Требования к межсетевому экрану нового поколения

Обзор

Контрольный список, приведенный в данном документе, описывает шесть необходимых функций, на которые следует обращать первостепенное внимание в процессе оценки межсетевого экрана нового поколения (NGFW). Эти шесть характеристик помогут вам определить, способно ли рассматриваемое решение обеспечить необходимую информационную безопасность вашего предприятия.

Решение NGFW должно обладать следующими функциями:

- Надежная интеграция функций безопасности в целях обеспечения высокоэффективной защиты от угроз и атак новейшего вредоносного ПО.
- Предоставление практической информации о нарушениях работы системы, позволяющей выявить активность вредоносного ПО.
- Предоставление возможности проведения всестороннего мониторинга состояния сети.
- Обеспечение поддержки в сокращении затрат и упрощении системы.
- Максимально эффективная и прозрачная интеграция с решениями по обеспечению безопасности сторонних производителей.
- Обеспечение защиты инвестиций.

Общие сведения

Системы обеспечения кибербезопасности, в основе которых используются исключительно технологии и инструменты защиты, ориентированные на конкретный момент времени, не способны конкурировать с современными высокотехнологичными и непрерывно развивающимися методами проведения многовекторных атак. На самом деле, согласно ежегодному отчету Cisco по информационной безопасности за 2014 год, любая организация должна принять во внимание тот факт, что ее система безопасности, скорее всего, подвергалась атакам[1]. Специалисты Cisco по исследованию угроз обнаружили вредоносный трафик в 100 процентах корпоративных сетей, участвующих в проверке, что говорит о том, что злоумышленники проникли в сети и, возможно, оставались незамеченными на протяжении продолжительного периода времени[2].

Сегодняшние многовекторные и непрерывные атаки, подверженные быстрым изменениям ИТ-среды, а также растущие скорости работы сетей подталкивают организации к поиску решения NGFW, которое способно обеспечить многоуровневую и интегрированную защиту от угроз посредством наилучших технологий обеспечения безопасности, демонстрирующих эффективное и прозрачное взаимодействие в рамках системы. Несмотря на то что на рынке проявилось множество технологий, направленных на решений описанных выше задач, уникальность рассматриваемого NGFW нельзя оставить без должного внимания.

[1] Ежегодный отчет Cisco по вопросам информационной безопасности за 2014 год: http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html.
[2] Там же.

Приведенный контрольный список и прочие характеристики, описанные в данном документе, помогут вам убедиться в том, что вложение инвестиций в выбранное решение NGFW действительно является оправданным. Такой межсетевой экран должен отвечать за целостное представление сети, анализ угроз и сетевого трафика в режиме реального времени, а также обеспечение защиты от целенаправленных и непрекращающихся атак вредоносного ПО, включая новые угрозы.

Платформа

Оценивая то или иное решение, обратитесь к платформе решения NGFW — пусть это будет вашим первым шагом. Именно отсюда начинается процесс принятия решения о покупке. Для того чтобы решение NGFW могло обеспечивать интегрированную и многоуровневую защиту от угроз, оно должно быть построено на базе платформы межсетевого экрана с отслеживанием состояния соединений. Не менее важным фактором является «послужной список» технологии в отношении ее подтвержденной на практике производительности.

Платформа решения NGFW должна быть оснащена усовершенствованным механизмом проверки с отслеживанием состояния, обеспечивающим защиту критически важных ресурсов путем всестороннего мониторинга скрытых угроз. Выбранное решение NGFW должно отличаться надежностью, позволяющей обеспечивать защиту от угроз на должном уровне, — даже в случае работы нескольких серверов. Кроме того, с помощью выбранного решения вы должны определять не только угрозы, но также подключаемых к сети пользователей и устройства с последующим отслеживанием их деятельности с целью выявления аномального поведения.

Контрольный список характеристик NGFW

Сверьтесь с пунктами контрольного списка, чтобы убедиться в том, что выбранное решение NGFW позволяет обеспечить защиту, внедрить политику, достигнуть согласованности, а также получить доступ и обменяться контекстной информацией — все это в рамках одной платформы и с соответствующей скоростью.

