http://www.lanmag.ru МАЙ 2017

ЖУРНАЛ СЕТЕВЫХ РЕШЕНИЙ LAN

Мониторинг ИТ-инфраструктуры

Проблемы мониторинга ИТ-инфраструктуры
Новинки ИБП и тенденции рынка
Как правильно организовать видеонаблюдение

ISSN 1027086-8
17005
771027086001

http://www.lanmag.ru
ЖУРНАЛ СЕТЕВЫХ РЕШЕНИЙ LAN

МАЙ 2017
ТОМ 23
НОМЕР 5 (239)

Читайте нас на Facebook

Читайте нас в Twitter

3data строит моновендорный ЦОД на основе оборудования Legrand

Уже в сентябре новый ЦОД будет готов принять первых клиентов.


Фото: Александр Барсков

Илья Хала: «Мы понимаем все минусы моновендорного подхода, но в данном случае плюсы перевешивают»

Алексис Конан: «Стратегия Группы Legrand — предлагать законченные решения для ЦОДов»


Фото: Александр Барсков

В середине апреля компания 3data и Группа Legrand объявили о строительстве в Москве первого в России ЦОДа, который будет полностью базироваться на технических решениях Legrand. Согласно объявленным планам, ЦОД примет первых клиентов уже 1 сентября текущего года. За обеспечение телеком-решений отвечает оператор связи «Мастертел».

Компания 3data уже построила в Москве сеть из 10 небольших коммерческих ЦОДов (до 100 стоек) недалеко от мест концентрации бизнес-центров. В течение ближайших 10 лет их число планируется увеличить до 50. Вместо организации крупных (мега-) ЦОДов в промышленных зонах компания делает ставку на реализацию принципа «шаговой доступности» и предоставление сервиса с «премиальным качеством».

По словам генерального директора 3data Ильи Халы, в своих ЦОДах компания эксплуатирует оборудование практически всех основных производителей. В какой-то момент появилась идея реализовать ЦОД полностью на базе оборудования одного поставщика. В 3data хорошо понимают потенциальные минусы такого варианта (зависимость от поставщика, ограниченный выбор продуктов), но все же плюсов, по мнению Ильи Халы, значительно больше. В первую очередь это экономия средств, сокращение сроков поставки и реализации, а также высокая степень интеграции. Сегодня, уверен Илья Хала, только три компании способны предложить полное решение. Хотя он и не назвал их, помимо Legrand, видимо, имелись в виду Schneider Electric и Huawei. При реализации обсуждаемого проекта выбор был сделан в пользу Legrand, чему в немалой степени способствовали серьезные инвестиции со стороны этого производителя.

Новый центр обработки данных сооружается на первом этаже технологического центра Legrand на Садовом кольце. На втором этаже будут находиться офисные помещения для обслуживания заказчиков, на третьем — учебный комплекс. Уникальность создаваемого учебного центра заключается в том, что его посетителям можно будет продемонстрировать решения компании непосредственно на примере действующего ЦОДа — естественно, с соблюдением строгого регламента доступа.

Как отметил Алексис Конан, генеральный директор представительства Группы Legrand в России и СНГ, компания уже более 20 лет работает в России и ее продукция пользуется устойчивым спросом во многих отраслях экономики. Однако решение об активизации деятельности на рынке решений для ЦОДов было принято относительно недавно. С этой целью компания пополнила свой портфель новыми предложениями, в том числе путем покупки таких производителей, как Minkels и Raritan. Первая известна прежде всего своими системами изоляции коридоров и оптимизации воздушных потоков, что позволяет существенно повысить эффективность охлаждения ЦОДов. Вторая — один из ведущих разработчиков переключателей KVM и блоков распределения электропитания.

Помимо названных продуктов, Legrand предлагает источники бесперебойного питания, трансформаторы, структурированные кабельные системы, кабелеенесущие системы для оптических трасс и т. д. Одна из немногих позиций, представленная пока продуктами сторонних производителей, — кондиционеры. В своих комплексных решениях Legrand применяет хорошо известные на рынке блоки охлаждения Stulz. Примечательно, что в других ЦОДах 3data использует оборудование Stulz, которое эксперты компании считают лучшим в своем классе.

Одним из важных положений деятельности Группы Legrand является локализация производства в России. В Ульяновской области уже работают два предприятия, где осуществляется сборка ИБП и конденсаторных установок, изготавливается защитно-коммутационное оборудование, кабелеенесущие системы и прочее электрооборудование. В планах компании — открытие еще одной производственной площадки в Ульяновской области в 2018 году.

Александр Барсков

Imperva открыла в России центр очистки трафика от DDoS-атак

Установленная в России система производительностью 100 Гбит/с стала частью распределенной сети узлов очистки с суммарной пропускной способностью более 3,5 Тбит/с.

