

ИНТЕЛЛЕКТУАЛЬНАЯ ОБЛАЧНАЯ СЕТЬ решения компании Cisco

К. Григорьев, компания Cisco

В последнее время многие предприятия и организации стали рассматривать облачную модель как одну из возможностей снижения своих расходов, повышения эффективности и развития новой инновационной бизнес-модели. По мнению 1300 ответственных ИТ-руководителей, опрошенных аналитической компанией Insight Express в 13 странах, включая Россию, к 2014 году более 50% трафика будет составлять трафик облачных сервисов и 60% предприятий к 2015 году осуществят миграцию и консолидацию своих сервисов и приложений в облачных средах.

Какие бывают облачные сервисы и для чего они нужны? Наиболее известный облачный сервис – это ваша электронная почта на публичном сервере (yandex.ru, mail.ru, gmail.ru и т.п.). Используя любой подключенный к Интернету компьютер, мобильный телефон, планшет, вы, находясь в любой точке мира, можете войти в свою почту и подключиться к данным своей учетной записи, хранящимся на удаленном сервере. Другой пример востребованных облачных сервисов – публичные ресурсы для резервного копирования и хранения данных (iCloud, Dropbox, Windows SkyDrive, Amazon Cloud Drive и др.). Среди публичных сервисов наибольшей популярностью у организаций и предприятий пользуются хостинг инфраструктуры, веб-присутствие, облачные решения для коммуникаций и совместной работы, а также бизнес-приложения. При этом многие компании, беспокоясь за сохранность своих данных, не готовы доверять обработку и хранение информации третьей стороне. Еще одна проблема – конфиденциальность. Потенциально к облачным сервисам компании можно подключиться с любого компьютера, имеющего доступ в Интернет.

Многие крупные организации начинают строить и использовать собственные частные облачные инфраструктуры, что позволяет им более гибко предоставлять услуги и ресурсы собственным

сотрудникам, а также снижать свои расходы на ИТ-поддержку и сопровождение.

Частное облако может находиться в собственности, управлении и обслуживании у самой организации или у третьей стороны, а располагаться как на территории предприятия, так и за его пределами. Многие облачные провайдеры предлагают виртуальные частные облака, выделяя ресурсы единственному заказчику и исключая при этом совместное использование этой виртуальной инфраструктуры несколькими клиентами.

Можно выделить два основных компонента облачной инфраструктуры: пользовательскую и облачную инфраструктуру. В первом случае имеется в виду традиционная сеть организации с подключенными к ней пользовательскими конечными устройствами. Для подключения к облаку пользователи могут применять любое устройство, подключенное к корпоративной сети или Интернету. Помимо маршрутизаторов и других сетевых устройств, в корпоративной сети могут использоваться средства мониторинга, контроля и оптимизации работы приложений.

Облачная же инфраструктура представляет собой центр обработки данных с собственной сетью, объединяющей системы хранения и серверы с поддержкой виртуализации, которые обеспечивают работу приложений и сервисов. Облачная

инфраструктура подключается к внешним сетям (Интернет или корпоративная сеть предприятия) при помощи маршрутизаторов.

Многие существующие распределенные WAN-сети построены на устаревшем оборудовании, которое не в состоянии обеспечить эффективное взаимодействие пользовательской и облачной инфраструктур и внедрение облачных сервисов по причинам своей невысокой производительности, отсутствия возможностей для безопасной и надежной передачи облачных приложений, а также из-за недостатка средств для мониторинга и управления облачным трафиком.

Концепция Cloud Intelligent Network ("Интеллектуальная облачная сеть") компании Cisco дает возможность решить большинство этих сетевых проблем, позволяя организациям эффективно и прозрачно подключать своих пользователей ко всем типам облачных сред (публичным, частным, гибридным) и обеспечивая высокий уровень производительности сервисов и безопасности частных сетей. При этом, как и в традиционных сетях, обеспечиваются богатые возможности по идентификации и мониторингу приложений в облачной среде, а также по управлению всей инфраструктурой облачной сети.

Маршрутизирующие платформы Cisco ASR 1000 и ISR G2 предоставляют широкий выбор интерфейсов (медный и оптический Ethernet, Serial, E1, DSL и т.д.) и возможность подключать к облачной среде центральные офисы и филиалы организаций, а также конечных пользователей.

