

Check Point Software Technologies - мировой лидер в области решений для защиты информации в Интернет. Компания признана ведущей на мировом рынке средств обеспечения информационной безопасности среди производителей корпоративных и персональных межсетевых экранов - Firewall, а также средств организации защищенных каналов взаимодействия - VPN. Набор продуктов Check Point позволяет реализовать функции широкого диапазона средств защиты Периметра сети, Web-соединений, обеспечения внутренней безопасности сети. Возможности продуктовой линейки компании позволяют наилучшим образом решить задачи обеспечения безопасности сетевой инфраструктуры компании. Продукты и решения компании Check Point продает и поддерживает сеть из 2,200 партнеров Check Point в 88 странах мира.



Сетевая безопасность

В наши дни компании сталкиваются с растущим числом угроз безопасности сети – по периметру, внутри сети, конечных узлах сетей. Решение каждой задачи в отдельности может привести к использованию все большего числа средств безопасности, сложно совместимых между собой и трудно управляемых.

Решения Check Point лидируют на рынке средств защиты сетевой инфраструктуры. Реализованная в данных решениях концепция единой архитектуры безопасности Check Point позволит Вам создать универсальную многоуровневую защиту своих сетевых ресурсов.

UTM-решения компании Check Point включают в себя линейку устройств для полной защиты периметра, от устройств Edge для небольших офисов (для 50-ти человек) до сверхмощных - с пропускной способностью измеряемой десятками гигабит в секунду.

Крупные банковские структуры часто используют edge-устройства для защиты банкоматов.

Уникальное на рынке специализированное решение Connectra позволяет удаленным и мобильным работникам безопасно и эффективно работать, получая доступ к корпоративным ресурсам из любой точки мира.

Защита данных

Для предприятий различных масштабов и государственных учреждений существует опасность потери конфиденциальных данных из-за потери ноутбука, USB-накопителей и других мобильных устройств хранения данных. Растет необходимость в безупречном решении, которое способно обеспечить безопасность данных на всех широко распространенных платформах, легко устанавливается, масштабируется в соответствии с потребностями предприятия любого размера и удовлетворяет жестким требованиям законодательства о защите тайны частной жизни и региональных нормативных актов.

Решения Check Point позволяют защитить данные на настольных и переносных ПК, мобильных устройствах и переносных накопителях. Сертифицированные независимыми организациями продукты Check Point в области защиты данных дают заказчикам гарантию соответствия нормативным требованиям предприятия, правительства. Благодаря эффективному сочетанию средств шифрования содержимого всего диска и данных на сменных носителях, контролю доступа и управлению портами обеспечивается безупречная защита информации.

Защита конечных точек сети

Check Point Endpoint Security™ - первый единый клиент безопасности для комплексной защиты конечных точек сети. Решение объединяет межсетевой экран, антивирусное и антишпионское ПО, средства контроля доступа к сети (NAC), программный контроль, средства защиты данных и организации удаленного доступа.

