

ИБ для облачных сервисов на базе Vblock'ов

Рассматриваются вопросы, связанные с информационной безопасностью (ИБ), при развертывании облачных сервисов на базе пакетированных, полностью виртуализированных, интегрированных VCE Vblock-платформ. В настоящее время при построении ИТ-инфраструктур на их основе предлагается весь необходимый функционал и отчетность для удовлетворения требований в области ИБ, например, таких стандартов, как: PCI DSS, HIPAA, SOX (GLBA), FISMA и ISO.

Данная публикация подготовлена на основе материалов, предоставленных компаниями EMC, Cisco, RSA, VMware, а также комментариев: Антона Жбанкова (EMC), Александра Чигвицера (RSA), Родиона Тульского (VMware), Александра Скороходова (Cisco), Олега Ковержнева (Cisco).

Введение

Тема информационной безопасности — одна из самых актуальных при рассмотрении вопроса о миграции на виртуальные инфраструктуры, которая, по оценкам многих опросов, занимает первые места среди других “чувствительных” проблем СІО. “Масло в огонь подливают” и ряд исследований. Так, например, компания Gartner в начале 2010 г. опубликовала отчет, связанный с безопасностью виртуализации (“Addressing the Most Common Security Risks in Data Center Virtualization Projects”, январь 2010 г.), в соответствии с которым, к 2012 г. 60% виртуализированных серверов будут защищены в меньшей степени, чем физические серверы, которые они заменяют. Но к 2015 г., как отмечает Gartner, эта величина снизится до 30%, и этому есть объективные предпосылки.

Однако технологии развиваются столь стремительно, что ситуация может существенно измениться не только за год, но и за 6 месяцев и менее. VCE-альянс (Virtual Computing Environment Company — образован Cisco и EMC с участием VMware и Intel) — один из первых, кто вышел на рынок виртуализированных пакетированных интегрированных предустановленных решений для развертывания облачных сервисов (SN №№ 1-4 (41-44) за 2010 г.). И в настоящее время Vblock-платформы от этих четырех вендоров имеют весь необходимый функционал и отчетность для удовлетворения требованиям в области ИБ, например, таких стандартов как: PCI DSS, HIPAA, SOX (GLBA), FISMA и ISO. В качестве примера можно привести множественные имплементации на базе Vblock'ов одного из крупнейших голландских банков — ING.

Необходимо заметить, что бытует распространённое мнение, что самое главное — изучить лучшие практики/рекомендации и следовать им, забывая при этом о том, что реализация этих рекомендаций без поддержки специализированных решений/технологий может стать трудно выполнимой задачей, вследствие ее сложности, недопустимой длительности из-за большого количества ручных операций, дополнительных затрат на персонал, отсутствием требуе-

мой отчетности, онлайнности и др. Таким образом, одними правильными советами без технологической поддержки на уровне решений многих проблем ИБ при построении ИТ-инфраструктур не решить!

Развитие ИТ-отрасли неразрывно связано с переходом на получение гибких ИТ-услуг, предоставляемых в любом месте, в любое время, независимо от типа клиентского устройства, и с оплатой только по факту использования, на базе частных и публичных облачных платформ. При этом необходимые ресурсы, как аппаратные, так и прикладное ПО (вместе с системным), для ИТ-услуги предоставляются по запросу — по схеме “оплата аренды по времени использования”. Основные преимущества для клиентов это: нулевые капитальные затраты на приобретение ПО и оборудования, снижение эксплуатационных затрат и одновременное повышение доступности, надежности, управляемости. В ряде случаев это также возможность доступа к ресурсам, которые ранее для определенных категорий компаний вообще были недоступны, например, библиотеки для НРС-моделирования, стоимость которых может составлять миллионы долларов. Подобный тип ИТ-услуг все больше связывается с термином “облачные”.

Vblock подобные решения после развертывания позволяют осуществлять все управленческие ИТ-инфраструктурой в полностью виртуализированной среде, что практически исключает необходимость какой-либо физической переконмутации оборудования, одновременно существенно упрощая само управление и масштабирование, сокращая издержки и время развертывания новых приложений/рабочих мест. В целом, такой подход позволяет максимально приблизить администрирование ИТ-инфраструктурой к бизнес-требованиям и уровню управления ею самими бизнес-менеджерами.

Если всего год назад ведущие разработчики ПО весьма неопределенно отвечали, что они предлагают для развития облачных ИТ-сервисов, то в настоящее время подобные предложения есть со стороны таких софтверных вендоров (и их партнеров) как: SAP, Oracle, Microsoft и многих др. Многие российские компании уже развернули свои почтовые сервисы на Google. Софтверные облач-

ные ИТ-сервисы (например, для андрэйдов) уже для большинства стали нормой. В России уже около десятка провайдеров предлагают все типы облачных сервисов (PaaS, IaaS, SaaS и др., в основном, на базе прикладного ПО Microsoft). К концу 2011 г. ожидается новая волна предложений облачных сервисов для массового применения.

Базой для современных ИТ-сервисов являются пакетированные высокоинтегрированные виртуализированные платформы, развиваемые, в основном, на базе стандартных серверов. Тезис “в любом месте, в любое время” для России остается во многом дискуссионным по причине неразвитости каналов связи в регионах. Вследствие этого, степень проникновения публичных облаков на российский рынок весьма невысока. Однако корпоративные ИТ-услуги давно “вышли” из концепции “один сервис — один сервер”, вплоть до полноценных внутрикорпоративных частных облаков.

Рассмотрим основные возможные причины, которые могут привести к снижению уровня ИБ при переходе на виртуальные инфраструктуры и облачные сервисы.

Причины снижения ИБ при переходе на виртуальные инфраструктуры и облачные сервисы

Одна из основных особенностей облачных ИТ-услуг, с точки зрения ИБ, — повышенный уровень возможной утечки информации, что связано с рядом причин. Во-первых: ИТ-услуги в публичных облаках поставляются с использованием общедоступных публичных разделенных каналов связи, поэтому понятие охраняемого периметра практически перестает существовать. При этом следует учитывать и тот момент, что технологии для злонameranного доступа к данным в каналах передачи постоянно совершенствуются. И, если до недавнего времени вполне хватало, например, SSL-протокола, то в современных условиях с переходом на глобально-распределенный доступ к данным/приложениям может требоваться шифрование с гораздо большей длиной ключа. Если же это невозможно происходит снижение уровня ИБ — вторая причи-

на. Поддержание шифрованного трафика (в распределенных сетях) может потребовать, в свою очередь, наличия в составе WAN-оптимизаторов соответствующего функционала.

В-третьих, в публичных облаках приложения могут обрабатываться у сторонней компании — провайдера — поставщика ИТ-услуг, который, в свою очередь, например, для развертывания собственных услуг может арендовать ресурсы у другого провайдера, и т.д. В этой ситуации контроль за действиями персонала (администраторов ИТ-инфраструктур) у провайдера со стороны клиента ИТ-услуг затруднен или просто невозможен.

Предоставление облачных ИТ-услуг возможно только на базе гибких, с точки зрения управления, высокомасштабируемых, высокоавтоматизированных виртуализированных датацентров. Виртуализация, повышая эффективность использования ресурсов, также и размывает физические границы, позволяя множеству приложений/ОС/процессов одновременно выполняться на одном физическом ресурсе, что снижает уровень их изолированности и повышает возможность злонамеренного доступа к ресурсам клиентов — это **четвертая** причина. Вдобавок к консолидации многих сервисов на одной физической машине, современные платформы виртуализации размывают само понятие "место исполнения" сервиса, виртуальная машина может свободно мигрировать в кластере, совершенно прозрачно для пользователей.