Маршрутизаторы ISR G2 (Integrated Services Router Generation 2) серий Cisco 800, 1900, 2900 и 3900 обеспечивают гибкость за счет интеллектуальной интеграции сервисов безопасности, коммутации, унифицированных коммуникаций, видео, беспроводной связи, оптимизации работы приложений в глобальных сетях и прикладных сервисов.

Анонсированная в 2012 году новая платформа Cisco ASR 1002-х с операционной системой IOS XE позволяет по мере необходимости наращивать производительность платформы (с 5 до 36 Гбит/с) с использованием лицензий и модели сервисов по требованию, что позволяет значительно снизить операционные расходы и обеспечить защиту капиталовложений.

Новый виртуальный маршрутизатор Cisco Cloud Services Router (CSR 1000v), с помощью которого организации могут обеспечить подключение к частным виртуальным сетям (VPN) в облаках, позволяет использовать широкий спектр сервисов Cisco, предназначенных для работы в сети и обеспечения

безопасности, в форм-факторе виртуального устройства для развертывания в облачных средах. CSR 1000v анонсирован в 2012 году и представляет собой операционную систему IOS XE, работающую на базе виртуальной машины гипервизоров (VMware ESXi 5.0, Citrix XenServer 6.0 и др.) для серверных платформ Cisco UCS (Unified Computing System). Операционная система IOS XE для CSR 1000v поддерживает технологии FlexVPN, протоколы маршрутизации OSPF/EIGRP/BGP, функциональность MPLS/VRF, механизмы NAT/HSRP/DHCP и многое другое. Возможности маршрутизатора CSR 1000v позволяют организациям осуществлять управление сетевыми ресурсами корпоративной сети при миграции в облачные среды, а провайдерам облачных услуг обеспечивают возможность получать дополнительную прибыль путем применения гибкой модели по запросу "сеть как услуга". Предприятия и организации получают возможность расширить свои WAN-сети до уровня виртуальных частных облаков (virtual Private Cloud, vPC) внутри публичной мультиарендной среды облачного провайдера.

Маршрутизатор CSR 1000v является дополнением к богатому портфелю решений компании Cisco для облачных сред, включающему виртуальный коммутатор Nexus 1000v, межсетевой экран ASA 1000v для защиты периметра частной облачной среды, виртуальный шлюз безопасности VSG для реализации политик безопасности на уровне виртуальных машин, а также vWAAS для WAN-оптимизации трафика в облачной среде.

Помимо необходимости обеспечения безопасного подключения пользователей к облачной сети нужно также обеспечить эффективную доставку приложений. При миграции к облачной модели возникает зависимость от качества и пропускной способности канала связи. Появляется необходимость оптимизировать передачу трафика, исключив передачу трафика нежелательных приложений, сильно загружающих полосу пропускания и влияющих на производительность канала связи.

Набор интегрированных средств AVC (Application Visibility and Control) для маршрутизаторов Cisco ASR 1000/ISR G2/CSR 1000v позволяет понять, какие приложения работают в облачной среде, обеспечить их мониторинг и контроль передачи по каналам связи. Используя протокол NBAR2 и механизмы глубокой инспекции пакетов (Deep Packet Inspection, DPI), можно идентифицировать около 1500 различных приложений, в том числе работающих через web-приложения с использованием протоколов HTTP/HTTPS. Интеграция технологий NBAR2 и Flexible Netflow дает возможность

для реализации мониторинга и анализа трафика от 2 до 7 уровней модели OSI. В отличие от традиционного Netflow, технология Flexible Netflow позволяет четко обозначить необходимые для мониторинга ключевые поля кэша потока данных (Netflow-записи) и передавать кэш на несколько различных коллекторов Netflow посредством экспорта Netflow version 9 (RFC 3954) или IPFIX (RFC 5101). Возможность использовать тип приложения, идентифицированного при помощи NBAR2, в качестве поля Netflow-записи позволяет получить детальную статистику использования приложений в облачной среде.

При доставке облачных приложений и сервисов необходимо понимать, насколько эффективно используется полоса пропускания, трафик каких приложений передается через каналы связи, кто является основным потребителем этого трафика. NBAR2 и Flexible Netflow позволяют получить ответы на эти вопросы и обеспечить гибкий мониторинг IPv4- и IPv6-трафика. В качестве коллекторов Netflow для экспортируемых данных могут быть использованы решения для всестороннего мониторинга и управления сетью Cisco Prime Infrastructure с лицензией Assurance, аппаратные платформы Cisco для сетевого анализа NAM (Network Analysis Module) и системы некоторых сторонних производителей.

