Требования к межсетевому экрану нового поколения для предприятий малого и среднего бизнеса и географически распределенных предприятий

Аргументы в пользу внедрения межсетевого экрана нового поколения на предприятиях малого и среднего бизнеса

Необходимость в межсетевых экранах нового поколения (NGFWs), ориентированных на защиту от угроз и способных эффективно снизить риски, что не под силу традиционным унифицированным системам предотвращения угроз (UTM) и отдельным специализированным решениям, подтверждена многочисленными исследованиями, в том числе и исследованиями компании Cisco — каждая организация должна понимать, что она может стать целью атаки хакеров. Специалисты Cisco по исследованию угроз обнаружили вредоносный трафик в 100 % корпоративных сетей, участвующих в проверке, что говорит о том, что злоумышленники часто проникали в эти сети и, возможно, оставались незамеченными на протяжении продолжительного периода времени.[1]

Современные многовекторные угрозы и непрерывные атаки, быстроменяющиеся ИТ-среды и повышение мобильности пользователей заставляют все больше компаний искать такой межсетевой экран, который бы смог обеспечить доступную и эффективную многоуровневую защиту от угроз. Сегодня появился целый ряд новых решений, которые пытаются решить эту задачу. Однако межсетевой экран, который бы включал в себя все необходимые функции для эффективной защиты, найти до сих пор очень сложно.

С существенными проблемами в области обеспечения информационной безопасности сталкиваются не только крупные предприятия, **но и любая организация, независимо от размера**. Как отмечается в отчете Национальной ассоциации информационной безопасности США, в 2014 году 41 % кибератак был направлен непосредственно на нанесение ущерба организациям со штатом до 500 сотрудников. Более того, по сообщению газеты *The New York Times,* в 2014 году все большее число компаний среднего и малого бизнеса обращалось к своим крупным партнерам за помощью во внедрении более эффективных программ защиты от угроз. Неудивительно, что усовершенствованная защита от угроз стала предметом обсуждений руководителями компаний на высшем уровне. Организации любых размеров заинтересованы в надежной защите данных своих клиентов, информации о сотрудниках, интеллектуальной собственности и корпоративных секретов.

Уже очевидно, что потребность малых предприятий в усовершенствованных средствах защиты от угроз, включая межсетевые экраны нового поколения, очень высока. Согласно результатам «Сравнительного исследования возможностей обеспечения информационной безопасности Cisco за 2015 год»,[2] в ходе которого были опрошены сотни ИТ-специалистов из 9 стран, организации среднего размера (500-999

[1] Ежегодный отчет Cisco по информационной безопасности за 2014 год: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
[2] Ежегодный отчет Cisco по информационной безопасности за 2015 год: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

сотрудников) успешно перенимают опыт более крупных аналогичных компаний в том, что касается следующих вопросов обеспечения безопасности:

- **Реагирование на инциденты**: в 92 % организаций среднего бизнеса имеются группы реагирования на внутренние инциденты (по сравнению с 93 % крупных предприятий).
- **Ответственные руководители:** в 94 % организаций среднего бизнеса имеются руководители, напрямую отвечающие за безопасность (по сравнению с 92 % более крупных предприятий).

Межсетевые экраны нового поколения уже давно считаются лучшими инструментами обеспечения безопасности, широко используемыми крупными организациями. Еще совсем недавно для организаций малого и среднего бизнеса и географически распределенных предприятий традиционно предлагалось только два варианта развертывания средств безопасности сети: унифицированные решения по предотвращению угроз (UTM), с ограниченными возможностями устранения угроз, или несколько разрозненных решений, предоставляющих отдельные функции: межсетевой экран с контролем состояния, управление приложениями, IPS и расширенные возможности защиты от вредоносного ПО. Ни один из этих вариантов не был в состоянии полностью удовлетворить потребности таких организаций: в первом случае приходилось довольствоваться защитой только от самых распространенных угроз, которую обеспечивали решения UTM, во втором — решать проблемы интеграции и управления множеством разрозненных решений, что выливалось в большие расходы. Теперь же появилась новая возможность: **межсетевой экран нового поколения (NGFW), специально адаптированный в соответствии с потребностями предприятий малого и среднего бизнеса и географически распределенных предприятий, с расширенными функциями защиты от угроз, низкой совокупной стоимостью владения и гибким управлением.**