Пятой, и, наверное, главной причиной снижения уровня ИБ является отсутствие должного внимания (или даже полное отсутствие) к ИБ на стадии проектирования. Она кроется в том, что часто виртуальная инфраструктура предлагается взамен существующей. При этом предполагается, что все существующие политики/процедуры/технологии ИБ могут быть интегрированы в новую инфраструктуру. Однако это далеко не так. В виртуальной инфраструктуре в разы увеличивается число ИТ-компонент (виртуальные серверы/машины, виртуальные коммутаторы, виртуальные тома) и простой перенос политик просто невозможен. Так, например, лидирующие решения по управлению уязвимостями не поддерживают виртуальные инфраструктуры, а работают только с физическими IP-устройствами. Далеко не все антивирусные решения поддерживают хотя бы основные платформы виртуализации. С административной точки зрения тоже все далеко не так гладко — администраторы зачастую не понимают, насколько изменилась инфраструктура, поскольку в целях экономии не оплачивается обучение.

Проблема разделения ролей управления виртуальной инфраструктурой и доступа к данным для всех платформ виртуализации в полной мере вообще не решена, и при переносе обработки конфиденциальных данных в виртуальную среду острота проблемы утечки конфиденциальной информации резко возрастает. Это возникает, прежде всего, из-за наличия так называемого "суперпользователя" в лице администратора виртуальной инфраструктуры (АВИ), и в случае публичных облаков — просто инсайдеров, у которых

есть доступ к данным, хотя они и не являются АВИ. Основная проблема заключается в том, что АВИ могут получить доступ к обрабатываемым внутри виртуальных машин (ВМ) конфиденциальным данным, даже когда эти ВМ выключены. Мало того, при этом совершенно нет необходимости получать физический доступ к инфраструктуре виртуализации, а можно все сделать по сети. И, более того, суперпользователь может "замести следы", очистив логи системы виртуализации, а любые системы защиты, находящиеся внутри операционной системы ВМ, в этот момент выключены, т.е. он не только может получить доступ, но и скрыть информацию об этом. Виртуальную машину можно запросто перенести на другое физическое оборудование путем обычного копирования папки с файлами виртуальной машины. Все настройки виртуальной машины хранятся в файлах в доступном для чтения и редактирования формате, а файлы виртуальных дисков содержат в себе все обрабатываемые на виртуальной машине данные. Это справедливо для всех систем виртуализации.

Помимо АВИ, в виртуальной инфраструктуре угрозы могут исходить и от множества других случайных сотрудников компании. Так, благодаря появлению в ВИ процедуры типа vMotion — миграции ВМ, несанкционированный доступ к каналу связи в момент ее осуществления может привести к утечке данных или полной замене всех ее политик безопасности.

Аудит также может стать большой точкой. Большая часть регулирующих требований не делает различий между физической и виртуальной ИТ-инфраструктурами, хотя, например, в Payment Card Industry (PCI) Data Security Standard это уже пересматривается для того, чтобы включить соответствующие руководства для виртуализированных сред. Например, в версии 2.0 предусмотрены следующие требования к виртуальной среде:

- запрещение предоставления сотрудникам доступа к гипервизору;
- назначение минимально необходимого уровня прав доступа, например, администратор ВМ не может назначить ей другой vSwitch;
- разделение функций и сетей с разными уровнями безопасности. Например, нельзя использовать VLANs с 802.1Q, если у них разные функции или уровни безопасности (п. 2.2.1);
- запрещение совмещения тестовых и производственных сред.

Все приведенные обстоятельства требуют при развертывании виртуальных инфраструктур и облачных сервисов более тщательного подхода к обеспечению уровня ИБ, а в ряде случаев — новых решений и дополнительных усилий по интеграции для того, чтобы переход не привел к его снижению. Это, по оценкам многих аналитических агентств, — один из основных факторов, сдерживающих продвижение современных ИТ-услуг/решений на рынке.

Уровни ИБ в распределенных виртуализированных средах

Все решения ИБ можно разделить на две группы: 1-я — решения для текущей операционной работы в составе онлайн-приложений датацентра; 2-я — решения

для проведения аудита ИБ в соответствии с требованиями стандартов (мониторинг политик безопасности, удовлетворение регламентам и др.). Первую группу можно разбить на следующие уровни контроля за информационными потоками:

- датацентр (управление компонентами датацентра — серверы, сеть, хранение; управление доступом к данным/системам управления; управление ролевым доступом к компонентам инфраструктуры);
- доступ к данным/ИТ-услуге и передача данных между клиентом и датацентром;
- использования информации (клиентские места).

Все технологии должны максимально интегрироваться с виртуальной инфраструктурой и ее системами управления, обеспечивая весь требуемый функционал ИБ, подобный физическим средам. При этом администрирование политиками безопасности, ключами доступа, ролевые назначения и др. должны быть максимально отделены от управления самой инфраструктурой и, соответственно, между сотрудниками.

В зависимости от типов распределенных датацентров, предоставляемых ими услуг, интеграция всех технологий ИБ и точки управления ими могут носить самый разный характер. Однако есть ряд специфичных особенностей, характерных только для виртуальных инфраструктур и распределенных датацентров.

Рассмотрим, как решаются выше обозначенные вопросы и проблемы ИБ при развертывании ИТ-инфраструктур на основе базовых решений Vblock'ов с возможными опциональными расширениями при необходимости. Цель обзора — показать всеобъемлемость технологий и решений для обеспечения ИБ ИТ-сервисов, предоставляемых в режиме мультиаренды на базе современных виртуализированных платформ, а также специфические особенности этих решений при использовании виртуализации.

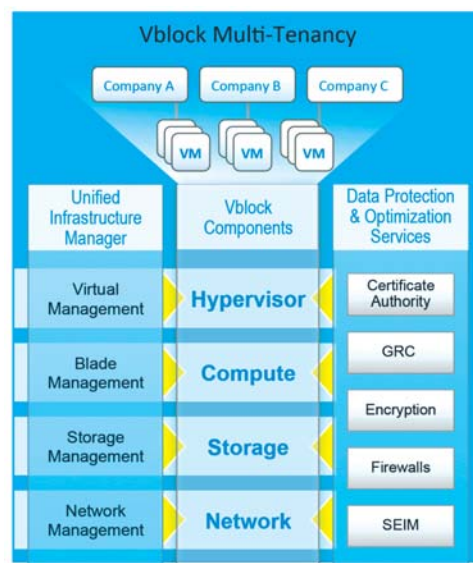


Рис. 1. Архитектура модели доверительной мультиаренды для Vblock-платформ.



Рис. 2. Шесть элементов модели доверительной мультиаренды для Vblock-платформ.

Обзор технологий ИБ для Vblock-платформ

Все решения и технологии для Vblock-платформ развиваются в рамках т.н. ТМТ-модели (Trusted Multi-Tenancy – доверительная мультиаренда), когда множество организаций совместно используют одни физические ресурсы (рис. 1) для получения ИТ-сервисов. Чтобы обеспечить выполнение этих фундаментальных требований, ТМТ-модель для Vblock-платформ строится на шести основополагающих элементах (рис. 2):

- Secure Separation – безопасное разделение;
- Service Assurance – сервисная гарантия;
- Security and Compliance – безопасность и комплайнс;

Табл. 1. Семейство технологий для разделения клиентов в мультиарендной инфраструктуре

Уровень инфраструктуры	Механизмы
Сетевой	Зонирование и виртуальные локальные сети (VLANs). Internet Protocol Security (IPsec) также обеспечивает независимое сетевое шифрование для приложений на уровне IP для дополнительной защиты
Вычислений	Интегрированные технологии в: Intel® процессоры, Cisco Unified Computing System™ (UCS) серверную инфраструктуру, VMware vSphere™ гипервизор
Храниения	Комбинация SAN-зонирования и Ethernet VLANs для обеспечения сегрегации, контроля и управления ресурсами хранения. Решения EMC также включают: шифрование при хранении; защиту передаваемых данных; изоляцию полосы пропускания, кэша и дисков.
Приложений	Специально разработанное приложение для мультиаренды или множество отдельных образов одного и того же приложения.

