Обеспечение безопасности для виртуальных серверов и приложений

Общие сведения

Вопросы безопасности чаще всего упоминаются в качестве препятствий для перехода на виртуализацию приложений и облачные вычисления. Простое дублирование политик безопасности для физической среды здесь не помогает - они могут ограничить эффект от виртуализации, не устранив новые проблемы с безопасностью, неизбежные при размещении приложений и данных на виртуальных серверах.

Виртуальные приложения (т.е. оптимизированные для виртуальной среды) - обычно это веб-приложения, к которым возможен доступ авторизованным пользователям для ввода, синхронизации и последующего считывания данных. Например, это могут быть серверы бизнес-приложений (Microsoft Exchange Server, SAP и Oracle E-Business Suite), а также приложения, разработанные на заказ, обычно состоящие из веб-сервера, сервера базы данных, инфраструктуры для разработки ПО и собственно приложения.

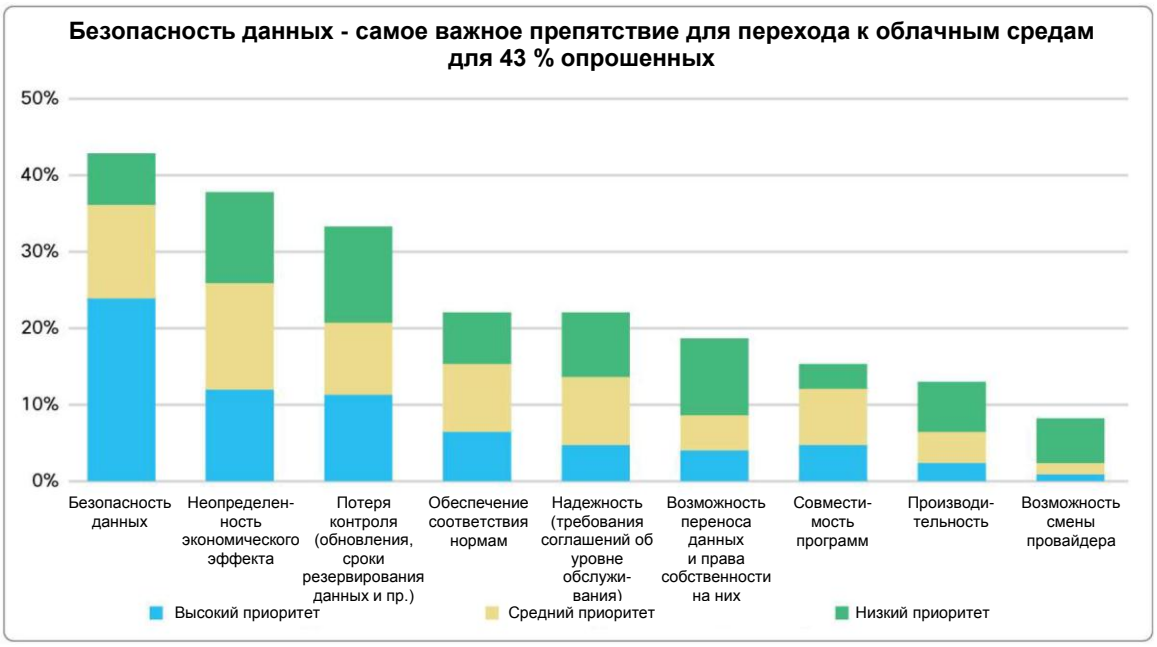
Для обеспечения безопасности таких виртуальных приложений необходима новая защитная инфраструктура, которая работает внутри уровня виртуализации ЦОД, обеспечивает безопасное соединение его с физическим ЦОД и решает дополнительные задачи, характерные для сред с большим числом пользователей и возможностью масштабирования.

Вопросы безопасности - основное препятствие на пути массовой виртуализации приложений

Для корпоративных приложений виртуализация серверов - это стратегический ход, способствующий консолидации и росту эффективности использования ресурсов при снижении затрат. Виртуализация обычно начинается с определенных приложений, размещенных в корпоративном ЦОД, но расширение этого процесса может подготовить предприятия к экономическому эффекту от облачных вычислений при работе как в частных облачных средах с внутренним управлением, так и в общедоступных средах с внешним управлением.