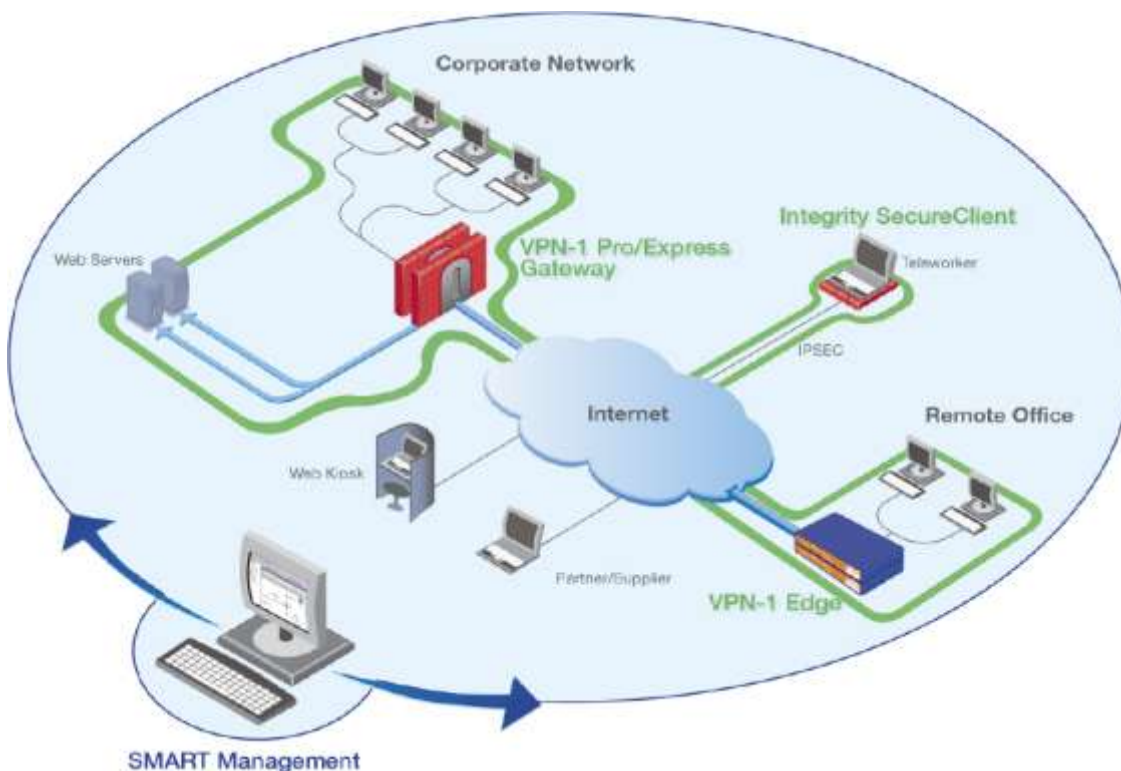
Решение Check Point обеспечивает непревзойденную защиту компьютеров, а также исключает необходимость в установке и управлении нескольких клиентов безопасности, что позволяет снизить общую стоимость владения системой безопасности.

Управление безопасностью

Сегодняшние компании вынуждены решать сложную проблему управления средствами безопасности. Ведь для обеспечения необходимого уровня защиты, компаниям приходится сочетать широкий спектр технологий информационной безопасности. Кроме того, есть ограничения в бюджете и необходимость соблюдения непрерывности бизнес-процессов.

Решения Check Point по управлению безопасностью представляют собой взаимозависимую систему, созданную на основе единой архитектуры безопасности. Это позволяет компаниям централизованно управлять политиками безопасности на различных уровнях инфраструктуры Check Point.

Типичная схема организации работы распределенной корпоративной сети на основе продукции Check Point



Case Study II *EQUITABLE BANK*

EQUITABLE BANK – был основан в 1927 году и долгое время специализировался на работе с клиентами приобретающими недвижимость. За последние годы банк значительно расширился, и хотя работа с недвижимостью остается его основной деятельностью – список услуг расширился до кредитования и других целей. *EQUITABLE BANK* всегда гордился скоростью и качеством работы своих сотрудников.

Сейчас банк открыл 10 отделений, в которых работают около 150-ти сотрудников. Это поставило его перед необходимостью построения распределенной, высокопроизводительной и безопасной корпоративной сети. Однако, как и многие представители среднего бизнеса, банк имел ограниченный ИТ-бюджет. С другой стороны, руководство штата предъявляло жесткие требования к финансовым структурам в области обеспечения безопасности данных пользователей.

Банк заменил старый интернет-канал на 100мбит, новым, оптоволоконным, предоставляемым местными провайдерами. Кроме того, банк нуждался в безопасном надежном VPN-решении, для организации удаленного доступа и соединения с сайтом-восстановления-после-сбоев. Местный интегратор - *JSO Technologies* порекомендовал *Check Point Express* как наилучшее решение в этой области. Оно включает в себя межсетевой экран, средство контроля приложений, VPN и простое централизованное управление. Используя это решение, *EQUITABLE BANK* соединил все разрозненные офисы в единую защищенную сеть.

Выгоды от использования решения Check Point:

- Удобные инструменты для работы сотрудников банка
- Надежный план восстановления после сбоев
- Добавление нового офиса в сеть компании происходит значительно проще
- Простое централизованное управление
- Соответствие стандартам безопасности

Использование Check Point Edge для защиты банкоматного трафика.