- Availability and Data Protection – доступность и защита данных;
- Tenant Management and Control – контроль и управление со стороны арендатора сервиса;
- Service Provider Management and Control – контроль и управление со стороны сервис-провайдера.

Первый элемент – Secure Separation – один из основных и обеспечивает эффективную изоляцию и сегментацию арендаторов и их активов в пределах среды мультиаренды.

Адекватное безопасное разделение гарантирует, что ресурсы существующих арендаторов остаются нетронутыми, а целостность приложений, рабочих нагрузок и данные не ставятся под угрозу, когда добавляются новые арендаторы.

С точки зрения сервис-провайдера, безопасное разделение требует системного развертывания различных механизмов управления защиты по всей инфраструктуре, чтобы гарантировать конфиденциальность, целостность и доступность данных, сервисов и приложений арендаторов. Логическая сегментация и изоляция активов и информации арендаторов являются основными для обеспечения конфиденциальности в мультиарендной среде. Фактически, гарантия секретности и защиты каждого арендатора становится ключевым требованием дизайнера в решении перехода на облачные услуги. Механизмы изоляции арендаторов на каждом из уровней инфраструктуры представлены в табл. 1.

В целях обеспечения непротиворечивых SLA через все компоненты инфраструктуры может использоваться следующий инструментарий: QoS in the Cisco Unified Computing System™ и Cisco Nexus® platforms, EMC Symmetrix® Quality of Service tools, EMC Unisphere® Quality of Service Manager (UQM) и VMware Distributed Resource Scheduler (DRS).

Весь набор технологий и решений, используемых для обеспечения решения всего комплекса требований и задач, представлен в табл. 2. Технологии и решения для ИБ тесно интегрируются с другими группами технологий. Вкратце остановимся на ключевых.

RSA Solution for Cloud Security and Compliance

Введенное в состав RSA-линейки около года назад и построенное на базе пакета RSA® Archer eGRC решение RSA Solution for Cloud Security and Compliance полностью интегрировано с платформой VMware, а также решениями EMC и дает возможность конечным пользователям, организациям и сервис-провайдерам оркестрировать и визуализировать безопасность их виртуальных VMware- и физических инфраструктур с одной консоли (рис. 3). Оно также позволяет обеспечить миграцию ИТ-инфраструктур из физической в виртуальную среду без какого-либо повышения рисков, с точки зрения ИБ.

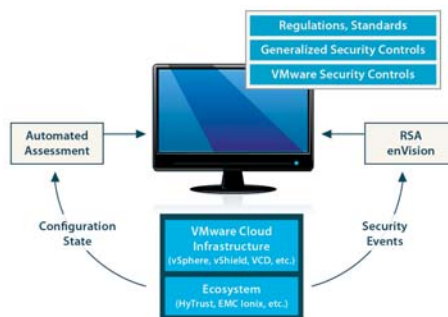


Рис. 3. RSA Solution for Cloud Security and Compliance обеспечивает единую консоль за мониторингом событий соблюдения политик безопасности и автоматизацию их назначения.

Табл. 1. Семейство технологий и решений для построения Vblock-платформ.

Management and Orchestration	EMC Data Domain®
Vblock Advanced Management Pod (AMP)	EMC Avamar®
EMC Ionix™ Unified Infrastructure Manager (UIM)	EMC Replication Manager
NimSoft Monitoring Solution	EMC RecoverPoint
	EMC RecoverPoint Storage Adapter for SRM
	EMC Data Protection Advisor
Security Technologies	
RSA Solution for Cloud Security and Compliance	
RSA enVision	
RSA SecurID	
RSA Authentication Manager	
RSA Data Loss Prevention	
RSA Data Loss Prevention Network	
RSA Data Protection Manager	
Cisco Virtual Security Gateway	
VMware vShield	
Cisco Adaptive Security Appliance	
Cisco Intrusion Prevention System	
Cisco Secure Access Control Server	
Storage Technologies	
EMC Symmetrix® V-MAX™	
EMC Symmetrix Management Console	
Symmetrix Priority Controls	
EMC Symmetrix Performance Analyzer	
EMC Fully Automated Storage Tiering (FAST)	
EMC Symmetrix Optimizer	
EMC PowerPath®/VE	
EMC Unified Storage	
EMC Unisphere® Management Suite	
EMC Unisphere Quality of Service Manager	
EMC Ionix Storage Configuration Advisor	
EMC Ionix ControlCenter	
EMC Virtual Storage Integrator	
EMC Networker	
Compute Technologies	
Cisco Unified Computing System	
VMware vSphere™	
VMware vSphere High Availability	
VMware vSphere Fault Tolerance	
VMware vSphere Distributed Resource Scheduler	
VMware vSphere Resource Pools	
VMware vMotion™	
VMware vCenter Server	
VMware vCloud™ Director	
VMware vCloud Request Manager	
VMware vCenter Configuration Manager	
VMware vCenter Site Recovery Manager	
VMware vCenter Capacity IQ	
VMware vCenter Chargeback	
Network Technologies	
Nexus 1000V Series	
Nexus 5000 Series	
Cisco Virtual PortChannels	
Nexus 7000 Series	
Cisco Overlay Transport	
Virtualization	
Cisco MDS	
Cisco Data Center Network Manager	
VLAN Separation	
Virtual Routing and Forwarding	
Hot Standby Router Protocol	
MAC Address Learning	
EtherChannel	

Процесс управления безопасностью и обеспечением регулирующих требований как для физических, так и виртуальных ИТ-инфраструктур, подобен, но важно отметить, что виртуализация предъявляет ряд уникальных требований. Одно из них – это большой динамизм изменений в виртуальной инфраструктуре, что, например, может быть связано с возможной миграцией виртуальных машин (ВМ) между физическими серверами. В связи с этим, политики безопасности сложно жестко привязать к физическим ресурсам и они, соответственно, должны динамически перемещаться за ВМ со всеми настройками.

В структуре новых версий стандартов типа PCI DSS 2.0 появились разделы, предъявляющие особые требования к политикам безопасности виртуальных инфраструктур, о которых говорилось выше.

Другим фактором, порождающим проблемы, при переходе от физических ИТ-инфраструктур к виртуальным, является то, что команды сотрудников по обеспечению безопасности и регулирующих требований часто отстранены от этапа проектирования виртуализированной ИТ-инфраструктуры. В результате этого, на этапе внедрения и эксплуатации компании несут незапланированные издержки вследствие:

- упущенной выгоды, когда внедрение проектов по виртуализации задерживается из-за их несоответствия регулирующим требованиям и безопасности;
- штрафов при проведении аудитов из-за невыполнения требований по безопасности виртуализированной инфраструктуры;
- снижения имиджа компании и доверия ее акционеров вследствие нарушения требований безопасности.