Этот официальный документ окончательно убедит вас в том, что предприятиям малого бизнеса или распределенным предприятиям необходимо инвестировать средства в эффективное решение NGFW. Для малых предприятий NGFW должен стать приемлемым по цене и управляемым проводником на их пути к построению системы усовершенствованной защиты от угроз. В филиалах и на географически распределенных предприятиях NGFW станет точкой обнаружения угроз и их мониторинга, будет в реальном времени анализировать угрозы и сетевой трафик на всем его пути и даст возможность получить полное представление о сети, частью которой он является. В обоих этих сценариях использования NGFW поможет обеспечить защиту вашей организации от целенаправленных, непрерывных атак вредоносного ПО, включая новые угрозы.

Критерии оценки основных решений по обеспечению безопасности сети

Как при оценке NGFW, так и при оценке решения UTM, важно понимать три основных фактора успеха. Ваше решение NGFW должно быть:

- **Предназначено специально для предприятий малого и среднего бизнеса и географически распределенных предприятий**
- **Ориентировано на защиту от угроз для эффективного обеспечения информационной безопасности и расширенной защиты от вредоносного ПО**
- **Обеспечивать снижение сложности и затрат**

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Решение, созданное специально для предприятий малого и среднего бизнеса и географически распределенных предприятий

Главный критерий здесь — «соответствие требованиям» — и не только с точки зрения затрат на приобретение и пропускной способности, но также и возможностей управления. На большинстве предприятий малого и среднего бизнеса ресурсы ограничены, т. е. типична ситуация, когда несколько ИТ-сотрудников отвечают за информационную безопасность, и это является лишь одной из многих других их должностных обязанностей. Таким предприятиям нужны решения по обеспечению безопасности, которыми можно эффективно управлять.

Если в крупных организациях обычно есть ресурсы и они могут позволить себе пользоваться всеми преимуществами установленных решений по управлению инцидентами и событиями информационной безопасности (SEIM), то для большинства небольших компаний такое решение может оказаться непрактичным. ИТ-менеджеру, ответственному за информационную безопасность, часто просто необходимо понимать, какие угрозы имеют наиболее высокий приоритет, чтобы его сотрудники могли быстро найти и устранить их.

Гибкость управления также важна для того, чтобы по мере роста организации, например при добавлении в ее структуру удаленных офисов, не обесценились первоначальные инвестиции. Обычно локальное управление больше подходит для развертывания одного экземпляра, а при развертывании нескольких экземпляров лучше использовать централизованное управление.

Решение, ориентированное на защиту от угроз

Более ранние межсетевые экраны и унифицированные решения по предотвращению угроз обычно объединяют в себе несколько разных функций безопасности, однако эффективность защиты при этом недостаточна. В них нет ни функциональности предотвращения вторжений (IPS) нового поколения (NGIPS), ни усовершенствованной защиты от вредоносного ПО. Для того чтобы решение по безопасности было действительно ориентировано на защиту от угроз, оно обязательно должно включать межсетевой экран с контролем состояния подключений, а также NGIPS и усовершенствованную защиту от вредоносных программ для обеспечения прозрачности сети и возможности идентификации и устранения вредоносных программ.

Помимо оценки угроз, NGFW должен иметь возможность составлять отчет по индикаторам компрометации (IoC) на основе корреляции как известных, так и предполагаемых факторов поведения, а также контролировать действия пользователей для определения аномального поведения. Для снижения воздействия угроз, а также соответствия нормативным требованиям или политикам внутреннего использования эти инструменты должны быть интегрированы с репутационной фильтрацией URL-адресов, функциями мониторинга приложений и контроля доступа.

Решение должно также устранять распространенные, но важные сетевые риски за счет использования политик доступа, сегментирования виртуальной сети и обеспечения надежных подключений типа «узел-узел» и удаленного VPN-доступа. Именно этот основополагающий критерий можно назвать отправным при принятии решения о покупке NGFW. Например, не все решения по управлению приложениями уровня 7 включают лучшие в своем классе функции межсетевого экрана с контролем состояния подключений и возможность подключения через VPN.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

И последнее, и возможно самое главное, NGFW должен обеспечивать непревзойденную производительность, даже тогда, когда одновременно работает несколько сервисов безопасности. Здесь важно найти поставщика, который поможет вам масштабировать ваше решение в соответствии с требованиями вашей среды и безопасности, и выбрать платформу, способную удовлетворить как ваши текущие, так и будущие потребности.