Определив нежелательные приложения (bit-torrent, youtube и т.д.), сильно загружающие каналы связи, организации могут блокировать их трафик с использованием традиционных механизмов QoS. Организации могут не только блокировать нежелательные приложения в облачной среде, но и оптимизировать трафик самих бизнес-критичных приложений (SAP, Oracle, виртуальные десктопы и т.д.), используя решение для оптимизации приложений Cisco Wide Area Application Services (WAAS). Cisco WAAS снижает количество передаваемого трафика по каналам связи, ускоряет работу приложений, оптимизирует пропускную способность и сокращает задержки, что, в свою очередь, повышает качество обслуживания конечных пользователей в глобальных сетях. В решении WAAS реализованы технологии оптимизации TCP-соединений, кэширования и сжатия данных, а также устранения избыточности при передаче трафика. Функции автоматического обнаружения устройств оптимизации существенно ускоряют процесс прозрачного внедрения этого решения в существующие сети. Решение Cisco WAAS доступно как в виде отдельных аппаратных устройств, так и в виртуальном

форм-факторе (virtual WAAS) для серверных платформ Cisco UCS (Unified Computing System).

Технология Cisco AppNav, анонсированная в 2012 году, обеспечивает гибкое управление оптимизацией глобальной сети по мере ее расширения, а также организацию работы и администрирование кластеров WAAS с балансировкой и распределением нагрузки. Для крупных центров обработки данных AppNav позволяет объединить несколько физических или виртуальных платформ WAAS в единый пул ресурсов Cisco WAAS, управляемый с помощью центрального контроллера.

Для более эффективного использования существующих каналов связи можно использовать технологию PfR (Performance Routing). Она позволяет расширить методы традиционной маршрутизации за счет учета информации о состоянии и метриках производительности каналов связи (потеря пакетов, загрузка канала, задержка и джиттер) в режиме реального времени. PfR дает также возможность обеспечить адаптивную динамическую маршрутизацию и балансировку нагрузки с распределением трафика через каналы связи с различной пропускной способностью. В результате предприятия могут обеспечить защиту трафика облачных бизнес-критичных приложений от потерь пакетов и повысить качество работы приложений для удаленных пользователей и подразделений.

Интегрированные решения для идентификации (NBAR2), мониторинга (Flexible Netflow) и контроля приложений (QoS, PfR) для маршрутизаторов Cisco ISR G2 и ASR 1000 позволяют обеспечить более эффективную доставку облачных сервисов через каналы связи с низкой производительностью. Плохое качество работы приложений, однако, может быть связано не только с сетевой частью облачной инфраструктуры. Проблема может заключаться в низком времени отклика самих серверов центров обработки данных. В таких случаях организациям трудно определить истинный источник проблем и узкое место при доставке облачных сервисов.

Маршрутизаторы Cisco ISR G2 с активированной функциональностью Performance Agent (IOS PA) могут обеспечить мониторинг времени отклика TCP-приложений для каждого сегмента (рис.1, 2) с использованием более 40 метрик, таких как время TCP-транзакции, время отклика сервера, сетевая задержка на стороне клиента, сетевая задержка на стороне сервера и т.д.

Агрегированные отчеты от одного или нескольких таких маршрутизаторов посредством Netflow-экспорта передаются системам