В конце августа 2010 г. RSA (подразделение EMC) анонсировала новое решение RSA Solution for Cloud Security and Compliance (RSA CSC), призванное минимизировать риски по безопасности и комплаинс при переходе на виртуализованные среды (на базе платформы VMware), в настоящее время — для частных облаков, в ближайшей перспективе будут расширения и для публичных. Основное преимущество нового решения в том, что, используя единую консоль на базе RSA® Archer™ eGRC platform, можно получить законченную оценку уровня безопасности и регулирующих требований для всей VMware виртуальной инфраструктуры. Оно также позволяет централизованно управлять безопасностью как виртуальной, так и физической инфраструктурами. Управляющая консоль интегрируется с более чем 100 библиотеками управления для VMware, которые отражают самые последние требования стандартов типа PCI-DSS, HIPAA, идентификации администрирования и др.

Платформа управления рисками и контроля соблюдения ИБ-политик RSA Archer совместно с другими своими решениями (это, в частности, платформа мониторинга событий информационной безопасности RSA enVision и система предотвращения утечки конфиденциальных данных RSA DLP) предлагает системный подход к обеспечению необходимого уровня безопасности при развертывании "облачных сервисов".

Основная идея, лежащая за предлагаемым RSA решением, заключается в строгом и формальном подходе к контролю состояния ИБ в облачной инфраструктуре:

- организация самостоятельно или с помощью внешних консультантов разрабатывает политики и правила, связанные с защитой данных в облачной инфраструктуре;
- данные политики формализуются и заносятся в платформу RSA Archer, которая использует их и будет сравнивать текущее состояние инфраструктуры (настройки, происходящие инциденты) с тем состоянием, которое требуется;
- RSA enVision и RSA DLP посылают уведомления и информацию о возникающих инцидентах ИБ в RSA Archer для обработки и определения по принятой методике текущего уровня угроз ИБ.

RSA® Archer eGRC Platform (eGRC – enterprise Governance, Risk, and Compliance) интегрируется с RSA enVision® log mana-

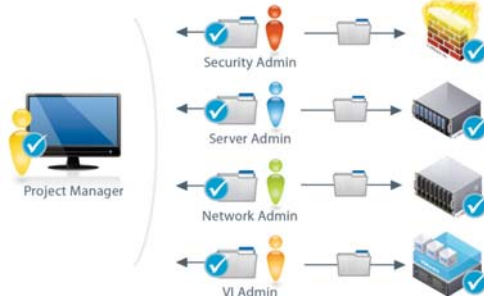


Рис. 4. RSA Archer eGRC Platform дает возможность менеджеру проекта распределять политики безопасности и управляющие процедуры соответствующим менеджерам.

gement, обеспечивая сбор и корреляцию событий безопасности и комплаинс от различных источников, включая RSA Data Loss Prevention suite, VMware vShield и VMware Cloud Director. Интеграция с другими инструментами, включая EMC Ionix® и HyTrust, будет добавлена в ближайшее время.

О степени доверия к платформе RSA enVision® может свидетельствовать тот факт, что логи RSA enVision® принимаются в качестве улик в судах США, известных возможностью опровергнуть и поставить под сомнение практически все, что угодно.

RSA CSC дает возможность рационализировать множество требований соглашения, управления структурами, стандартами и лучшими практиками в централизованный набор политик безопасности, который может быть использован в составе виртуальной инфраструктуры. Через автоматизированные назначения и простые технологические процессы решение упрощает процесс управления задачами между группами безопасности, которые определяют политики, и группами IT-операторов, ответственных за осуществление этих политик (рис. 4).

Пакет RSA CSC ориентирован как на конечных потребителей (компании), так и сервис-провайдеров, желающих оркестрировать и визуализировать безопасность их VMware виртуализованных и физических инфраструктур с единой консоли. RSA CSC дает возможность эволюционного перехода к удовлетворению требований регуляторов и безопасности при переходе на облачные ИТ-сервисы, не создавая полностью новые схемы управления и не ломая полностью старые.

Необходимо отметить, что решение RSA CSC дает возможность только управлять и контролировать политики безопасности на уровне бизнес-процессов/приложений/процедур администрирования. Для непосредственного обеспечения безопасности на более низком технологическом уровне используются другие решения (например, для шифрования/дешифрования, авторизации и др.). При этом востребованность решений подобных RSA CSC возрастает с повышением уровня масштабируемости виртуальной ИТ-инфраструктуры, когда управление/контроль за сотнями и тысячами ВМ (и десятками, и сотнями физических серверов) "вручную" становится невозможным, и уже требуется автоматизация процессов поддержания безопасности.

Решение RSA Archer eGRC Suite с большим набором интегрированных политик, стандартов контроля/управления, процедур и метрик, разработанных с учетом последних отраслевых и законодательных требований, позволяет в большей степени минимизировать все негативные факторы при переходе на виртуальную ИТ-инфраструктуру. Более чем 130 процедур контроля/управления в библиотеке Archer написаны специально для VMware vSphere 4.0 Security Hardening Guide и соотнесены с требованиями по безопасности таких стандартов как PCI, COBIT, NIST, HIPAA и NERC. Кроме того, библиотека включает тысячи других процедур контроля/управления для операционных систем,

баз данных, сетевых устройств и других активов инфраструктуры.

Процедуры контроля/управления VMware обеспечивают определенные инструкции для конфигурирования и управления инфраструктурой VMware в следующих областях:

- контроль доступа;
- безопасность платформы;
- информационная безопасность;
- операционная безопасность.

Используя автоматизированные процедуры в составе RSA Archer eGRC Platform, менеджер проекта может распределять политики безопасности и управлять соответствующими процедурами для каждого из администраторов, как физических, так и виртуальных ИТ-инфраструктур. В качестве администраторов может выступать администратор серверов/безопасности/сети/виртуальной инфраструктуры. Например, требования по конфигурированию VMware ESX-сервера посылаются VMware-администратору, требования по конфигурации хранения — администратору хранения, требования по конфигурации безопасности сети — администратору безопасности и т.д. В пределах RSA Archer eGRC Platform менеджер проекта может полностью отследить выполнение всех управляющих процедур с одной консоли.

RSA решение включает новое ПО, которое существенно автоматизирует оценку того, действительно ли VMware контроль безопасности был осуществлен правильно за счет развертывания автоматизированных агентов измерения (Automated Measurement Agent – AMA). Результаты этих автоматизированных проверок конфигурации передаются непосредственно в RSA Archer eGRC Platform, которая также получает результаты проверок конфигурации физических активов через интеграцию с коммерчески доступными технологиями просмотра. В результате RSA Archer eGRC Platform является точкой консолидации для непрерывного управления мониторингом как физической, так виртуальной инфраструктурой.

RSA enVision

RSA enVision — это платформа "3-в-1", позволяющая эффективно управлять логами и событиями безопасности — SIEM (security and information event management), а также собирать и анализировать большое число данных в реальном времени. RSA enVision легко масштабируется и снижает потребность в фильтрации и развертывании агентов.

RSA enVision обеспечивает:

- простоту контроля на соответствие регулирующим требованиям за счет законченного учета всей сетевой активности, всесторонней отчетности со встроенными и пользовательскими настройками, полной отчетности по логам, преконфигурированных отчетов для всех основных стандартов, включая PCI DSS, HIPAA, FISMA и ISO;
- расширенную безопасность за счет уведомлений в реальном масштабе времени о высоких событиях риска, упрощенном процессе обработки инцидента, а также отчетов/сообщений по наиболее уязвимым активам;

— оптимизацию сетевых и ИТ-операций за счет определения сетевой доступности и статуса, идентификации сетевых проблем и дефектного оборудования, визуализации специфических аспектов поведения пользователей с целью оптимизации производительности сети.