- **Выбранное решение обеспечивает возможность надежной интеграции функций безопасности в целях обеспечения высокоэффективной защиты от угроз и атак новейшего вредоносного ПО.**

  Решение NGFW оснащено интегрированными уровнями обеспечения безопасности, которые взаимодействуют между собой. Новые способы работы, такие как облачные вычисления и мобильность, увеличивают площадь, подвергаемую воздействию кибератак; взаимодействие между интеллектуальными средствами мониторинга угроз на всех уровнях обеспечения безопасности позволяет выявить атаки, которым удается «проскочить» через слабые участки системы, оставаясь незамеченными. Для данного уровня защиты требуется непрерывное взаимодействие между инструментами защиты, конечными точками и центральной консолью управления, которое позволит специалистам по безопасности отследить угрозы и своевременно принять меры по восстановлению.

  При выборе решения NGFW следует отдавать предпочтение ориентированной на предотвращение угроз технологии, которая обеспечит комплексную защиту от атак и вредоносного ПО, выявляя угрозы на раннем этапе. Функции обнаружения угроз, которыми оснащено решение NGFW, направлены на оказание поддержки специалистам по информационной безопасности не только в контексте выявления и предотвращения атак вредоносного ПО, но также понимания их сути.

- **Решение NGFW предоставляет практическую информацию о нарушениях работы системы или показатели компрометации, позволяющие выявить активность вредоносного ПО.**

  Показатели компрометации (IoC) являются своего рода «тегами» на узле, указывающими на вероятность проникновения вредоносного ПО. Показатели компрометации используют взаимосвязь между безопасностью сети и безопасностью конечных точек. С их помощью определяется активность вредоносного ПО на узлах и конечных точках, вследствие чего обеспечивается возможность высокоточного мониторинга на предмет выявления подозрительного и вредоносного поведения.

  В сочетании с перечисленными выше функциями решение NGFW становится инструментом для быстрого выявления, предотвращения распространения и последующего восстановления.

- **Технология NGFW обеспечивает функцию комплексного мониторинга состояния сети.**

  Решение NGFW должно обеспечивать доступ к полной контекстуальной информации и четкому целостному представлению о том, что происходит в сети в каждый отдельно взятый момент времени. Это распространяется на пользователей и устройства, связь между виртуальными машинами, угрозами и уязвимостями, доступ к приложениям и веб-сайтам, передачу файлов и многое другое.

  В рамках комплексного контроля состояния сети должен осуществляться непрерывный и пассивный мониторинг всех ресурсов вашей сети. С помощью инструментов автоматизации данная информация может быть использована с целью оптимизации эффективности обеспечения безопасности посредством динамических элементов управления, реагирующих на изменения в среде ИТ или со стороны угроз в режиме реального времени. Решение должно обеспечивать реальное представление о текущей ситуации, которое станет отправной точкой в рамках выявления и реагирования на пробелы в системе обеспечения безопасности, оптимизации политики обеспечения безопасности и, наконец, сокращения числа событий, имеющих нежелательные и серьезные последствия.

  Решение NGFW также отвечает за автоматизацию ответных действий после возникновения атаки, включая локализацию и предотвращение распространения угрозы, что в конечном итоге значительно упрощает работу специалистов по информационной безопасности.

- **NGFW обеспечивает поддержку в рамках сокращения затрат и упрощения системы.**

  Демонстрирующее эффективность в борьбе с новейшими угрозами решение NGFW объединяет функции обеспечения безопасности на всех уровнях защиты. Интегрированный, многоуровневый подход к обеспечению безопасности позволяет осуществлять более углубленный мониторинг угроз и, как следствие, улучшать показатели функций защиты. Консолидация множества устройств в рамках одной платформы упрощает систему обеспечения безопасности в целом и сокращает затраты, устраняя необходимость в приобретении и управлении широким набором решений.

Дополнительные преимущества решения NGFW

- **Высокая масштабируемость.** NGFW с функцией многоуровневой защиты от угроз позволяет сетевым администраторам обеспечивать непрерывную и надежную защиту на уровне небольших филиалов, узлов интернет-периметра и крупных центров обработки данных в рамках физической и виртуальной сред.