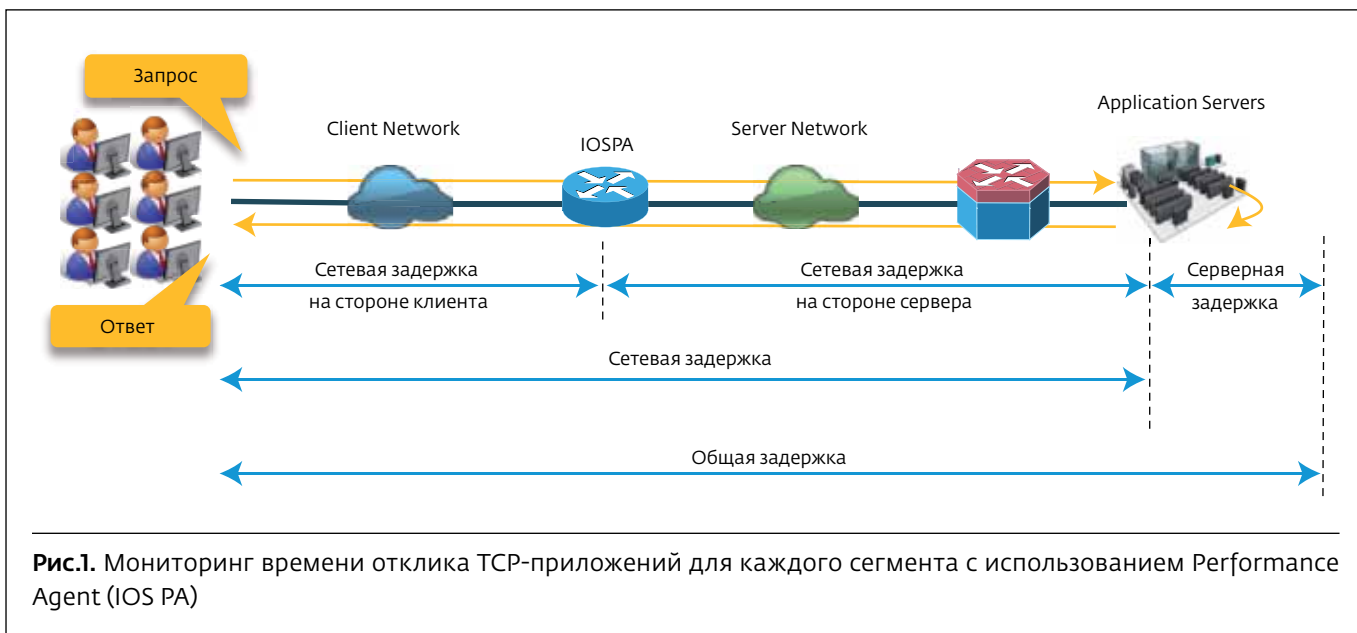


Рис.1. Мониторинг времени отклика TCP-приложений для каждого сегмента с использованием Performance Agent (IOS PA)

мониторинга Cisco Prime Infrastructure с лицензией Assurance или Cisco NAM, позволяющим получить общую информацию о временных метриках работы и доставке облачных приложений, классифицированных при помощи NBAR2.

Еще одна задача, с которой сталкиваются организации, внедряющие облачные технологии, – обеспечение локальной устойчивости облачного приложения для удаленного подразделения или филиала. Качественная работа облачных сервисов сильно зависит от качества, надежности