RSA enVision позволяет производить постоянный контроль как физической (сетевое оборудование, вычислительные фермы, поддерживающие работу виртуальной инфраструктуры), так и виртуальной инфраструктуры. Например, RSA enVision, используя VMWare VI API, может очень детально контролировать все манипуляции с виртуальными машинами и все действия привилегированных пользователей.

RSA enVision включает преконфигурированную интеграцию со всеми компонентами Vblock платформы, включая Cisco UCS и Nexus; EMC storage; VMware vSphere, vCenter, vShield и vCloud™ Director. В дополнение, RSA enVision имеет преконфигурированную интеграцию и поддержку с более чем 235 другими ИТ-компонентами, включая сети, системы безопасности, операционные системы, базы данных и приложения.

RSA SecurID/Authentication Manager

RSA SecurID — двухфакторная аутентификация/идентификация, основанная на пароле или PIN-коде и аутентификаторе/удостоверении для обеспечения более надежного уровня пользовательской идентификации, чем пароли многократного использования. RSA SecurID автоматически изменяет пользовательские пароли каждые 60 секунд.

RSA Authentication Manager — компонента управления RSA SecurID, которая используется для верификации аутентификационных запросов и централизованного управления политиками аутентификации в корпоративных сетях. RSA Authentication Manager является совместимым со многими сетями, удаленным и беспроводным доступом, VPN, Internet и приложениями.

RSA Authentication Manager поддерживает логические партиции, благодаря которым провайдер может определить и предписать отдельную опознавательную политику, назначая каждому арендатору/организации свой защищенный домен.

RSA Data Loss Prevention

RSA Data Loss Prevention (DLP) — это решение, основанное на политикоориентированном подходе для обеспечения безопасности данных в центрах данных, сетях и конечных точках. RSA DLP отслеживает действия пользователей с конфиденциальным (с точки зрения принятых в конкретной организации критериев) контентом и может сигнализировать о возникающих инцидентах, а также и самостоятельно предотвращать возможные потери критически важных данных. Основные особенности RSA DLP:

- обнаружение и классификация “чувствительных” данных;
- обучение конечных пользователей;
- обеспечение гарантий использования данных в соответствии с установленными в организации регламентами;

— предоставление отчетности о снижении/увеличении рисков и степени удовлетворения политикам при использовании данных.

RSA DLP снижает TCO, имеет высокий уровень масштабируемости и автоматизации сервисов защиты данных, а также одну из самых обширных библиотек в индустрии для классификации и политик чувствительных данных. RSA DLP улучшает защиту данных типа интеллектуальной собственности, стратегических программ развития, финансовой отчетности, а также отвечает требованиям комплайнс.

RSA Data Loss Prevention Network

RSA Data Loss Prevention (DLP) Network идентифицирует и назначает политики для “чувствительных” данных, передаваемых через: корпоративную электронную почту (SMTP-протокол), webmail, службу передачи мгновенных сообщений, FTP-протокол, web-инструменты на базе протоколов HTTP (или HTTPS) и универсальные TCP/IP-протоколы. Ключевые особенности RSA DLP Network:

- всесторонность политик и наличие библиотек с разными классами политик позволяет увеличить ROI, устранить потребность в тонкой настройке политик и быстро развернуть DLP;
- всесторонняя поддержка многочисленных протоколов значительно уменьшает возможность ошибок;
- фиксация логов действий конечного пользователя помогает администраторам упростить процесс комплайнса;
- многочисленные автоматические и ручные возможности по настройке политик позволяют их кастомизировать при изменении уровней риска;
- глубокая видимость нарушений сетевых политик отправителем, получателем, а также в содержании контента.

RSA DLP Network виртуальное устройство может быть развернуто для каждого клиента в рамках TMT-модели.

RSA Data Protection Manager

RSA Data Protection Manager — система управления ключами шифрования корпоративного уровня в приложениях, базах данных и системах хранения. RSA Data Protection Manager снижает TCO, связанную с шифрованием, давая воз-

можность их администрирования с единой консоли. RSA SafeProxy™ архитектура использует уникальную комбинацию токенизации, расширенного шифрования и открытых технологий для защиты “чувствительных данных” с многоуровневым подходом к их защите.

Cisco Virtual Security Gateway

Cisco Virtual Security Gateway (VSG) это ключевая компонента в защите вычислительного уровня и является виртуальным шлюзом безопасности, используемым совместно с программными коммутаторами серии Nexus 1000V. VSG позволяет в рамках TMT-модели различным клиентам с разными профилями безопасности использовать общую инфраструктуру.

VSG может быть развернут на нескольких уровнях в рамках виртуальной инфраструктуры (рис. 5):

- для защиты периметра инфраструктуры клиента;
- для защиты каждого виртуального дата-центра внутри инфраструктуры клиента;
- для защиты каждого виртуального приложения.

Cisco и VMware сотрудничают в области интеграции шлюза Cisco VSG для Nexus 1000V с решением VMware vCloud Director, чтобы воспользоваться интеграционными возможностями vShield Manager.

VSG позволяет: решать одну из ключевых проблем виртуальных инфраструктур — защита трафика виртуальных машин; применять настройки “на ходу”, динамически их менять и увязывать их с работой администратора по безопасности, а также при переходе с физических сред в виртуальные сохранять границы ответственности между администраторами, которые исторически сложились в не виртуализованных центрах данных. VSG состоит из двух блоков: 1) непосредственно из VSG, отвечающего за настройку и выполнение политик безопасности и 2) Virtual Network Management Center (VNMC), который служит станцией управления и позволяет выделять функции управления безопасностью в отдельный домен управления, обслуживать несколько VSG одновременно, предоставлять функции управления безопасностью клиентам за счет API.

Основные характеристики и преимущества VSG:

- широкие возможности зонирования на уровне виртуальных машин. Помимо поддержки политик информационной безопасности при выполнении виртуализированных заданий в сетях VLAN или на общей физической вычислительной инфраструктуре, виртуальный шлюз безопасности создает зоны повышенной защищенности для групп виртуальных машин на основе контекстуальной информации. Функция зонирования с учетом контекста виртуальных машин позволяет легко управлять политиками безопасности на уровне виртуальных машин в одной или нескольких виртуальных сетях VLAN и в разделяемой вычислительной инфраструктуре ЦОД. При этом выполнение административных задач ничуть не мешает функциям информационной безопасности, сетевым и серверным задачам;

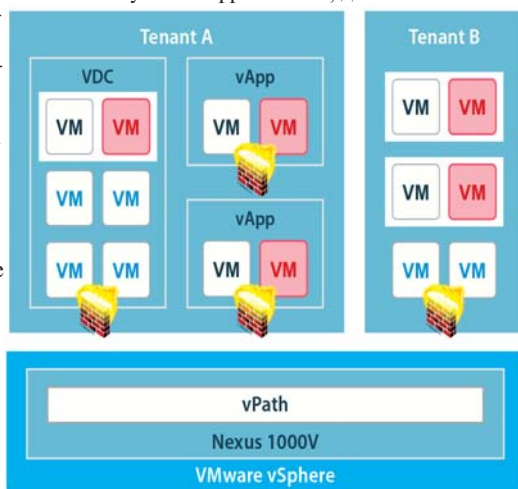


Рис. 5. Различные варианты использования Cisco Virtual Security Gateway.