Снижение сложности и сокращение затрат

В некоторых организациях имеется выделенный центр по обеспечению безопасности (SOC) или выделенные сотрудники, занимающиеся обеспечением информационной безопасности. Оценивая решение для обеспечения безопасности, ответьте на следующие вопросы:

- Сможет ли это решение использоваться обычными ИТ-специалистами?
- Сможет ли это решение сократить время выполнения сотрудниками трудоемких операций, таких, например, как ликвидация последствий воздействия вредоносного ПО?
- Способно ли оно избавить ваших аналитиков от необходимости каждый раз решать, какие события действительно важны и требуют принятия определенных мер?
- Обеспечит ли это решение автоматизацию функций безопасности, чтобы средства защиты автоматически подстраивались в соответствии с индивидуальными политиками и постоянно меняющейся средой?
- Предоставляет ли это решение согласованную и ясную картину событий, которая позволит оптимизировать и ускорить приоритизацию и анализ?

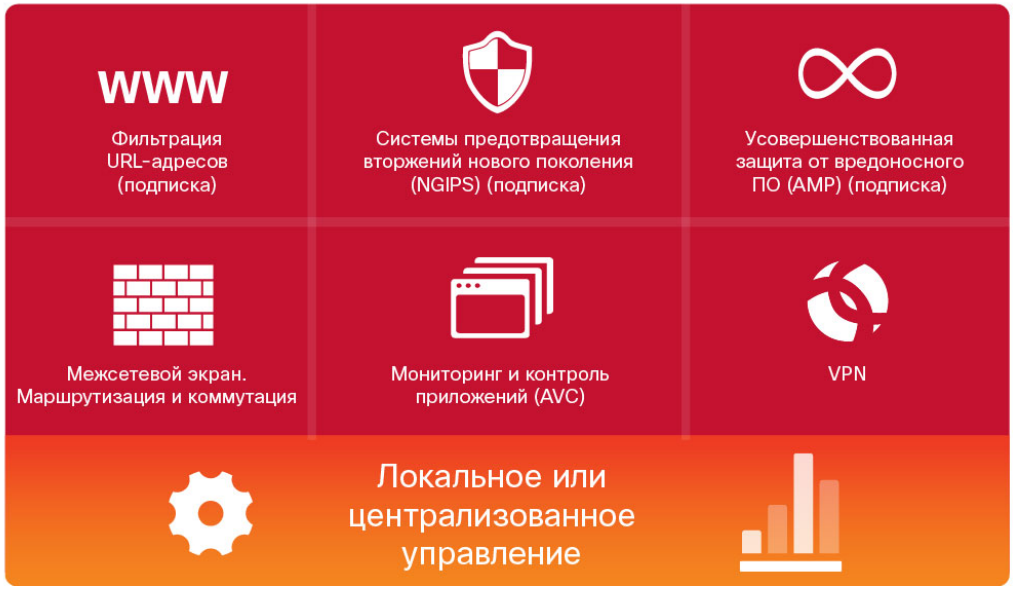
Удовлетворение потребностей предприятий малого и среднего бизнеса: Cisco ASA с сервисами FirePOWER

Cisco ASA с сервисами FirePOWER™, представленный моделями 5506-X, 5508-X и 5516-X, а также моделью 5506H-X — для использования в неблагоприятных условиях и моделью 5506W-X — с возможностью беспроводного доступа, обеспечивает непревзойденную защиту от угроз, низкую совокупную стоимость владения и гибкость управления. Межсетевой экран с контролем состояния подключений, VPN и все функции NGFW объединены в одном локальном модуле, расширенной версии Cisco Adaptive Security Device Manager (ASDM), что идеально подходит для развертывания одного экземпляра и автономных систем.

Если предпочтительным вариантом является централизованное управление, управление межсетевым экраном ASA с сервисами FirePOWER осуществляется посредством решений Cisco Security Manager (CSM) и Cisco FireSIGHT™ Management Center. При использовании централизованного управления только это решение NGFW обеспечивает интегрированную защиту от угроз на всем протяжении атаки — до, во время и после (см. рис. 1).

