимости от целей использования решения, поэтому важным показателем в данном случае будет стоимость на кВт отводимой/подводимой мощности и стоимость юнита для установки оборудования. Будет ли решение востребованным — покажет время.

Автоматизация процессов поддержки ИТ-услуг Группы компаний «Детский мир»

О Заказчике

Группа компаний «Детский мир» лидирует в розничной торговле товарами для детей и подростков в России. Узнаваемый бренд, широчайший ассортимент и оптимальное сочетание цены и качества товаров помогают Группе удерживать ведущие позиции. Сеть магазинов «Детский мир» состоит из 126 форматных супер- и гипермаркетов в 68 городах России. Головной офис находится в Москве.

Практически сразу после открытия в 1957 г. старейшего универмага сети с товарооборотом в 93 миллиона рублей, что на тот момент было огромными деньгами, «Детский мир» сконцентрировал на своих площадях всю продажу детских товаров в Москве. А затем стал лидером этого сегмента рынка в стране.

Летом 2000 года с приходом в акционеры АФК «Система» началось возрождение национальной сети «Детский мир». В то время на рынке детских товаров не было ни одного крупного оператора.

Сегодня Группа компаний «Детский мир» входит в рейтинг «Топ-300 самых динамичных компаний России». А по данным за последние 5 лет ИД «КоммерсантЪ» и журнал «Секрет фирмы» поставили Группу на 3-место в отрасли потребительских услуг. При этом «Детский мир» опередил такие компании как «X5 Retail group», «Азбука вкуса», «АШАН», «METRO cash and carry».

Динамичное развитие потребовало применения лучших информационных технологий для построения эффективной операционной модели бизнеса, обеспечивающей устойчивое конкурентное преимущество. Сотрудники ИТ-департамента «Детского мира» демонстрируют высочайшую квалификацию, участвуя в реализации бизнес-стратегии Группы.

Задачи

В какой-то момент руководство ИТ-подразделения группы «Детский мир» осознало нехватку инструментов для воплощения всех своих стратегических планов. В частности, ИТ-департамент компании хотел накапливать единую базу знаний, которая помогла бы в кратчайшие сроки решать уже встречавшиеся ранее задачи и повышать компетенции сотрудников. Также была потребность в единой базе данных, содержащей необходимую для сотрудников информацию обо всей ИТ-инфраструктуре и связях между ее компонентами. Инструменты учета заявок были, но не хватало удобного поиска по базе данных и отслеживания связей заявок с элементами инфраструктуры. Нужна была возможность интеграции системы управления с почтовой системой, системой мониторинга, кадровой системой. Руководству ИТ требовалось больше управленческой информации для принятия решений.

Функционирование ИТ-инфраструктуры обеспечивалось наработанными процедурами, но требовало слишком больших усилий сотрудников, средства автоматизации применялись в недостаточном объеме. Например, подача заявок сотрудников на ИТ-обслуживание проходила через почтовую систему, они регистрировались диспетчером, который вручную распределял поток и фиксировал статистику обращений.

ИТ-специалисты компании «Детский мир» искали решение, которое могло бы дать им мощный инструмент управления, автоматизировать процессы ИТ-департамента. При этом не требовалось «с нуля» создавать методы управления, основные процессы и распределение ролей — эта задача к моменту старта проекта была успешно решена ИТ-департаментом.

Компания «Инфосистемы Джет» предложила заказчику решение поставленной задачи, и была начата совместная работа по созданию автоматизированной системы управления ИТ.

Сергей Кашинский, заместитель директора технического центра компании «Инфосистемы Джет»: «*Внедрение инструментов управления может оказать как положительное, так и отрицательное влияние на сложившуюся в организации систему управления ИТ. Изменение принципов деятельности часто не только влечет за собой тяжелый процесс адаптации сотрудников, но может стать и причиной серьезных сбоев в работе. Поэтому перед стартом проекта по автоматизации управления ИТ надо четко оценивать, насколько эффективны уже существующие бизнес-процессы, и стоит ли строить все заново. В нашем случае по результатам обследования выяснилось, что сформированная система управления работает, в целом, слаженно, и приоритетным стало сохранение основных сценариев работы сотрудников ИТ-департамента*».

Решение

На первом этапе проекта специалисты компании «Инфосистемы Джет» провели обследование существующих процессов управления ИТ. На основании полученной информации были разработаны рекомендации по оптимизации системы управления и необходимая документация. Были учтены не только существующие практики, но и перспективы развития системы управления.

Далее специалисты компании «Инфосистемы Джет» провели разработку, тестирование и развертывание на площадке ОАО «Детский мир — Центр» (управляющей компании Группы) системы автоматизации на базе ПО компании Hewlett Packard Service Manager 7.0. Решение было интегрировано с рядом внешних информационных систем, функционирующих в компании, таких как Active Directory, Lotus Notes, MS SMS.

Сергей Рогов, ИТ-директор Группы компаний «Детский мир»: «*Наша компания развивается, постоянно открывает для себя новые возможности, пробует разные методы работы. Кроме того, каждый сотрудник очень ответственно подходит к задачам и стремится к достижению личных профессиональных результатов. В такой активной творческой среде сложно было предупредить все изменения проекта, запрограммировать результат заранее. В ходе работы мы увидели перспективы развития системы и осознали для себя ценность их реализации*».

По результатам опытно-промышленной эксплуатации базовый функционал был существенно доработан. В итоге получилось решение, насыщенное полезными функциями, автоматизирующими работу сотрудников ИТ и их руководителей. Инструмент управления на основе HP Service Manager 7.0 содержит ряд таких полезных элементов, как оперативный контроль сроков выполнения заявки на обслуживание, в том числе через веб-интерфейс, контроль целевых параметров обслуживания, накопление централизованной базы знаний, накопление данных для составления отчетности и т.д.

Сергей Кашинский: «*Успешно завершенный в «Детском мире» проект в очередной раз подтверждает, что эффект дает не внедрение инструмента само по себе, а целенаправленное решение управленческой задачи. Профессиональная ИТ-команда в составе компании с огромной историей открыла новые возможности для бизнес-процессов и успешно взяла их на вооружение*».

При необходимости система управления может быть расширена благодаря масштабируемости программной платформы. Решение успешно прошло этап опытной эксплуатации и было тиражировано в Санкт-Петербургский филиал.

Результат

Основным итогом проекта стала оптимизация работы ИТ-службы по обработке пользовательских заявок. Важным результатом является также выстраивание механизмов принятия решений на уровне подразделения и компании в целом, а также повышение удовлетворенности конечных пользователей — сотрудников бизнес-подразделений компании.

Сергей Рогов, ИТ-директор Группы компаний «Детский мир»: «*Мы получили хорошую возможность для совершенствования своей работы, для постоянного повышения качества предоставления ИТ-сервисов сотрудникам нашей компании. Система управления облегчает работу всем нам*».

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Слободчикова Т.А. *(slobodchikova@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555