Компания Imperva, один из ведущих мировых разработчиков продуктов для защиты Web-приложений и СУБД, сообщила об открытии первого в России центра очистки трафика от DDoS-атак — Incapsula. Соответствующий облачный сервис компания приобрела в 2014 году вместе с одноименным разработчиком (компания Incapsula). В России точка присутствия (PoP) Incapsula размещена в Москве на площадке коммерческого ЦОДа IXcellerate. Производительность этой точки PoP составляет 100 Гбит/с, при этом представители Imperva отмечают, что она может быть легко увеличена по мере необходимости.

Как поясняет Давид Шульман, руководитель направления Imperva Incapsula, ранее трафик российских клиентов приходилось направлять для очистки через Варшаву и Стокгольм, что негативно сказывалось на производительности и вело к задержке получения уже очищенного трафика. Кроме того, для многих крупных отечественных компаний критически важно, чтобы обрабатываемый трафик не выходил за пределы территории РФ.

До открытия PoP в России сервисом Incapsula пользовались около двух десятков частных компаний, для которых выход трафика за границы страны особого значения не имел. За первые три месяца после открытия узла к числу пользователей сервиса добавилось пять крупных заказчиков, среди которых — общенациональный платежный сервис и телеканал.

«Мы являемся единственным западным производителем (систем защиты от DDoS), который инвестировал средства в организацию собственного центра очистки в России, — подчеркивает Давид Шульман. — Это открывает нам двери к новым категориям заказчиков, включая государственный сектор, крупные банки, ведущие торговые сети и т. д.».

Помимо защиты от DDoS-атак, московский узел Incapsula поддерживает ряд других функций. Это интеллектуальное кеширование и оптимизация контента на основе технологий CDN, межсетевое экранирование Web-приложений (WAF), а также балансировка нагрузки для обеспечения высокого уровня доступности приложений.

По словам Александра Шахлевича, директора по продажам Imperva в России и СНГ, чтобы сегодня эффективно бороться с масштабными DDoS-атаками, нужна разветвленная сеть высокопроизводительных центров очистки. У Imperva таких центров уже 33, и число их будет постоянно увеличиваться. Суммарная производительность сети центров очистки Incapsula составляет более 3,5 Тбит/с. Как рассказал представитель Imperva, буквально в декабре 2016 года система Incapsula заблокировала атаку общей мощностью 650 Гбит/с. Если бы эту атаку отразить не удалось, она могла бы «положить» сеть национального оператора связи крупной страны.

Защита от DDoS-атак крайне необходима организациям из различных отраслей экономики. Острота проблемы возрастает с развитием Интернета вещей (IoT). Подключаемые к Сети «вещи», как правило, не оснащаются средствами информационной защиты, при этом они постоянно находятся в режиме онлайн, чем активно пользуются злоумышленники. Как рассказал Александр Шахлевич, недавно в массированной атаке были задействованы около 100 тыс. подключенных устройств IoT.

Инвестиции в московский узел очистки трафика — лишь часть стратегического плана экспансии Imperva на российский рынок, в котором производитель видит огромный потенциал. Одна из важнейших задач компании — развитие канала продаж и дальнейшее увеличение числа пользователей продуктов и сервисов Imperva. Немаловажная роль в ее решении отводится взаимодействию Imperva с дистрибьютором — компанией RRC. По словам Юлии Грековой, менеджера по развитию бизнеса RRC Security, с открытием московского узла Incapsula существенно расширяется поле деятельности для партнеров, продающих решения SaaS. «Теперь в портфеле RRC Security есть полноценный пакет SaaS-продуктов: защита от DDoS-атак, балансировка нагрузки, WAF и прочее», — отметила Юлия Грекова.

Александр Барсков


Фото: Александр Барсков

Давид Шульман: «Мы являемся единственным западным производителем систем защиты от DDoS, который инвестировал средства в организацию собственного центра очистки в России»

Злоумышленники копят силы

Согласно отчету «Лаборатории Касперского», в I квартале зафиксировано уменьшение числа DDoS-атак и снижение их продолжительности. Подобное начало года является достаточно традиционным — такая ситуация наблюдается на протяжении последних пяти лет. Как заметил Алексей Киселев, менеджер Kaspersky DDoS Prevention в России, злоумышленники тоже не прочь устроить себе отпуск. Однако, если сравнивать с аналогичным периодом предыдущего года, сложность атак продолжает расти: в «Лаборатории Касперского» отмечают рост числа атак с использованием шифрования, что соответствует тенденции усложнения DDoS-атак, которые становится нелегко обнаружить стандартными защитными инструментами.

ЦОД с акцентом на безопасности

В Москве введен в эксплуатацию ЦОД SafeDC, который ориентирован на предоставление облачных сервисов безопасности.