- **Автоматизация повседневных задач, направленных на обеспечение безопасности.** Решение NGFW должно отвечать за автоматизацию следующих процедур.
  - **Оценка воздействия.** Автоматическое сопоставление угроз с интеллектуальными средствами выявления уязвимостей узла, топологией сети и контекстуальной информацией об атаке позволяет аналитикам по вопросам безопасности сфокусироваться только на тех событиях, которые гарантируют возможность мониторинга и реагирования в кратчайшие сроки.
  - **Оптимизация политик обеспечения безопасности.** Автоматизация процессов выделения ресурсов, корректировки и непрерывного внедрения политики обеспечения безопасности по всему предприятию позволяет специалистам по обеспечению безопасности оптимизировать эффективность системы и функции реагирования на изменения в среде и новые атаки в режиме реального времени. Автоматизация управления политиками безопасности является критически важным аспектом для отделов ИТ, ограниченных в ресурсах.
  - **Идентификация пользователей.** Решение NGFW должно быть оснащено функцией соотнесения идентификационной информации пользователей с событиями безопасности. Наличие данной функции экономит время аналитиков по вопросам безопасности, обеспечивая поддержку в предотвращении распространения угроз и восстановлении в более краткие сроки.
- **NGFW обеспечивает максимально эффективную и прозрачную интеграцию с решениями по обеспечению безопасности сторонних производителей.**

Решение NGFW позволяет оптимизировать совокупную стоимость владения (TCO) и минимизировать сложность управления эффективной системой безопасности для вашей среды путем простой интеграции и сопряжения с технологиями сторонних производителей. Сюда входят средства обнаружения уязвимостей, решения по управлению программным обеспечением, системы классификации проблем или полученных от абонентов жалоб, платформы для управления событиями и информацией по безопасности (SIEM), которые уже развернуты в рамках вашей сети или рассматриваются с целью внедрения.

Интеграция с решениями сторонних производителей углубляет многоуровневую защиту, обеспечиваемую решением NGFW путем комбинирования основных уровней защиты в рамках одной платформы. Данный подход упрощает развертывание средств обеспечения безопасности и текущие процессы посредством поддержки существующих технологий и обмена средствами мониторинга угроз в целях согласования и организации ответных действий.

Отдавайте предпочтение NGFW с поддержкой обширной «экосистемы» технологий, оснащенных открытыми API-интерфейсами для решений сторонних производителей, включая:

- системы управления уязвимостями;
- системы визуализации сети и платформы для управления событиями и информацией по безопасности (SIEM);
- средства управления доступом к сети (NAC);
- инструменты технической экспертизы сети;
- средства реагирования на события.

ДОПОЛНИТЕЛЬНЫЕ АРГУМЕНТЫ В ПОЛЬЗУ ПРИОБРЕТЕНИЯ: УСЛУГИ МИГРАЦИИ И ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Миграция на NGFW представляет собой мероприятие значительного масштаба. После принятия решения о переходе на NGFW и отказа от предложений сторонних производителей и традиционных межсетевых экранов вам предстоит найти поставщика, который оказывает услуги миграции. Профессиональные услуги миграции, предоставляемые как на объекте, так и на удаленной основе, позволяют упростить и ускорить процесс. Любой поставщик решений NGFW или его сертифицированные партнеры должны предоставлять широкие знания, практические рекомендации и необходимые инструменты, позволяющие максимально смягчить расхождения в графике выполняемых работ и поддержать непрерывность ведения бизнеса в ходе миграции — и сделать это без чрезмерных затрат.

При выборе технологии также необходимо уделить внимание уровню и качеству услуг технической поддержки, предоставляемых вашей организации поставщиком решений NGFW. К примеру, услуги удаленного управления позволяют сократить совокупную стоимость владения (TCO) путем непрерывного мониторинга и управления системой безопасности сети, тем самым освобождая вас от решения рутинных задач и предоставляя возможность фокусироваться на ключевых бизнес-приоритетах. Кроме того, услуги, обеспечивающие возможность выполнения анализа текущего состояния защищенности, проверки политик и эффективности вашей инфраструктуры безопасности, в конечном итоге оказывают поддержку в развитии и оптимизации вашей программы безопасности.