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Рис. 1. Cisco ASA с сервисами FirePOWER



Cisco ASA с сервисами FirePOWER — это первое ориентированное на защиту от угроз решение NGFW, созданное 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. Решение NGFW объединяет проверенные функции безопасности **многофункционального устройства обеспечения безопасности Cisco ASA и сервисов FirePOWER**.

Cisco ASA

Cisco ASA — это наиболее широко распространенный межсетевой экран корпоративного класса с контролем состояния, функциями удаленного доступа к сетям VPN и расширенной кластеризацией, обеспечивающий быстрый и безопасный доступ и высокую надежность систем для непрерывности бизнес-процессов. Кроме того, решение тесно интегрируется с мобильным клиентом Cisco AnyConnect® версии 4, который, помимо прочего, поддерживает раздельное VPN-туннелирование на основе приложений. VPN-клиент Cisco AnyConnect — самый распространенный в мире VPN-клиент, его использует более 130 миллионов пользователей. В случае если организации предпочитают использовать собственные VPN-клиенты, многие из них также поддерживаются Cisco ASA, а также оригинальными клиентами, включая Apple iOS и Samsung Android.

Сервисы Cisco FirePOWER

Лучшая в своем классе многоуровневая защита от угроз на одной платформе

Сервисы FirePOWER — это лучшая в отрасли система защиты от угроз и вредоносных программ, обеспечивающая первоклассную и эффективную защиту от угроз, подтвержденную результатами независимых испытаний, проведенных компанией NSS Labs.[3]

---

[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=Cj0KEQjw7bgBRC45uLY_avSrdgBEiQAD3OIx8BtffrsQkNYs3AtCojRqyy42V1yLfGyh78OMov3iUAaAlNc8P8HAQ.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Как показано на рисунке 1, Cisco ASA с сервисами FirePOWER обеспечивает следующие возможности:

- **Непревзойденная система многоуровневой защиты от угроз** обеспечивает защиту от известных и неизвестных типов угроз, включая целенаправленные и непрерывные 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.
- **Система предотвращения вторжений нового поколения (NGIPS)** обеспечивает эффективное предотвращение угроз и полный учет контекста пользователей, инфраструктуры, приложений и контента, 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. По оценкам агентства Gartner Group, конкурирующие решения UTM и NGFW предоставляют лишь базовые возможности IPS, но не полноценную функциональность NGIPS.
- **Функция детального мониторинга и контроля приложений (AVC)** поддерживает распознавание более 3000 приложений и управление рисками для них на основании установленных политик обнаружения угроз в системе предотвращения вторжений IPS, что позволяет значительно повысить эффективность защиты.
- **Надежная функциональность VPN** обеспечивает не только традиционные подключения типа «узел-узел» и возможности удаленного доступа, но также и более широкие возможности VPN для мобильных устройств, включая возможность раздельного туннелирования важных корпоративных приложений и пользовательских приложений, используемых в личных целях.

Гибкие возможности управления

Cisco ASA с сервисами FirePOWER предлагает широкий выбор решений для управления, как централизованных, так и локальных. Для развертывания одного экземпляра рекомендуется использовать локальное решение Cisco Adaptive Security Device Manager (ASDM) версии 7.3 и более поздних. Решение ASDM отличает возможность консолидированного управления всеми функциями NGFW и сокращения временных трудозатрат сотрудников на управление NGFW. В случае развертывания нескольких экземпляров управление Cisco ASA с сервисами FirePOWER осуществляется централизованно посредством решения Cisco FireSIGHT Management Center. Это решение 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.

В таблице 1 ниже приведены различия между решениями Cisco FireSIGHT Management Center и ASDM.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Таблице 1. Сравнение решений FireSIGHT Management Center и Adaptive Security Device Manager (ASDM)