- гибкость установки программного обеспечения. Виртуальный шлюз безопасности и менеджер виртуальных сетей (Virtual Network Manager) работают как виртуальные машины, которые используют все ресурсы управления и высокой доступности, имеющиеся в виртуальной инфраструктуре;
- простота развертывания и повышение производительности. Виртуальный шлюз безопасности хорошо интегрируется с технологией Cisco vPath, встроеной в коммутаторы Nexus 1000V, обеспечивая максимальную масштабируемость и производительность. Технология Cisco vPath использует функции динамического контроля доступа Nexus 1000V для "умного" управления сетевым трафиком и данными на уровне каждого индивидуального потока;
- централизованное управление. Шлюзы Cisco VSG интегрируются с центром управления виртуальными сетями Cisco Virtual Network Management Center для централизованного управления всеми политиками в пределах виртуализированного центра обработки данных. Центр управления виртуальными сетями позволяет администраторам создавать и контролировать многопользовательские профили безопасности и распределять масштабируемые ресурсы виртуальных шлюзов безопасности с помощью интерфейсов API в автоматическом режиме. Кроме того, он хорошо интегрируется с системой VMware vCenter и позволяет увязывать контекст виртуальных машин с политиками информационной безопасности.

VMware vShield

В условиях виртуальной среды применить стандартный подход, применяемый в традиционных средах к обеспечению безопасности, не представляется возможным. С одной стороны, среди причин, по которым традиционный подход не работает это появление новых сущностей инфраструктуры и высокая степень динамичности виртуальной инфраструктуры. С другой – это невосприимчивость виртуальной среды к определенным видам атак, которые характерны для традиционных сред, например таких, как "MAC spoofing" или "Random frame". Но для виртуальной среды есть свои особенности:

- отсутствие прозрачности взаимодействия виртуальных машин внутри одного хоста между собой;
- постоянная балансировка нагрузки виртуальных без выключения и разрыва сессий может быть нарушена статическими правилами традиционных решений, которые не готовы поддерживать такие варианты существования и работы инфраструктуры;
- возрастающая сложность в связи с распространением VLAN, которые чаще всего используют для изоляции трафика, в том числе и в виртуальных средах;
- новые сущности инфраструктуры, приостановленные виртуальные машины, спящие виртуальные машины, тестовые виртуальные машины и др.

Для построения безопасных сред, учитывающих динамичность виртуальной инфраструктуры, компания VMware представила семейство продуктов, объединенных единым названием vShield. В данное семейство вошли следующие продукты: vShield Edge, vShield App, vShield EndPoint, vShield Zones, vShield Manager.

vShield Edge

Продукт vShield Edge представляет собой форпост, призванный защищать границу между внешней инфраструктурой, например, глобальной сетью интернет и внутренней средой, например демилитаризованной зоной или внутренней сетевой инфраструктурой. Продукт предлагает комплексную защиту на основе нескольких компонентов. Ключевым компонентом является межсетевой экран, который позволяет анализировать и контролировать сетевой трафик, проходящий через форпост. При этом данный межсетевой экран полностью интегрирован с платформой виртуализации vSphere, как с точки зрения управления, что позволяет привязать фильтрацию трафика именно к объектам виртуальной среды, так и с точки зрения понимания и интеграции с функционалом. Так, например, vShield Edge полностью понимает технологию vMotion и не разрывает сессии, контролируя трафик при балансировке виртуальных машин в рамках виртуальной инфраструктуры. Кроме межсетевого экрана, в vShield Edge включены: компонент, который позволяет построить и обслуживать VPN туннель между площадками; сервис автоматического

назначения сетевых настроек для внутренней среды, что позволяет упростить настройки и автоматизировать их, а также сервисы балансировки нагрузки трафика для веб-сервисов. При этом все компоненты полностью интегрированы с виртуальной инфраструктурой и не разрушают ее динамическую среду.

vShield App

Продукт vShield Edge представляет собой решение для зонирования виртуальной инфраструктуры на определенные зоны безопасности. При этом каждая из таких зон может быть распределена между многими серверами, одновременно сосуществовать в рамках одного аппаратного сервера и не останавливать контроль при изменении месторасположения виртуальных машин. Это позволяет построить виртуальные барьеры для контроля взаимодействия виртуальных машин из различных зон, а также контролировать взаимоотношения между виртуальными машинами, даже в том случае, если они обмениваются данными в рамках одного аппаратного сервера и трафик не покидает его пределов.

vShield EndPoint

Данный компонент, в отличие от предыдущих, не является именно продуктом, а представляет собой набор API-интерфей-

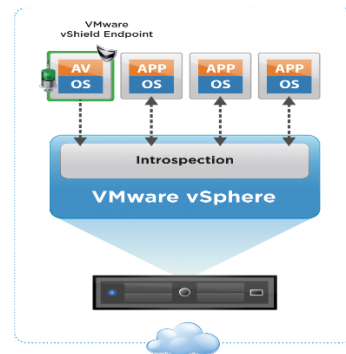


Рис. 7. vShield EndPoint за счет установки в отдельной VM антивирусного решения обеспечивает защиту сразу всех VM на ESX-сервере, снижая сложность и накладные затраты.

сов для организации продвинутой антивирусной защиты, ориентированной именно на виртуальные среды. Особенность заключается в том, что использование данных API-интерфейсов предполагает использование внешнего антивирусного решения и отменяет требование по установке антивируса в среду операционной системы каждой виртуальной машины. Каждый раз, когда приложения или операционная система будут обращаться к аппаратным компонентам для выполнения определенной операции, например, для чтения или записи, этот запрос из виртуальной машины будет направляться к компонентам гипервизора, где и будет перехватываться средствами vShield EndPoint, перенаправляться во внешний антивирус, который и будет принимать решение о правомочности операции, а также выявлять вирусную активность (рис. 7). Внешний антивирус – это решения от партнеров VMware, которым были отданы компоненты vShield EndPoint, для того, чтобы они смогли разработать свое собственное решение, использующее новый функционал. Среди таких партнеров присутствуют гранды

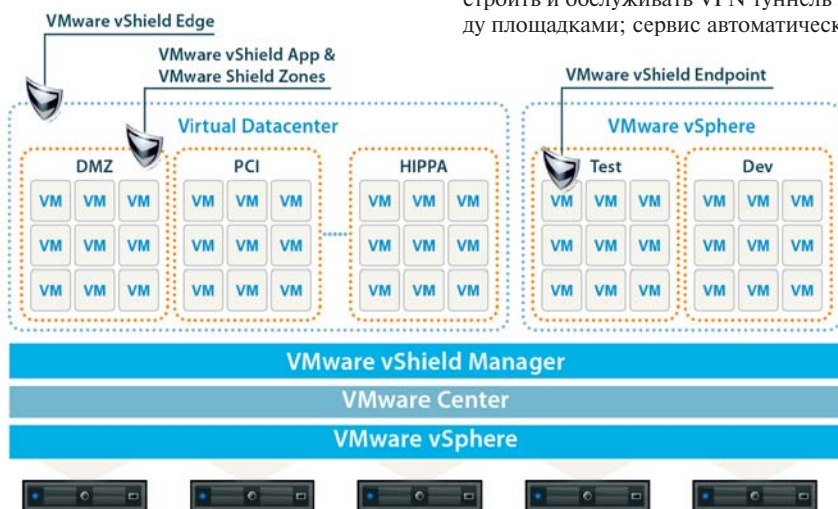


Рис. 6. Семейство решений VMware vShield.

в области разработок решений безопасности: TrendMicro, MacAfee, Symantec, RSA.