Игорь Калайда: «Примерно два года назад компания приняла решение предоставлять услуги на базе своих продуктов, для чего и было начато строительство ЦОДа»

В середине мая компания «НИИ СОКБ» объявила о запуске коммерческого ЦОДа SafeDC, который будет специализироваться на предоставлении услуг Security as a Service (SecaaS), реализованных на базе собственных решений компании и на платформах ее партнеров. По сути, это первый профильный ЦОД в России, ориентированный на сервисы защиты данных и информационной безопасности.

Как рассказывает Игорь Калайда, генеральный директор НИИ СОКБ, будучи одним из лидеров российского рынка информационной безопасности, примерно два года назад компания приняла решение о предоставлении услуг на базе своих разработок, для чего и было начато строительство ЦОДа. Он называет две основные причины для принятия такого решения. Во-первых, это стремление многих российских заказчиков переложить свои расходы с капитальных затрат (CAPEX) на текущие (OPEX). Во-вторых — тенденция к импортозамещению, которая дает новые возможности российским разработчикам.

ЦОД SafeDC расположен в Москве, в районе метро «Калужская», на подземных этажах бизнес-центра. Помещения ЦОДа находятся в собственности НИИ СОКБ. Общая площадь ЦОДа —240 м^2, подведенная электрическая мощность — 1 МВт, ЦОД способен вместить до 120 стоек с ИТ-оборудованием. Объект спроектирован с учетом требований, предъявляемых к ЦОДам уровня Tier III, однако в получении соответствующего сертификата (от Uptime Institute) представители НИИ СОКБ необходимости пока не видят. Вместе с тем SafeDC аттестован на соответствие первому классу и первому уровню защищенности ИС для работы с государственными информационными ресурсами и персональными данными граждан.

SafeDC имеет собственный оптический канал до M9. Прямая оптическая связь реализована и с резервной площадкой, которая также располагается в Москве. Серверная инфраструктура ЦОДа основана на решениях Flex System компании Lenovo, а сетевая инфраструктура — на оборудовании Juniper Networks.

Одним из первых сервисов безопасности, доступных на базе SafeDC, стал сервис защищенной мобильной связи, построенный на базе MDM-системы SafePhone, разработанной НИИ СОКБ. Это решение обеспечивает управление корпоративными мобильными устройствами и приложениями, а также оперативное реагирование на различные связанные с ними инциденты (утеря, кража и пр.). Защищенная связь для этого сервиса предоставляется на базе решений «ИнфоТеКС».

Кроме того, на базе SafeDC уже доступны или будут доступны в самое ближайшее время целый ряд других сервисов SecaaS. В частности, сервис PayControl на базе решений компании SafeTech для безопасной аутентификации на порталах и в системах, а также для подписи документов с использованием мобильных устройств. На платформе Skybox будет развернута система постоянного контроля сетевой безопасности клиентов ЦОДа — с информированием о наличии уязвимостей и выработкой рекомендаций по их устранению.

Решение еще одного партнера НИИ СОКБ — компании Group-IB — стало основой для предоставления услуг по предупреждению киберпреступлений. А компания Qualys планирует развернуть на базе SafeDC облачный сервис по управлению уязвимостями и контролю соответствия отраслевым стандартам, требованиям регуляторов и корпоративным политикам безопасности.

Важным преимуществом проекта SafeDC является то, что сервисы безопасности могут применяться в связке, что позволит комплексно решать задачи по защите ИТ-ресурсов заказчика. Одним из примеров применения сразу нескольких решений является защита сервиса «Медкарта 24» — облачной платформы для врачей и пациентов, которая также будет развернута в SafeDC.

НИИ СОКБ планирует расширять набор предоставляемых на базе ЦОДа сервисов. Владимир Бычек, директор по развитию НИИ СОКБ, заявил о том, что компания намерена превратить SafeDC в «конвейер услуг информационной безопасности». Кроме того, в планах НИИ СОКБ — формирование «коробочных решений», чтобы облачные сервисы безопасности могли предоставлять и другие коммерческие ЦОДы. Таким образом, в других ЦОДах руководители НИИ СОКБ видят не конкурентов, а скорее потенциальных партнеров.

Помимо сервисов безопасности, на базе SafeDC предоставляются и классические услуги коммерческого ЦОДа, включая размещение оборудования, аренду стоек, предоставление виртуальных серверов и т. д. Для дополнительной защиты устанавливаемого в ЦОДе оборудования НИИ СОКБ предлагает вариант «ЦОД в ЦОДе» на базе сейфовых шкафов Lampertz. Однако, учитывая небольшие размеры SafeDC, предоставлять облачные сервисы выгоднее, так как они дают гораздо больший доход с единицы площади.

Руководители НИИ СОКБ не раскрывают объема инвестиций в новый ЦОД, но надеются, что они окупятся в течение 4–5 лет.

Александр Барсков