Хотя большинство крупных компаний уже получает эффект от виртуализации второстепенных приложений, многие хотят перейти к виртуализации основных рабочих приложений и облачным средам. Пока самым распространенным препятствием на пути к виртуализации является безопасность виртуальных приложений и сред (рис. 1). До сих пор организациям был доступен лишь тот уровень безопасности, который обеспечивают наилучшие технологии защиты для физической среды.

Рис. 1. Препятствия на пути виртуализации



Источник: AlphaWiseSM, Morgan Stanley, “**Cloud Computing Takes Off, Market Set to Boom as Migration Takes Off**”, 23 мая 2011 г.

Проблемы в области безопасности для виртуальных сред

Рассмотрим кратко возможные угрозы и сложности, возникающие при виртуализации приложений и переходе к облачным средам.

- **Цели высокой ценности.** ЦОД и важные приложения все чаще и чаще выбираются в качестве целей внешними хакерами и теми, кто действует внутри организаций. Исследования утечек данных, проведенные компанией Verizon в 2011 г., показали, что данные, украденные с серверов, составляют 94% от всех известных случаев кражи информации (рост на 18%), и 96 % пострадавших не обеспечили соблюдение требований отраслевого стандарта защиты данных платежных карт (PCI DSS). Эта тенденция сохранилась и в 2012 г., причем в каждом месяце этого года заметен рост относительно аналогичного месяца 2011 г.
- **Мобильность нагрузок.** Виртуализация серверов позволяет приложениям перемещаться между серверами и даже между удаленными ЦОД и облачными средами. Такая мобильность увеличивает сложность того уровня сети, который отвечает за безопасность. Обычно он работает с неподвижными ресурсами и статичными частными сетями при реализации политик безопасности. Гибкость перемещения политик безопасности в соответствии с изменением виртуальных рабочих нагрузок является сложной задачей.
- **Увеличение числа точек атак.** В результате виртуализации серверов возникают новые точки атаки, в частности, на уровне виртуализации, включая гипервизор, среду виртуальных машин и программные коммутаторы, заменяющие физические коммутаторы уровня контроля доступа в сети. Появление этих дополнительных слоев увеличило число уязвимых мест ЦОД. Действительно, по своей сути уровень виртуализации хуже защищен по сравнению с физическими устройствами из-за отсутствия физического разделения и особенностей, связанных с большим числом пользователей.

- **Большое число пользователей**. В то время как в небольших распределенных центрах обработки данных размещается малое число приложений или поддерживается одна организация, в современных консолидированных ЦОД и облачных средах часто работают разные группы пользователей, которым требуется полное разделение сетевого трафика и строгие политики контроля доступа, даже если их физические серверы и сетевая инфраструктура являются общими. Такие же требования относятся и к частным виртуальным центрам обработки данных и частным облачным средам, в которых внутренним пользователям необходимо разделение.
- **Ограничения виртуальных локальных сетей**. В физических локальных сетях для разделения групп пользователей и ресурсов в основном используются виртуальные сети. Такое решение непригодно для виртуальных ЦОД, поскольку, как правило, приложения не могут перемещаться между виртуальными сетями. В результате исчезает основное преимущество виртуализации - возможность использования любого доступного ресурса в центре. Поэтому возникает необходимость в новых средствах разделения сетей и обеспечения безопасности.
- **Разделение обязанностей при администрировании ЦОД**. В информационных технологиях принято строгое распределение ответственности между администраторами серверов, администраторами сетей и службой безопасности. Виртуализация серверов усложнила такое разделение труда, поскольку те, кто работает с серверами, как правило, взяли на себя вопросы обслуживания сетей и обеспечения безопасности уровня виртуализации, закрепленного за серверами и средой виртуальных машин. Необходимы средства, позволяющие использовать функции групп безопасности и единообразные политики безопасности на уровне виртуализации.
- **Размер и сложность консолидированных ЦОД**. Консолидация привела к возникновению проблем с масштабированием и сложностью, которые ограничивают ИТ-персонал при разработке и внедрении политик безопасности с соответствующими решениями, а также при организации работы с ними.

Требования к контекстно-зависимым политикам безопасности в ЦОД.

Обычно приложения ЦОД и клиенты настольных систем отвечали за большинство функций аутентификации пользователя и контроля доступа. При повышении уровня мобильности и появлении незащищенных устройств, а также более сложных угроз большая часть задач по реализации политики безопасности должна перейти от оконечных устройств к сетям по мере роста зависимости их работы от контекста и приложений.