Такой подход не только упрощает управление антивирусным решением, минимизируя количество антивирусов, за которыми постоянно необходимо наблюдать и обслуживать, но и предлагает ряд других преимуществ. Именно такой подход позволяет минимизировать риски для спящих, тестовых, новых и старых виртуальных машин. Виртуальная машина может быть запущена после того, как она находилась в приостановленном состоянии, на любом сервере, при этом не надо беспокоиться о том, был ли установлен в ней антивирус на момент ее предшествующей работы, был ли он обновлен, актуальны ли его базы. При отсутствии антивируса внутри виртуальная машина всегда остается защищенной внешним антивирусом, работающим на основе API-интерфейсов vShield EndPoint. Еще одним преимуществом такого подхода является вопрос обслуживания, ведь количество обслуживаемых компонентов, антивирусных систем, сокращается во много раз, что напрямую влияет на доступность системы, снижая ее сложность.

Для развертывания средств ИБ на базе платформы VMware в ее составе предлагается специальный интерфейс – VMware VMsafe API к ядру гипервизора, позволяющий "видеть" весь трафик, идущий через него. На базе этого интерфейса и должны в данном случае строиться все решения ИБ для обеспечения межсетевое экранирования, предотвращения вторжений (IDS/IPS) и др. (рис. 8). При этом специальная VM защищает все гостевые VM "снаружи" и без каких-либо изменений самой VM.

Для разделения ролей в среде VMware можно использовать возможности решения vSphere, позволяющие ввести разграничения для 110 полномочий, собираемые в роли. При помощи этих полномочий можно регулировать и доступ к данным на хранилищах. Для более детального контроля можно использовать решение vGate от компании "Код безопасности".

VMware vShield Manager

VMware vShield Manager – это интерфейс управления для всех vShield-решений. Интегрированный с VMware vCenter и разворачиваемый в собственной виртуальной машине, vShield Менеджер усиливает возможности vSphere. С его помощью обеспечивается возможность настройки всех опций vShield-продуктов. Тесная интеграция с vCenter позволяет визуализировать все основные ресурсы пулов vSphere в пределах vShield Manager. Сервис-провайдер может использовать консоль VMware vShield Manager для управления и развертывания политик для всей среды vCenter.

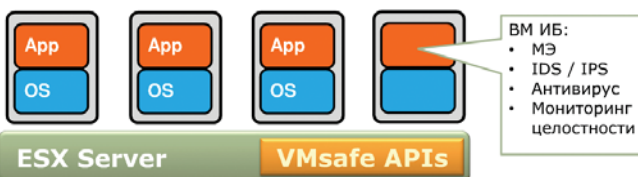


Рис. 8. VMware VMsafe API к ядру гипервизора, позволяющий "видеть" весь трафик, идущий через него.

Cisco Adaptive Security Appliance

Cisco Adaptive Security Appliance (ASA) является специализированным устройством безопасности, которое объединяет систему сетевой защиты Virtual Private Network (VPN) и опционные средства защиты контента, а также предотвращение вторжений в рамках всего центра данных. Один Cisco ASA может разделяться многими виртуальными файрволами (контексты безопасности – security contexts, SC). Каждый SC действует как отдельная система сетевой защиты с собственной политикой безопасности, интерфейсами и конфигурацией, хотя некоторые особенности недоступны для виртуальных файрволов типа IPSEC, SSL VPN, динамических протоколов маршрутизации (Dynamic Routing Protocols), Multicast and Threat Detection.

Cisco Intrusion Prevention System

Устройства Cisco Intrusion Prevention System (IPS) обеспечивают защиту от известных и появляющихся угроз, точно идентифицируя, классифицируя и останавливая злонамеренный трафик, включая черви, spyware, adware, сетевые вирусы и неправильное использование приложений.

Cisco Secure Access Control Server

Cisco Secure Access Control Server (ACS) – это высокомасштабируемая и высокопроизводительная система доступа на основе политик, которая централизует аутентификацию, доступ пользователей и политики доступа администратора, снижая административные и управленческие издержки. Cisco ACS поддерживает протоколы аутентификации, авторизации и управления доступом – AAA (authentication, authorization, accounting) – в таких системах/сетях управления, как: TACACS+, RADIUS, LDAP, Active Directory и др.

Технологии ИБ, используемые при хранении

При переходе с традиционных инфраструктур на полностью виртуализированные, например, на базе Vblock-платформ, основные методы управления ИБ и политиками безопасности существенно не меняются. Отличительной особенностью Vblock-платформ является использование конвергентных сетей на базе FCoE и, отчасти, более широкие возможности по шифрованию на уровне СХД.

Для виртуализированных окружений особую актуальность приобретает вопрос разграничения прав доступа. Если нет доверия к команде администраторов, то даже RDM-доступ не дает уверенности, и, скорее, для его решения необходимо прибегать к использованию технологий шифрования.

В присутствии виртуализации вычислений все или почти все ранее используемые технологии ИБ сохраняют актуальность. В частности, механизмы безопасности, опирающиеся на WWN для управления доступом к данным, могут быть использованы с использованием NPIV-функциональности, когда виртуальная машина выполняет независимый FLOGI в SAN со своим WWN, получает доступ

к своим LUN и т.д. В известном смысле, можно сказать, что средства сетевой поддержки виртуализации в сетях передачи данных (Nexus 1000V, VM-FEX) реализуют ту форму VM-awareness сети передачи, которая уже существует в SAN с использованием NPIV. Управление SAN вообще и функциями безопасности в частности, осуществляется единым образом через систему управления Fabric Manager.

В целом, тему безопасности сетей хранения данных можно разделить на несколько частей:

- управление – используются стандартные методы контроля доступа на уровне устройств SSH, RBAC, VSAN-based RBAC и традиционные методы фильтрации трафика средствами firewall;
- безопасность самой сети хранения от подключения нелегальных устройств: FC-SP, fabric binding, port security;
- безопасность данных in fly (например, между ЦОД): TrustSec;
- безопасность данных at rest: SME (сервис Storage Media Encryption в коммутаторах Cisco MDS), шифрование средствами хранилищ;
- разграничение доступа внутри СХД: VSAN, zoning, LUN masking;
- изоляция окружений для улучшения защиты от сбоя: VSAN, zoning, port monitoring;
- сохранение безопасности в DR-окружениях: расширение VSAN на все сайты (с применением IVR), репликация ключей шифрования носителей, шифрование передаваемых данных с помощью TrustSec или IPsec;
- аудит системы безопасности: syslog, call home.

В составе EMC СХД могут использоваться следующие методы разделения данных клиентов: VSAN, VDM, пулы, маскирование и маппирование, SymACL, User Authorization Enhancements for VMware и др.

VSAN – это коллекция портов хостов, коммутаторов и СХД, объединяемых в виртуальную фабрику. VSANs создают отдельные фабрики, использующие свои политики безопасности, зонирование и название сервисов.

Virtual Data Mover (VDM) – это программная опция EMC Celerra X-Blade, которая допускает группирование файловых систем и CIFS-серверов в виртуальные контейнеры. Каждый VDM содержит все данные, необходимые для поддержки одного или более CIFS-серверов и их файловых систем. VDM может быть загружен и разгружен, перемещен от Data Mover к Data Mover или реплицирован в удаленный Data Mover как автономный модуль.

Пулы – это логические контейнеры, содержащие от двух до максимально большого числа HDD (в составе СХД), организованные в одну RAID-группу, для которых могут применяться технологии "тонкого выделения ресурсов", компрессия и Fully Automated Storage Tiering (FAST). Пулы могут иметь смесь различных типов дисков: SSD, FC, SAS, SATA.