Многофункциональность устройств сетевой защиты Check Point Edge, учитывая невысокую цену, делает его оптимальным решением для защиты многочисленных критических точек банковской инфраструктуры, которыми являются банкоматы.

Реализация управления безопасностью в распределённой сети является важной частью системы защиты, поскольку напрямую влияет на качество защиты и затраты на обслуживание. Устройства VPN-1 Edge централизованно управляются через единую консоль станции управления SmartCenter, используемую также и для управления межсетевыми экранами и site-to-site VPN. Интеграция компоненты LSM (Large-scale VPN management) в станцию управления Check Point SmartCenter позволяет комфортно осуществлять все функции управления системой (настройка и установка политик безопасности на удаленные сайты) и компонентами системы защиты (лицензиями, сертификатами, обновлением программного обеспечения) для неограниченного количества удаленных шлюзов из единой точки управления, например, из главного офиса.

Case Study II. Major Bulgarian bank

Задача стоявшая перед банком

Задача обеспечения конфиденциальности и доступности данных, передаваемых через общедоступные каналы связи, представляет сегодня наиважнейшую задачу для любого банка, предоставляющего онлайн сервисы своим клиентам. Кроме того, эта задача является критичной как для бизнеса, так и для репутации банка. Для повышения качества обслуживания клиентов, перед сотрудниками отдела информационной безопасности банка была поставлена задача обеспечения защиты транзакций, конфиденциальности передаваемых данных между удалёнными банкоматами и главным офисом, а также обеспечения высокой надежности доступа к ресурсам сети банка.

Технические условия

Большое количество территориально распределённых банкоматов (320 шт.).

Банкоматы работают на базе операционной системы WinNT, не имеющей встроенных средств обеспечения необходимого уровня защищённости данных. Необходимость в централизованном управлении всей системой защиты.

Предложенное решение

Для решения поставленных задач, было предложено использовать решения компании Check-Point: VPN-1 Pro, VPN Edge, SmartCenter. Программный продукт VPN-1 Pro используется в качестве VPN-образующего шлюза в отказоустойчивой конфигурации в главном офисе, а в качестве конечных устройств для создания VPN-каналов защиты передаваемых данных между главным офисом и банкоматами использованы программно-аппаратные решения VPN-1 Edge, со специальной лицензией на два узла (два IP-адреса). Для управления территориально распределённой системой защиты на базе VPN-1 Edge и шлюза VPN-1 Pro, использовано программное обеспечение SmartCenter с встроенной компонентой LSM.

Защищённость передачи информации

Программное решение VPN-I Pro и программно-аппаратные решения VPN-I Edge позволяют установить защищенные VPN-каналы для обмена информацией между банкоматами и внутренними серверами банка, предотвращая попытки неправомерного доступа к конфиденциальной информации клиентов со стороны третьих лиц. Эти задачи решаются, в том числе с помощью встроенного в VPN-I Pro и VPN Edge продукта Check Point Firewall-1, включающего в себя самые передовые технологии контроля и предотвращения несанкционированного доступа, а также внутренний сервер цифровых сертификатов для более строгой аутентификации. Архитектура устройств VPN-I Edge позволяет довольно легко и быстро их интегрировать в существующую сеть, и, кроме того, решение не требует установки дополнительного программного обеспечения непосредственно на банкомат.

Надежность и доступность

Программное решение VPN-I Pro может быть установлено в отказоустойчивой конфигурации (High Availability), обеспечивая бесперебойную работу шлюзов VPN в главном офисе, и позволяя сотрудникам и клиентам банка быть уверенными в доступности необходимых им сервисов. Это решение позволяет организовать резервирование таким образом, что при выходе из строя основного шлюза весь трафик переключается на резервный шлюз, причем это происходит незаметно для всех пользователей, поскольку между главным и резервным шлюзом происходит синхронизация состояния и данных. Кроме того, после того, как основной шлюз возвращается в рабочее состояние, автоматически происходит переключение трафика на основной шлюз, а временно рабочий шлюз вновь становится резервным. Второе переключение происходит также незаметно для пользователей сервисов, поскольку ни одна сессия при этом не прерывается. Отказоустойчивая конфигурация на базе продуктов Check Point может включать в себя до 5 шлюзов, что позволяет обеспечить необходимый для любой компании уровень надежности доступа к ресурсам.