Инфраструктура сетевой безопасности все в большей степени требуется для реализации политик идентификации и политик на основе ролей, а также для принятия других связанных с контекстом решений. Основой блокировки передачи трафика в приложения или на серверы в центре обработки данных или облаке больше не могут быть стандартные исходные или конечные адреса узлов. Теперь она должна выполняться с учетом идентификационных данных или роли пользователя, процесса или приложения в операции. Доступ также может зависеть от привязанных к контексту характеристик, отличных от идентификаторов, включая тип устройства, обращающегося к приложению, местонахождения пользователя, время запроса и пр. Реализацию этих контекстно-зависимых политик все чаще берут на себя межсетевой экран ЦОД и система предотвращения вторжений (IPS), которые должны расширить свои возможности для контроля сети и принятия решений на их основе, а также для контроля наличия вредоносных программ, попыток несанкционированного доступа и различных атак.

Разработка модели безопасности для консолидированного ЦОД с большим числом пользователей

Проблемы, возникающие с виртуализацией ЦОД, вынудили организации пересмотреть порядок внедрения решений для обеспечения сетевой безопасности. Для реализации эффективного подхода по обеспечению многоуровневой безопасности необходимо развернуть ряд дополняющих друг друга сервисов безопасности в соответствующих точках сети ЦОД. Ниже перечислены наилучшие общие подходы к проектированию сетей ЦОД, основные требования к решениям для обеспечения сетевой безопасности и роли каждого из сервисов безопасности.

Защита ЦОД от неавторизованных пользователей и внешних атак

Для обеспечения безопасности ЦОД сначала нужно отделить его от всего неавторизованного входящего и исходящего трафика, проходящего по локальной сети. Предусмотрите динамический межсетевой экран перед ЦОД или большую группу ресурсов серверов общего пользования (front-end), которые могут блокировать весь трафик, идущий из неавторизованных источников по неверным адресам в ЦОД. Для этого можно использовать устройство обеспечения сетевой безопасности высокой производительности, например, многофункциональное устройство Cisco® ASA 5585-X.

Предотвращение вторжений и сдерживание вредоносного ПО

Нормальный трафик, входящий в ЦОД, может содержать вредоносное ПО, в том числе троянские программы, вирусы и черви. Предусмотрите систему предотвращения вторжений с достаточной производительностью и возможностью масштабирования всего трафика на входе в ЦОД или в ряде точек внутри него. Это может обоснованно гарантировать отсутствие угроз во всем трафике ЦОД и виртуальных машинах. Есть небольшая вероятность того, что такое вредоносное ПО будет атаковать другие виртуальные машины, если они будут отделены от приложений в других надежных зонах виртуальным межсетевым экраном. Cisco ASA 5585-X - это многоцелевое защитное устройство с функциями предотвращения вторжений, которые дополняют возможности высокопроизводительного динамического МСЭ.

Защита границы сети пользователей проверенным межсетевым экраном

Используйте проверенные средства защиты для физической среды в виртуальных и облачных средах. Обеспечьте безопасность отдельных подразделений или зон пользователей мощными средствами защиты периметра - это повысит защищенность обмена данными между пользователями. Облачный межсетевой экран Cisco ASA 1000V вместе с виртуальным коммутатором Cisco Nexus® 1000V выполняет эти функции защиты, обеспечивая при этом функции основного шлюза и защиту от сетевых атак.

Закрепление виртуальных машин за разделенными надежными зонами и реализация политик контроля доступа

Внутри ЦОД следует использовать политики безопасности, изолирующие обмен данными между группами приложений. Это исключит доступ пользователей и сервисов одного приложения к приложениям в других надежных зонах при отсутствии разрешения. Такой уровень контроля доступа и логической изоляции обеспечивают межсетевые экраны. Но раньше эти функции нельзя было ввести на уровне виртуальных машин, в том числе для изоляции машин, работающих на одном сервере. Межсетевые экраны физических сетей не воспринимали виртуальные машины в качестве отдельных элементов сети. Теперь возможно применение средств детального контроля с использованием виртуального шлюза безопасности Cisco (VSG) для коммутатора Cisco Nexus 1000V.