Предоставление услуг технической поддержки после развертывания решения NGFW в вашей среде является не менее важным критерием. Может ли поставщик предложить вашим ИТ-специалистам в любой момент времени (24 часа в сутки, 365 дней в году) услуги специализированных инженеров? Может ли он обеспечить универсальное обслуживание самого разного оборудования, а также проактивную диагностику устройств, ресурсы и инструменты для самообслуживания и возможности онлайн-обучения? Доступны ли оказываемые услуги и поддержка по всему миру? Качественная техническая поддержка позволяет сократить время простоя сети и гарантирует непрерывную работу вашего предприятия.

- Решение NGFW обеспечивает защиту инвестиций.

Возможно, перед тем как вы вложите инвестиции в решение обеспечения безопасности нового поколения, обеспечивающее комплексную защиту вашего предприятия, вам следует рассмотреть доступные альтернативные решения. Отдавайте предпочтение поставщику решений NGFW, который сможет предложить вам несколько решений, демонстрирующих очевидные преимущества для вашей компании, а именно:

- снижение затрат и повышение производительности путем сокращения жизненных циклов ИТ и проактивного управления;
- обновление технологических ресурсов, отталкиваясь от текущей бизнес-стратегии и вашего представления об ее изменениях в будущем;
- доступ к комплексным и недорогим решениям, включая аппаратное обеспечение, программное обеспечение и сопутствующее оборудование сторонних производителей.

Решение NGFW, отвечающее всем пунктам контрольного списка: Cisco ASA с сервисами FirePOWER

Cisco ASA с сервисами FirePOWER отвечает всем критериям, обозначенным в контрольном списке выше. Фактически, оно является единственным решением NGFW корпоративного класса, обеспечивающим интегрированную защиту от угроз на протяжении всего цикла атаки: до ее возникновения, в процессе ее проведения и по ее завершении (см. рисунок 1).

Рисунок 1. Интегрированная защита от угроз на протяжении всего процесса атаки

Cisco ASA с сервисами FirePOWER является первым адаптивным, ориентированным на угрозы решением NGFW, созданным с учетом современных требований к защите от угроз и вредоносного ПО. Его динамичные элементы управления обеспечивают возможность беспрецедентного мониторинга и защиты от угроз в режиме реального времени. Данное решение NGFW сочетает в себе следующие проверенные функции безопасности.

- **Многофункциональное устройство безопасности Cisco ASA**. Наиболее широко распространенный межсетевой экран корпоративного класса с контролем состояния, функциями удаленного доступа к сетям VPN и расширенной кластеризацией, обеспечивающей быстрый и безопасный доступ и высокую надежность систем для непрерывности ведения бизнеса.
- **Сервисы FirePOWER**. Лидирующая в отрасли система защиты от угроз и вредоносных программ Sourcefire®, обеспечивающая первоклассную и эффективную защиту от угроз, подтвержденную результатами независимых испытаний, проведенных NSS Labs[3].

Cisco ASA с сервисами FirePOWER: многоуровневая защита от угроз и встроенная защита от угроз в рамках одной платформы

Как показано на рисунке 2, решение Cisco ASA с сервисами FirePOWER предоставляет следующие функции в рамках одной платформы.

- **Непревзойденная система многоуровневой защиты от угроз** обеспечивает защиту от известных и неизвестных типов угроз, включая целенаправленные и непрекращающиеся атаки вредоносного ПО.
- **Усовершенствованная защита от вредоносного ПО** демонстрирует лидирующие в отрасли показатели эффективности выявления проникновений и оптимизации совокупной стоимости владения наряду с непревзойденным уровнем защиты. Для обнаружения, распознавания и блокировки проникновения новейшего вредоносного ПО в рамках данной технологии используются большие данные. AMP обеспечивает преимущества мониторинга и контроля, необходимые для предотвращения угроз, которым удалось обойти другие уровни системы безопасности.