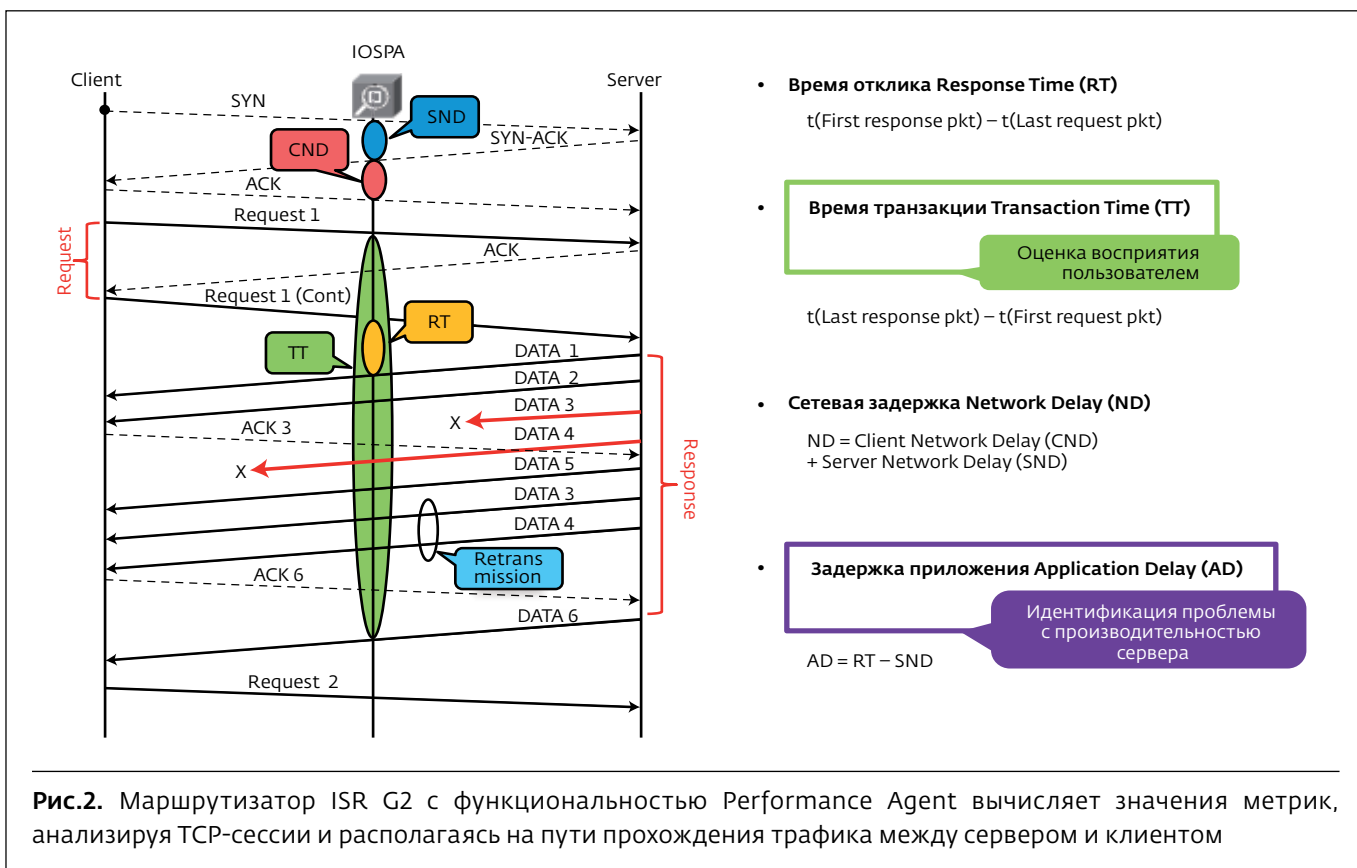


Рис.2. Маршрутизатор ISR G2 с функциональностью Performance Agent вычисляет значения метрик, анализируя TCP-сессии и располагаясь на пути прохождения трафика между сервером и клиентом



Рис.3. Серверные модули UCS E для маршрутизаторов ISR G2

и производительности канала связи. Как обеспечить работу облачных приложений в случае, если возникают те или иные проблемы с WAN-каналом и удаленные ресурсы и сервисы становятся недоступны? Новые серверные платформы Cisco UCS E для маршрутизаторов Cisco ISR G2 серий 2900 и 3900, анонсированные в 2012 году, позволяют обеспечить консолидацию сервисов и ресурсов и их резервирование на локальном уровне в случае их недоступности из облака. UCS E представляют собой модули одинарной или двойной ширины для маршрутизаторов Cisco ISR G2, обеспечивающие интегрированную вычислительную мощность с помощью собственных аппаратных ресурсов (рис.3).

В UCS E установлены современные 4- или 6-ядерные процессоры Intel Xeon серий E3/E5 Sandy Bridge, поддерживается оперативная память DRAM до 48 Гб и память для хранения до 3 Тб с поддержкой RAID0/RAID1/RAID5. Эти серверные блейды отличаются низким энергопотреблением (до 130 Вт) по сравнению с отдельно стоящими серверами и получают питание непосредственно от маршрутизатора. Все модули бесплатно комплектуются контроллером Cisco Integrated Management Controller (CIMC) для полноценного мониторинга состояния системы, удаленного управления электропитанием и аппаратными параметрами (в том числе BIOS), а также виртуальной KVM. Особенности UCS E позволяют решить еще одну непростую проблему: обеспечить раздельное и независимое управление между сетевыми и серверными IT-администраторами. Аппаратные платформы UCS E поддерживают установку различных операционных систем (Windows Server

2008, Red Hat Enterprise Linux, SUSE Linux, Oracle Linux) и гипервизоров (Microsoft Hyper-V, VMware vSphere 5.0, Citrix XenServer 6.0). Таким образом, на базе этих интегрированных в маршрутизаторы модулей можно обеспечить локальные архивы и сервисы облачных приложений в случае отказа WAN-канала связи и доступа к сервисам через облако. Интеграция UCS E в маршрутизаторы позволяет снизить совокупную стоимость владения благодаря уменьшению объема серверного оборудования и снижению операционных расходов на энергопотребление, охлаждение, пространство и место в стойке. К тому же очевидно, что проще управлять одним устройством, консолидирующим все сервисы для филиала в рамках одной платформы. Возможность управлять всеми сервисами удаленно из центрального офиса позволяет организациям решить вопрос нехватки квалифицированных специалистов в региональных подразделениях и филиалах и снизить затраты IT-специалистов на командировки.