Централизованное управление политиками

Формирование профилей безопасности на основе шаблонов может упростить разработку и внедрение политик безопасности, а также управление ими. Такая модель администрирования поддерживается центром управления виртуальными сетями Cisco (VNMC), который может управлять виртуальным шлюзом Cisco VSG внутри зоны и виртуальным межсетевым экраном Cisco ASA 1000V на ее границе.

Поддержка мобильности виртуальных машин

При закреплении политик безопасности за виртуальными машинами или виртуальных машин за надежными зонами такие политики должны перемещаться внутри ЦОД, отслеживая перемещение виртуальных машин между серверами. Поскольку межсетевой экран работает вне виртуальной машины, при реализации такой мобильности возникли серьезные сложности. Вместе с тем, такие функции являются стандартными для шлюза Cisco VSG, который рассчитан на определение атрибутов виртуальных машин.

Безопасный доступ к виртуализированным ЦОД и приложениям

Технлогии VPN являются надежным средством подключения внешних пользователей напрямую к основным сервисам, особенно в общедоступной облачной среде, использующей серверы веб-приложений. Обычно шлюз VPN считается надежным шлюзом для доступа пользователей к локальной сети, но он также может обеспечивать безопасный доступ к основным серверам и приложениям ЦОД. Решения VPN для ЦОД практически всегда используются совместно с межсетевыми экранами. Они должны обеспечить тот же уровень возможностей масштабирования, эффективности работы, возможностей подключения и надежности, что и остальные элементы инфраструктуры ЦОД. Кроме того, решения VPN обеспечивают детальный контроль доступа к приложениям, размещенным в частном облаке ЦОД.

Возможность масштабирования

Современные ЦОД и облачные сети сдерживают возможности масштабирования у организаций, которые увеличивают уровень консолидации и привлечения внешних исполнителей для резкого снижения затрат. Эта тенденция стала заметна недавно, поскольку крупные организации только начинают переходить к использованию частных облачных сред с размещением на собственных серверах и больших общедоступных облачных сред. Провайдеры, обеспечивающие работу больших коммерческих облачных сред, уже создали отдельные ЦОД, каждый из которых охватывает десятки тысяч серверов, и глобальные облака с удаленными объектами из сотен тысяч серверов.

- Полная реализация преимуществ, получаемых за счет наличия дешевых ресурсов в оптимальном месте, требует возможности масштабирования сети на уровне L2, поскольку недостаточная расширяемость ограничивает область передачи нагрузки к определенному приложению. Вопросы масштабирования имеют особую важность для определения точек реализации политик безопасности, поскольку на них не должно влиять перемещение виртуальных приложений между серверами, центрами обработки данных и элементами облачной инфраструктуры. Автоматизация внедрения сервисов и политик безопасности по мере развертывания приложений внутри ЦОД определяет успех и экономическую эффективность развертывания облачной среды.

Разделение обязанностей администраторов безопасности, сети и серверов

Виртуализация нагрузок приложений и, в частности, сервисов безопасности создает дополнительные проблемы для ИТ-служб. По мере перехода сервисов безопасности из сети на виртуальные машины, работающие на серверах, вопросы внедрения политик безопасности и управления инфраструктурой обеспечения безопасности передаются от администраторов сетей администраторам серверов. Даже при нормальной организации совместной работы корпоративные политики часто требуют строгого разделения обязанностей между этими группами специалистов. Это необходимо для сохранения полноты ответственности администраторов сетей за безопасность и управление работой виртуальных устройств. Управление развертыванием и внедрением виртуализированных средств обеспечения безопасности должно быть реализовано вне серверов. При этом они должны работать совместно с физическими устройствами обеспечения безопасности с жестким разделением обязанностей.

Интеграция облачного межсетевого экрана Cisco ASA 1000V Cloud Firewall и шлюза Cisco VSG с коммутаторами Cisco Nexus 1000V

Устройства Cisco ASA 1000V и Cisco VSG дополняют друг друга с точки зрения функциональности. Межсетевой экран Cisco ASA 1000V вместе с виртуальным коммутатором Cisco Nexus 1000V помогает защитить виртуальные и облачные многопользовательские среды на уровне границ между зонами подразделений.