[3] «Матрица значений безопасности NSS Labs для систем выявления проникновений: усовершенствованная защита от вредоносного ПО Sourcefire является лидирующим решением в вопросах эффективности и оптимизации совокупной стоимости владения», Sourcefire.com: https://info.sourcefire.com/NSSBreachDetectionReportSEM.html?gclid=Cj0KEQjw7b-gBRC45uLY_avSrdgBEiQAD3Olx8BtffrsQkNYs3AtCojRqyy42V1yLfGyh78OMov3iUAaAlNc8P8HAQ.

- **Показатели компрометации с высокой практической ценностью.** Cisco ASA с сервисами FirePOWER предоставляет целостные, дающие основания для действий показатели компрометации, которые сопоставляют детальные сведения о событиях в сети и на оконечных устройствах, предоставляя специалистам по безопасности преимущества еще более детального мониторинга проникновений вредоносного ПО в систему. Решение NGFW также способно сопоставлять события, связанные с проникновением, и выполнять автоматическую оценку воздействия атаки на целевой объект.
- **Комплексный мониторинг и контроль состояния сети.** Cisco ASA с сервисами FirePOWER управляется централизованно с помощью центра управления Cisco FireSIGHT™ Management Center. Он обеспечивает беспрецедентный уровень мониторинга состояния сети и автоматизации ответных действий, предпринимаемых в рамках реагирования на изменения условий среды или новые атаки. Благодаря центру управления FireSIGHT Management Center специалисты по безопасности получают полное представление о состоянии сети на любой момент времени, включая сведения о пользователях, устройствах, взаимодействии между виртуальными машинами, уязвимостях, угрозах, клиентских приложениях, файлах и веб-сайтах.

Ведущий в отрасли межсетевой экран Cisco ASA с системой предотвращения вторжений нового поколения FirePOWER (NGIPS) значительно повышает эффективность защиты от угроз и предоставляет полную контекстуальную информацию о пользователях, инфраструктуре, приложениях и содержимом, что позволяет вовремя обнаруживать многовекторные угрозы и автоматизировать процесс защиты. Благодаря определению траектории файла вредоносного ПО вы получаете сведения, позволяющие локализовать угрозу и выявить причину ее возникновения, таким образом ускоряя процесс восстановления.

Используя центр управления FireSIGHT Management Center, администраторы получают возможность централизованного управления сотнями устройств. В то же время, благодаря функции детального контроля и мониторинга приложений (AVC), которой оснащено устройство Cisco ASA с сервисами FirePOWER, они могут оптимизировать эффективность безопасности путем использования 3000 элементов управления уровня приложений, ориентированных на угрозы и задействующих политики обнаружения угроз системы предотвращения вторжений IPS.

- **Автоматизация как средство сокращения затрат и упрощения системы.** Помимо прочего, центр управления Cisco FireSIGHT помогает администраторам в согласовании операций, направленных на классификацию угроз, оценку их воздействия, автоматическую настройку параметров политики безопасности, а также в сопоставлении идентификационной информации пользователей с событиями безопасности. Центр управления осуществляет непрерывный мониторинг изменений в сети, выполняя автоматическую оценку угроз с целью выявления событий, требующих незамедлительного принятия ответных мер. Благодаря углубленному представлению о состоянии сети сотрудники по безопасности могут направлять основные усилия на восстановление системы и оптимизацию средств обеспечения ее безопасности.
- **Интеграция с решениями сторонних производителей.** Cisco ASA с сервисами FirePOWER обеспечивает возможность бесперебойной и прозрачной интеграции с решениями по обеспечению безопасности сторонних производителей, включая средства обнаружения уязвимостей, решения по управлению программным обеспечением, системы классификации проблем или полученных от абонентов жалоб, что, в конечном итоге, позволяет оптимизировать совокупную стоимость владения (TCO). Вы получаете преимущества открытой системы в сочетании с возможностями Cisco OpenSource. OpenAppID, открытый язык обнаружения, ориентированный на приложения и процессорный модуль для Snort®, системы предотвращения и обнаружения вторжений (IPS/IDS), разработанной Sourcefire, позволяет специалистам в области ИТ создавать, внедрять средства обнаружения приложений и предоставлять к ним общий доступ.