Возможности	FireSIGHT Management Center (централизованное, удаленное управление)	ASDM (локальное управление)
Обзор	Управление до 300 сенсорами ASA с сервисами FirePOWER на один экземпляр FireSIGHT. FireSIGHT используется вместе с Cisco Security Manager (CSM).	Локальный, встроенный модуль управления, поставляемый по умолчанию во всех конфигурациях: оптимально использовать в небольших организациях и при развертывании одного экземпляра. Интегрированное управление всей функциональностью продуктов с удобным интерфейсом.
Учет контекста и мониторинг	Расширенная функциональность: включена базовая функциональность, а также возможность пассивного обнаружения узлов сети, функция Context Explorer и отслеживание пути файлов.	Базовая функциональность: геолокация и теги клиента поддерживаются по умолчанию. События IPS могут экспортироваться в SEIM для учета контекста на основе SEIM.
Сетевое средство защиты от вредоносных программ (AMP)	Расширенная функциональность: включена базовая функциональность, а также захват файлов, изоляция их в «песочнице» и динамический анализ. Для решения для оконечных устройств необходим сервис FireSIGHT с усовершенствованной защитой от вредоносных программ Cisco AMP (расширяет возможности контроля, обеспечивает исправление клиента).	Базовая функциональность: обнаружение и блокирование вредоносного ПО и запрещенных типов файлов за счет анализа файла. Обеспечение доступа к облаку Cisco для анализа вредоносного ПО (хеши файлов, файлы .not отправляются в облако для анализа).
Панель управления	Расширенная функциональность: на панели управления FireSIGHT Context Explorer можно посмотреть динамически обновляемые данные визуализации и анализа сетевой среды.	Базовая функциональность: на панели управления решения ASDM имеются виджеты, предоставляющие информацию о лицензии, данные мониторинга системы, сведения о модуле FirePOWER и т. д. Здесь же можно посмотреть информацию о системе.
Автоматизация, анализ степени воздействия, корреляция событий и т. д.	Включено: автоматическая оценка угроз с целью установления приоритетов и степени воздействия, функции корреляции и восстановления для оперативного реагирования на угрозы и автоматизированная настройка политик для защиты от новых угроз.	Отсутствует.
IPS	Расширенная функциональность: включена базовая функциональность, а также настройка предварительного процессора и полная функциональность NGIPS в соответствии с определением компании Gartner Group.	Базовая функциональность: использование модуля IPS Snort и функции настройки правил IPS.
Пользователи/обнаружение пользователей и геолокация	Полная функциональность. Интеграция с Active Directory и контроль доступа на основании данных геолокации трафика.	Полная функциональность. Интеграция с Active Directory и контроль доступа на основании данных геолокации трафика.
Мониторинг и контроль приложений (AVC)	Расширенная функциональность: включена базовая функциональность, а также детекторы пользовательских приложений на основе сопоставления с регулярными выражениями или обнаружение протоколов и портов.	Базовая функциональность: включена функция мониторинга и контроля доступа на уровне 7, с поддержкой распознавания более 3000 приложений и управлением угроз для них.
Проверка работоспособности	Расширенная функциональность: включена базовая функциональность, а также настраиваемые предупреждения о возможных неисправностях по более чем 30 функциям.	Базовая функциональность: состояние ЦП и загрузки памяти.
Политики системы	Расширенная функциональность: включена базовая функциональность, а также более 17 функций управления доступом, ведения журнала и предупреждений. В отличие от параметров системы, которые индивидуальны для каждого отдельного устройства, такие политики обычно одинаковы для всего развертывания.	Базовая функциональность: уведомления по электронной почте, поддержка протокола Simple Network Management Protocol (SNMP) и синхронизация времени.

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Возможности	FireSIGHT Management Center (централизованное, удаленное управление)	ASDM (локальное управление)
Отчетность	Расширенная функциональность: включена базовая функциональность, а также пользовательские шаблоны и возможность экспорта.	Базовая функциональность: фильтрация и отчетность по основному трафику, типам файлов, пользователям, приложениям и многому другому.
События	Расширенная функциональность: включена базовая функциональность, а также: больше емкость хранения событий и скорость обработки событий в секунду.	Базовая функциональность: поток событий в реальном времени для устранения неполадок.
Поддержка API	Расширенная функциональность: включена базовая функциональность, а также восстановление, входные данные узла и API-интерфейсы для доступа к базе данных.	Базовая функциональность: API-интерфейс FirePOWER eStreamer для совместного использования событий с платформами SEIM.

Более подробная информация о функции мониторинга, предоставляемой решением Cisco FireSIGHT Management Center, содержится в документе «Требования, которые необходимые учитывать при выборе межсетевого экрана нового поколения».