Маппирование и маскирование дают администратору хранения возможность формировать логические хост-группы, ка-

ждая из которых имеет доступ только к данным томов, назначенных этой хост-группе. В этом случае два клиента/арендатора могут иметь доступ к одному и тому же массиву, но их взгляд на активы хранения будет полностью независим.

Symmetrix Access Control (SymACL) дает возможность использовать хост-авторизацию. Каждый хост имеет уникальный WWID, который используется для назначения прав управления. Благодаря этому, два хоста будут "видеть" и управлять полностью различными ресурсами.

User Authorization Enhancements for VMware позволяют администраторам vCenter, основываясь на пользовательском ID клиента, назначать подсистему ресурсов хранения, к которым другие администраторы клиентов не могут обратиться. User Authorization Enhancements поддерживается EMC Symmetrix VSI plugin for vCenter.

Сервис WAN-оптимизации с поддержкой мультиаренды

По мере миграции ИТ-услуг в сторону распределенных ИТ-сервисов роль WAN-оптимизаторов возрастает. В составе Vblock-платформ предлагается решение Cisco Virtual WAAS — полностью готовое решение для работы в облачных средах.

Cisco Virtual WAAS — это виртуальное устройство, работающее на VMware ESXi гипервизоре и Cisco Nexus 1000V в составе Cisco Unified Computing System™ (UCS) x86 серверов. Cisco Virtual WAAS полностью совместимо с существующими Cisco WAAS устройствами и интегрированными в маршрутизатор модулями, которые все могут управляться Cisco vWAAS Central Manager (vCM). Cisco vWAAS поддерживает такие расширенные функции, как SAN-хранение для DRE-кэша (Data Redundancy Elimination), обеспечивая быстрое восстановление после отказов/сбоев за счет разделения вычислительных и ресурсов хранения. Cisco

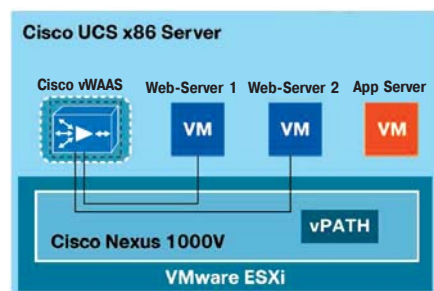


Рис. 9. Cisco vWAAS может развертываться по запросу с минимальным сетевым конфигурированием, используя интеграцию с Cisco Nexus 1000V.

vWAAS дает возможность развертывать WAN-оптимизацию как сервис для виртуальных машин (рис. 9) в условиях мультиаренды.

Предотвращение утечек из-за инсайдеров в виртуализированных датацентрах

Это одна из самых болезненных тем в распределенных виртуальных средах, особенно, если речь идет об ИТ-услугах на базе публичных облаков, поэтому на ней следует остановиться отдельно. Утеч-

ки "чувствительных" (и не только) данных могут быть связаны с тремя обстоятельствами: 1) отсутствием контроля за действиями персонала сервис-провайдера со стороны клиента; 2) отсутствием в составе платформ виртуализации функционала, позволяющего в полной мере разделить функции управления виртуальной инфраструктурой и доступа к данным клиентов; 3) неразвитостью и ресурсоемкостью средств онлайн-офлайн криптографии при обработке данных клиентов на стороне сервис-провайдеров.

В связи с этим, многие западные сервис-провайдеры подписывают отдельное соглашение с клиентами о том, что защита данных находится в сфере ответственности клиента. Так, пример пункта такого соглашения с Amazon гласит (<http://aws.amazon.com/agreement/>, 9 марта 2011 г.): 4.2 Other Security and Backup. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content.

Альянс по координации усилий в области разработки стандартов для облачных сред — CSA (Cloud Security Alliance) рекомендовал шифрование данных в облаке в качестве одного из основных механизмов защиты данных клиентов. Но при этом сразу встают вопросы: "Что именно шифровать?", "Какими технологиями шифровать и на уровне каких компонент ИТ-инфраструктуры?", "Кто будет шифровать?", "Как управлять ключами шифрования?", "Сколько это будет стоить?" Для России это усложняется еще и скудостью возможных для использования сертифицированных решений (конкурентоспособность гостовских решений в этой связи сдерживается не только отсутствием собственных чипов, но и невозможностью распараллеливания процессов криптографии из-за ограничений, накладываемых ГОСТ'ом). Проще говоря, в России это можно получить только в качестве сервиса, предоставляемого западным сервис-провайдером.

Возможности управления политиками безопасности и ключами доступа с клиентской стороны, например, в составе Vblock'ов, как было описано в предыдущем разделе, имеются. Однако полное использование всех средств защиты данных, включая криптографию при обработке ("in fly") и хранении данных ("at rest") в России сдерживаются, прежде всего, легитимностью этих решений, хотя поставщики оборудования (программные средства трудно применимы из-за ресурсоемкости онлайн-офлайн криптографии) уже поставляют их для всех уровней инфраструктуры.

Заключение

Современный уровень развития ИТ позволяет не только пользоваться всеми достижениями типа облачных сервисов, но и самостоятельно разворачивать их в рамках компании (с возможностью предоставления облачных сервисов на базе своего дата-центра подрядчикам и дочерним компаниям), например, на базе Vblock-платформ, при этом полностью решая все задачи, свя-

занные с процедурами комплайенса международных стандартов.

Однозначно можно сказать одно: "Если не забывать об ИБ с самого начала, и переходить к использованию облаков (как частных, так и публичных) совместно с внедрением как технических решений, так и новых административных политик, то уровень информационной безопасности не будет существенно снижен. Напротив, в большинстве ситуаций он может быть даже существенно повышен благодаря новым возможностям, появившимся именно в облачных средах и платформах виртуализации. Важно использовать проверенные промышленные решения и не пытаться "экономить на спичках", когда потери могут исчисляться миллионами".

Cisco: новые решения для унифицированных ЦОД

Март 2011 г. — Компания Cisco анонсировала технологические инновации для всего семейства продуктов Data Center Business Advantage. Объявления сделаны в рамках развития стратегии "унифицированная матрица коммутации" (основана на технологии Ethernet и анонсирована 3 года назад). Данная стратегия объединяет и взаимно дополняет решения для унифицированных вычислений и унифицированных сетевых услуг, создавая интегрированную матрицу коммутации для ЦОД. Она также решает следующие задачи: предоставлять (в рамках ЦОД или сетевого облаке) глобальную доступность вычислительных ресурсов в ситуации непрерывно меняющихся требований бизнеса и законодательства при неограниченной масштабируемости ИТ-ресурсов и высоком уровне безопасности.

Среди объявлений следующие:

- технология Multi-hop FCoE для устройств MDS 9500 и Nexus 7000;
- новые платформы Nexus 5548-UP, 5596-UP и Nexus 3000 со сверхнизкой задержкой;
- решения Adapter-FEX (имеют функцию "умной" сегментации полосы пропускания для существующих сетевых карт) и VM-FEX — расширение матрицы коммутации на серверный гипервизор;
- технология DCNM для управления конвергентными сетями LAN/SAN;
- новая платформа UCS B260-M2;
- протокол Location ID/Separation для глобальной мобильности рабочих заданий;
- поддержка виртуальных частных сетей MPLS VPN на сетевом уровне L3 (это позволяет строить хорошо защищенную сетевую инфраструктуру в облачных средах), а также протокола LISP (Location/ID Separation Protocol — протокол определения местоположения и разделения идентификации) для коммутаторов Nexus 7000;
- модули ACE-30, ES-40 и ASA для коммутаторов Catalyst 6500;
- расширенная поддержка FEX на коммутаторах Nexus 7000.