Рисунок 2. Cisco ASA с сервисами FirePOWER

Cisco ASA с сервисами FirePOWER: дополнительные аргументы в пользу приобретения

Выбирая Cisco ASA с сервисами FirePOWER в качестве решения NGFW, вы приобретаете ряд неоспоримых преимуществ.

- **Защита инвестиций.** Программы финансирования Cisco Capital® доступны на условиях, выгодных для вашего бизнеса и бюджета. Заключая договор аренды с Cisco Capital на выгодных для вас условиях, вы можете платить за эксплуатацию оборудования, а не за владение им. Вы имеете возможность гибкого дооснащения и обновления оборудования по мере необходимости, тем самым устраняя риск его устаревания.
- **Дополнительные услуги и техническая поддержка.** Корпорация Cisco получила сертификацию компании J.D. Power по программам предоставления технологических услуг и оказания поддержки сроком на пять и восемь лет[4]. Предложения по оказанию услуг и поддержки Cisco в рамках Cisco ASA с сервисами FirePOWER.
  - **Услуги Cisco по миграции для межсетевых экранов**, предоставляемые инженерами Cisco по безопасности или специализированными партнерами Cisco по безопасности, предназначены для оказания поддержки организациям в рамках перехода на Cisco ASA с сервисами FirePOWER. Экспертное руководство и поддержка Cisco помогают предприятиям сохранить информационную безопасность во время миграции, а также повысить точность и завершенность процессов.
  - **Услуги удаленного управления Cisco** позволяют сократить совокупную стоимость владения (TCO) путем непрерывного мониторинга и управления системой безопасности сети, тем самым предоставляя ИТ-персоналу возможность сфокусироваться на ключевых бизнес-приоритетах.
  - **Услуги Cisco по оптимизации сетей** включают набор интеллектуальных аналитических инструментов, оснащенных интуитивным графическим интерфейсом и позволяющих получить максимально углубленное представление о производительности сети. Данные преимущества обеспечивают возможности упрощения сети, повышения производительности, контроля соблюдения политик безопасности, сокращения рисков, а также проактивного обнаружения и нейтрализации потенциальных нарушений в работе сети. Данная услуга значительно повышает рентабельность инвестиций, согласно исследованию Forrester Research, превышая показатель в 120 процентов[5].

[4] «Корпорация Cisco отмечена за выдающееся качество обслуживания заказчиков в рамках программ предоставления технологических услуг и оказания поддержки сроком на пять и восемь лет», пресс-релиз J.D. Power, 21 июля 2014 г.: http://www.jdpower.com/press-releases/certified-technology-service-and-support-program#sthash.7oyGxBUo.dpuf.
[5] «*Общий экономический эффект™ как результат предоставления услуги Cisco по оптимизации сети и оказания целенаправленной технической поддержки»,* отчет подготовлен Forrester Research для Cisco, ноябрь 2009 г: http://www.cisco.com/en/US/services/ps6889/TEI_of_SP_NOS_FTS_Forrester.pdf.

- **Пакет услуг Cisco SMARTnet®** помогает снизить простои сети и сократить количество других критических проблем благодаря службе круглосуточной технической поддержки, а также широкому охвату обслуживаемого оборудования и проактивной диагностике устройств.

Загрузка программного обеспечения

Для загрузки ПО Cisco ASA с сервисами FirePOWER посетите центр Cisco Software Center.

Дополнительная информация

Дополнительные сведения см. на веб-страницах:

- www.cisco.com/go/asafps — более подробно о Cisco ASA с сервисами FirePOWER;
- www.cisco.com/go/asa — более подробно о межсетевых экранах нового поколения Cisco ASA серии 5500-X;
- www.cisco.com/go/services/security — более подробно об услугах Cisco по миграции для межсетевых экранов;
- www.cisco.com/go/smartnet — более подробно о пакете услуг Cisco SMARTnet;
- www.ciscocapital.com — дополнительная информация и ссылки для обращения к местным представителям Cisco Capital.

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

Напечатано в США C11-733098-00 10/14