В рамках своей концепции Cloud Intelligent Network компания Cisco представила так называемый Cloud Connector – программный компонент, улучшающий производительность, безопасность и доступность облачных приложений для филиалов и удаленных предприятий и организаций. Наиболее известным примером реализации Cloud Connector на сегодняшний день является решение ScanSafe для защиты от интернет-угроз и проникновения вредоносных программ в корпоративную сеть, обеспечивающее более эффективный контроль и безопасный доступ в Интернет. Это решение анализирует каждый запрос к интернет-ресурсам и допустимость этого запроса в соответствии с заданной политикой безопасности и обращается к облаку ScanSafe для проверки вредоносности. Тем самым обеспечивается защита прямого доступа из удаленных узлов в облако организации или в сеть Интернет. Преимущество этого решения состоит в том, что конечный пользователь избавляется от необходимости производить дополнительные настройки своей системы и web-браузера – функциональность ScanSafe интегрирована в программный код Cisco IOS для маршрутизаторов и активируется при помощи лицензии. Cloud Connector может быть как реализован в качестве функциональности, встроенной в операционную систему IOS маршрутизатора, так и работать на базе аппаратной платформы UCS E для маршрутизатора ISR G2. UCS E позволяет реализовать как хостинг сервисов Cisco, так и собственные приложения облачных провайдеров и организаций.



Рис.4. Сетевые решения Cisco для построения интеллектуальных облачных сетей

Управление всей инфраструктурой облачной сети Cisco реализовано на базе унифицированной системы управления Cisco Prime Infrastructure, содержащей решения для управления доступом, а также настройки конфигурации, мониторинга, поиска и устранения неполадок. С помощью дополнительной лицензии Assurance система Cisco Prime обеспечивает согласованный контроль и мониторинг производительности облачных приложений.

Компания Cisco продолжает наращивать богатый портфель решений для построения интеллектуальных облачных сетей. В дополнение к ранее выпущенным маршрутизаторам серии ASR 1000 и ISR G2, в 2012 году был анонсирован маршрутизатор ASR 1002-x, который может использоваться не только в центрах обработки данных и центральных офисах, но и в крупных филиалах компаний. Новый виртуальный облачный маршрутизатор CSR 1000v, с помощью которого организации могут обеспечить подключение к частным виртуальным сетям (VPN) в облаках, является дополнением к линейке маршрутизаторов ASR 1000 и может использоваться в облачных средах и центрах обработки данных. Новые серверные модули UCS E-серии для маршрутизаторов ISR G2 позволяют обеспечить локальное хранилище данных и сервисов для филиалов, а также работу специализированных программных компонент

(Cloud Connector) для взаимодействия с облачными сервисами на базе интегрированных аппаратных ресурсов. В дополнение к широкой линейке устройств оптимизации WAAS, как физических (WAVE 294, 594, 694, 7541, 7571, 8541), так и виртуальных (vWAAS), в 2012 г. было анонсировано новое решение AppNav для управления и распределения нагрузки в рамках кластеров WAAS для крупных центров обработки данных. Широкий портфель решений и платформ Cisco (рис.4) позволяет строить интеллектуальные облачные сети в соответствии с современными тенденциями.

ИСТОЧНИКИ

1. www.cisco.com/web/RU/solutions/trends/cloud/cloud_intelligent_network.html.
2. www.cisco.com/en/US/prod/collateral/routers/ps10537/zk_white_paper_cloudverse.pdf.
3. www.cisco.com/en/US/solutions/collateral/ns1015/white_paper_idc-architecting_the_network_for_the_cloud.pdf.
4. www.cisco.com/en/US/prod/collateral/ps10265/ps12629/cloud_connected_solution_aag.pdf.
5. www.cisco.com/en/US/prod/collateral/routers/ps10536/cisco_cloud_connect_v3.pdf.
6. www.cisco.com/en/US/solutions/collateral/ns1015/ns1184/whitepaper_c11-706172.html.
7. www.cisco.com/en/US/prod/collateral/routers/ps10536/white_paper_c11-706801.html.