Работая как основной шлюз системы, он обеспечивает защиту от сетевых атак. Организации может потребоваться разделить пользователей для соблюдения требований норм, например, для изоляции всех приложений, работающих с ценной технической или финансовой информацией, а также с данными платежных карт, от остальных приложений. ЦОД с большим числом пользователей или частная облачная среда, естественно, требуют изоляции трафика приложений для различных пользовательских зон, приложений и групп пользователей в зависимости от принятой политики.

Виртуальный шлюз безопасности Cisco VSG вместе с коммутатором Cisco Nexus® 1000V обеспечивает детальную безопасность при контакте между виртуальными машинами в пределах одной зоны. Он работает в качестве сетевого шлюза и обеспечивает безопасность на основе атрибутов зон и контекстно-зависимую защиту виртуальных машин.

Если организации необходимы разные политики внутри одной области, она может быть поделена дальше на надежные зоны, т.е. изолированные виртуальные машины с собственной операционной системой. Шлюз Cisco VSG обладает функциями виртуального межсетевого экрана, что обеспечивает возможность детальной реализации политик на уровне виртуальных машин. Поэтому он способен эффективно разделить нагрузки виртуальных машин, работающих в разных надежных зонах на одном физическом сервере.

Шлюз Cisco VSG обеспечивает логическое разделение виртуальных машин и трафика для разных надежных зон без использования виртуальных сетей, которые обычно изолируют разные области сети. Наличие виртуальных сетей в ЦОД может быстро ограничить возможность масштабирования, снизив эффект от консолидации и виртуализации этого центра. Только виртуализированные сервисы безопасности, встроенные в уровень виртуализации, могут выполнять те же функции, что и виртуальные сети в физических сетях, без ограничения возможности масштабирования.

Совместное использование устройств Cisco VSG и ASA 1000V обеспечивает надежную защиту границ областей для безопасного обмена данными между пользователями. Коммутатор Cisco Nexus 1000V также обеспечивает последовательное использование сервисов виртуальным шлюзом безопасности и межсетевым экраном ASA 1000V.

Например, в сфере здравоохранения, клиники, перешедшие к виртуализации, могут разделить функции выставления счетов, ведения медицинской документации, анализа бизнеса и научных исследований. Вместе с тем, иногда данные из медицинской документации требуются для клинических исследований. Совместное использование устройств Cisco ASA 1000V и VSG обеспечивает безопасный обмен данными между этими двумя группами пользователей с защитой личной информации и исключением неправомерного внесения изменений в медицинскую документацию.

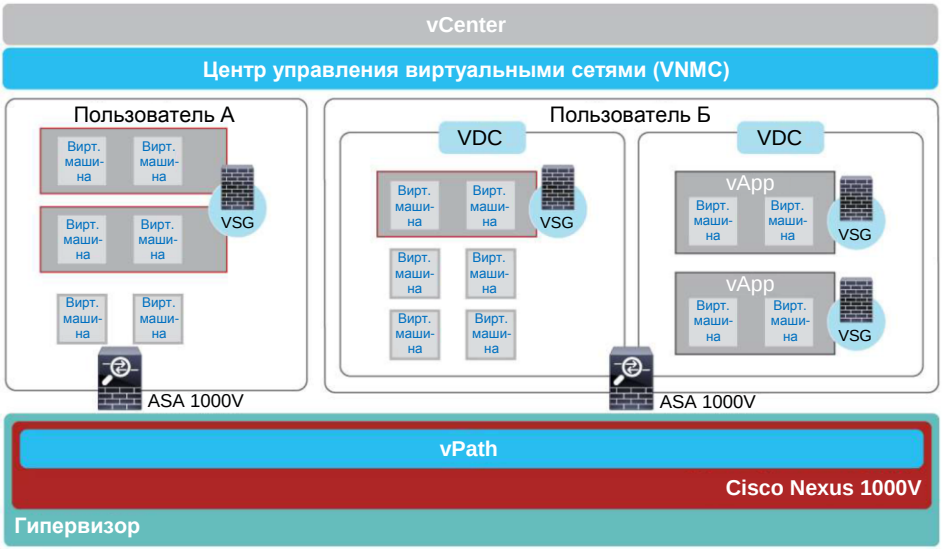
Виртуальный межсетевой экран, установленный между виртуальными машинами, также может предотвратить атаки на уровне виртуальных машин, гипервизора или основных операционных систем, а также сбор сетевых данных вредоносным приложением или сервером. Для использования политик детальной безопасности для отдельных виртуальных машин виртуальные МСЭ Cisco ASA 1000V и VSG рассчитаны на тесную интеграцию с виртуальным коммутатором Cisco Nexus 1000V и гипервизором на уровне виртуализации сервера. По мере создания виртуальных машин или их перемещения между серверами, политики безопасности для них перемещаются вместе с ними, предоставляя все сервисы безопасности автоматически.