Дополнительная информация: средства Cisco для анализа угроз и каналы передачи информации об угрозах

Для более эффективной защиты как от уже известных, так и от новых угроз, организациям необходимо решение NGFW, которое включает в себя лучшие в отрасли средства анализа угроз для обеспечения защиты на современном уровне. Исследователи угроз из экосистемы коллективной информационной безопасности (CSI) объединяют наиболее полные в отрасли аналитические данные по угрозам, данные телеметрии от огромного количества устройств и сенсоров, информацию из общедоступных и частных веб-каналов по уязвимостям, а также от сообщества разработчиков открытого ПО, поддерживаемого Cisco. Ежедневный объем этой информации составляют миллиарды веб-запросов, миллионы сообщений электронной почты, образцов вредоносного ПО и данных о сетевых проникновениях.

Эти данные обрабатываются в развитой инфраструктуре, которая позволяет исследователям и самообучающимся системам отслеживать угрозы в различных сетях, центрах обработки данных, терминалах, мобильных устройствах, виртуальных системах, веб-сайтах, электронной почте и облачных системах с целью определения основных причин и масштабов распространения угроз. Итоговые данные анализа немедленно распространяются по всему миру среди клиентов Cisco и используются для защиты наших продуктов и сервисов в режиме реального времени. Решения Cisco по обеспечению безопасности постоянно обновляются последней информацией об угрозах, которая поступает по каналам передачи такой информации.

Выбирая Cisco ASA с сервисами FirePOWER в качестве решения NGFW, вы получаете следующие преимущества.

- Услуга Cisco SMARTnet
- Защита инвестиций
- Сервисы и техническая поддержка

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Услуга Cisco SMARTnet

Эта услуга обеспечивает доступ к технической экспертной поддержке 24 часа в день, 365 дней в году, а также предоставляет гибкие возможностям по ремонту оборудования. Cisco получила сертификат J.D. Power, предоставляя сертифицированную J.D. Power программу предоставления технологических услуг и оказания поддержки сроком на пять и восемь лет.[4]

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.

Сервисы и техническая поддержка

Предложения по оказанию услуг и поддержки Cisco в рамках Cisco ASA с сервисами FirePOWER включают:

- **Услуги Cisco по миграции для межсетевых экранов:** предоставляются инженерами Cisco по безопасности или специализированными партнерами Cisco по безопасности и 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 Cisco по удаленному управлению:** с помощью этих услуг обеспечивается непрерывная проверка соблюдения требований безопасности, и ваши ИТ-специалисты смогут сосредоточить свое внимание на других задач.
- **Услуги Cisco по оптимизации сети:** оптимизируют работу сети, соблюдение политик, надежность и значительно повышают окупаемость инвестиций, которая, по данным исследования Forrester Research, может превышать 120 %.[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] Отчет «Общий экономический эффект от использования услуги оптимизации сети и выделенной технической поддержки Cisco (The Total Economic Impact™ of Cisco SP Network Optimization Service and Focused Technical Support)», подготовленный Forrester Research для компании Cisco, ноябрь, 2009 г.: http://www.cisco.com/en/US/services/ps6889/TEI_of_SP_NOS_FTS_Forrester.pdf

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.

Дополнительная информация

Для получения дополнительной информации о решениях и услугах для межсетевых экранов нового поколения Cisco NGFW посетите следующие страницы:

- 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
- www.meraki.cisco.com — дополнительная информация о решениях Cisco Meraki
- www.cisco.com/go/mmsecurity — последняя информация о продуктах, решениях и тенденциях Cisco в сфере информационной безопасности
- www.cisco.com/go/partnermidmarket — информация для партнеров Cisco, анонсы последних решений и событий

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

Cisco и логотип Cisco являются товарными знаками или зарегистрированными товарными знаками корпорации Cisco и/или ее дочерних компаний в США и других странах. Чтобы просмотреть список товарных знаков Cisco, перейдите по ссылке: www.cisco.com/go/trademarks. Товарные знаки сторонних организаций, упомянутые в настоящем документе, являются собственностью соответствующих владельцев. Использование слова «партнер» не подразумевает наличия партнерских взаимоотношений между Cisco и любой другой компанией. (1110R)

Напечатано в США C11-734294-00 04/15

© Корпорация Cisco и/или ее дочерние компании, 2015. Все права защищены.
В данном документе содержится общедоступная информация корпорации Cisco.