Виртуальные межсетевые экраны можно создавать и использовать совместно в зависимости от потребностей для оптимизации использования ресурсов. И экран Cisco ASA 1000V, и шлюз Cisco VSG используют технологию управления трафиком vPath коммутатора Cisco Nexus 1000V для передачи трафика к нужным сетевым сервисам для реализации политик. Это позволяет таким устройствам за один шаг обеспечивать защиту виртуальных машин на различных серверах с возможностью масштабирования инфраструктуры безопасности ЦОД или облака и простого управления ей. Число шагов масштабирования этих устройств определяется по необходимости, позволяя реализовать большое число политик с учетом особенностей разных виртуальных приложений. Такая архитектура позволяет конечному пользователю оптимизировать использование ресурсов и снизить затраты.

Интегрированное решение также рассчитано на масштабирование в гетерогенных средах гипервизоров. По мере масштабирования коммутатора Cisco Nexus 1000V на разных типах гипервизоров его сервисы, включая виртуальный шлюз безопасности и межсетевой экран ASA 1000V, также масштабируются для защиты таких сред.

Администрирование политик безопасности для устройств ASA 1000V и Cisco VSG организовано на уровне центра управления виртуальными сетями Cisco (VNMC). Это прозрачное масштабируемое многопользовательское решение предназначено для управления объектами на основе политик с целью обеспечения комплексной безопасности виртуальных и облачных сред. Этот центр обеспечивает быстрое развертывание на основе динамического управления на базе политик с использованием шаблонов и профилей безопасности. Он обеспечивает повышение гибкости управления благодаря интерфейсу API XML, поддерживающему интеграцию со сторонними средствами управления и координации. Центр VNMC предоставляет администраторам средств обеспечения безопасности возможность раздельного управления приложениями, серверами и сетями в целях обеспечения соответствия нормам.

Рис. 2. Организация совместной работы устройства Cisco ASA 1000V с виртуальным коммутатором Nexus 1000V и шлюзом Cisco VSG.



Заключение

Защита виртуальных приложений и уровня виртуализации ЦОД является сложным препятствием на пути получения результатов от консолидации и виртуализации ЦОД с переходом к облачной модели формирования затрат. Необходимы новые виртуальные сервисы безопасности, обеспечивающие прозрачность виртуальных приложений, которые могут дополнить традиционные средства физической защиты ЦОД.

Межсетевой экран Cisco ASA 1000V блокирует внешние атаки на пользователей виртуальных и облачных сред в виртуальных ЦОД и отсекает неразрешенный трафик. Он обеспечивает реализацию существующих политик безопасности в среде виртуальных приложений, решая проблемы защиты при совместном использовании ресурсов в облачных средах с большим числом пользовательских зон.

Шлюз Cisco VSG обеспечивает реализацию подробных политик безопасности, способных различать виртуальные машины, и помогает изолировать трафик и приложения так, как это не способны делать традиционные средства обеспечения безопасности, без ущерба для возможностей масштабирования всего ЦОД или простоты доступа к виртуальным приложениям.

Устройства Cisco ASA 1000V и Cisco VSG работают совместно с виртуальным коммутатором Cisco Nexus 1000V. Централизованное управление устройствами Cisco ASA1000V и Cisco VSG посредством системы VNMC помогает разделить обязанности между администраторами сетей и серверов приложений в целях обеспечения соблюдения норм. При этом упрощается и общее администрирование для больших облачных сред.

Дополнительная информация

http://www.cisco.com/go/vsg

http://www.cisco.com/go/asa1000v

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465

Компания Cisco имеет более 200 офисов по всему миру. Адреса, номера телефонов и факсов приведены на web-сайте компании Cisco по адресу www.cisco.com/go/offices.

Отпечатано в США C11-652663-01 09/12