Check Point
SOFTWARE TECHNOLOGIES LTD.

РЕШЕНИЯ CHECK POINT ДЛЯ ОПЕРАТОРОВ СВЯЗИ И СЕРВИС-ПРОВАЙДЕРОВ

Современную организацию трудно представить без информационных систем. Информация, ее сбор, обработка, хранение и передача являются важнейшей частью бизнес-процессов компаний принадлежащих различным секторам экономики. И безопасность информации безусловно рассматривается сейчас как важнейшая часть процесса управления рисками. Это в большей степени очевидно для телекоммуникационных компаний, для которых информация и операции с ней связанные являются самой сущностью их бизнеса и, следовательно, областью, где информационный ущерб напрямую сопряжен с ущербом репутационным и финансовым.

Операторы связи, провайдеры различных информационных услуг всегда были объектами пристального внимания злоумышленников и неудивительно, что рост значимости информационной компоненты бизнеса приводит к росту угроз, идущих из киберпространства. Но одновременно перед современной телекоммуникационной компанией стоят и вызовы другого рода. Постоянно меняющийся ландшафт информационного поля требует адекватного ответа – изменения своих информационных систем. Растущие возможности каналов обмена информацией, увеличение скоростей и объемов передаваемого трафика, появление новых технологий передачи данных, мобильность пользователей, лавинообразное распространение персональных устройств, виртуализация и облачные сервисы – вот лишь некоторые отличительные черты того киберпространства, с которым работает современная телекоммуникационная компания. В условиях жесткой конкуренции на постоянно меняющемся рынке информационных услуг важным преимуществом провайдера становится возможность обеспечить устойчивость и адекватную защиту предоставляемых сервисов, а также предложить своим клиентам новые услуги, в том числе и сервисы по обеспечению информационной безопасности. Телекоммуникационным компаниям приходится, таким образом, отвечать на вызовы, брошенные не только им самим, но так же и их клиентам, покрывая широкий спектр возможных угроз.

Появление новых векторов атак, связанных с таргетированными действиями, угрозами «нулевого дня», распределенными атаками типа «отказ в обслуживании» (DDoS) большой мощности, возросший уровень «хактивизма», активное использование социальных сетей как инструмента распространения вредоносного ПО, кибервойны, ведущиеся крупными компаниями и правительствами, – все это наряду с традиционными угрозами требует изменения механизмов и процессов обеспечения информационной безопасности (ИБ) на уровне операторов связи.

Говоря о современных проблемах, стоящих перед телекоммуникационными компаниями, нельзя не упомянуть также и о задачах, связанных с обеспечением соответствия информационных систем требованиям различных регуляторов. Такие требования могут предъявляться как государственными, так и отраслевыми организациями, а также сертификационными органами. Соответствие таким требованиям рассматривается операторами связи как одна из важнейших компонент управления рисками и, безусловно, должна оказывать влияние на систему ИБ.

При построении системы защиты неизбежно приходится решать задачу оптимизации со многими ограничениями. Это тем более важно в случае оператора связи, где передача информации и предоставление услуг с ней связанных составляет самую сущность бизнеса. Экономическая эффективность такой системы будет напрямую влиять на финансовые показатели компании. Основными факторами, влияющими на решение такой задачи, являются:

- Необходимость обеспечения гибкости решения с учетом динамики информационных систем (например, появление новых технологий передачи данных, вариативность профиля сервисов, востребованных клиентами) и изменения ландшафта угроз;
- Необходимость соблюдения параметров производительности системы ИБ как части инфраструктуры оператора связи;
- Необходимость обеспечения ИБ в информационных системах, разделенных между многими клиентами, включая виртуальные и облачные;
- Требование обеспечения эффективности инвестиций и минимизации себестоимости предоставляемых сервисов;
- Возрастание значения требований регуляторов.

Компания Check Point Software Technologies Ltd. (www.checkpoint.com) предлагает широкий спектр продуктов и решений, позволяющих телекоммуникационным компаниям построить эффективную систему информационной безопасности, отвечающую совре-

менным и перспективным требованиям. Являясь мировым лидером по обеспечению безопасности в сети Интернет, она предлагает своим клиентам надежную защиту против всех типов угроз, уменьшая сложность задачи по обеспечению безопасности и снижая совокупную стоимость владения. Будучи первой компанией, представившей на рынок межсетевой экран FireWall-1 с запатентованной технологией Stateful Inspection, Check Point и сегодня продолжает быть инновационной компанией, предоставляя клиентам простые и гибкие решения, которые могут быть полностью адаптированы для соответствия требованиям безопасности любой организации. Check Point является единственным производителем, который не ограничивается только лишь технологией, но определяет безопасность как бизнес-процесс. Подход компании Check Point к ИБ уникальным образом сочетает политики, человеческий фактор и обеспечение соблюдения требований для создания более эффективной защиты информационных активов и помогает организациям внедрить решения ИБ, соответствующие их бизнес-требованиям.

Ключевыми компонентами, составляющими решение компании Check Point по защите информационной системы телекоммуникационных компаний, являются:

- Защита инфраструктуры оператора связи, включая защиту сетей мобильных операторов, использующих технологии 3G и 4G LTE;
- Механизмы безопасности, связанные с технологиями виртуализации: программно-определяемые сети (SDN, Software Defined Networks) и виртуализация сетевых функций (NFV, Network Function Virtualization);
- Механизмы построения виртуальных частных сетей (VPN);
- Система управления сервисами безопасности;
- Обеспечение соответствия требованиям регуляторов.

Защита инфраструктуры оператора связи

Определяя информационную безопасность как непрерывный бизнес-процесс, компания Check Point предоставляет телекоммуникационным компаниям решения для защиты всех элементов их инфраструктуры, учитывая развитие и особенности используемых технологий передачи данных.

И если для традиционных операторов фиксированных услуг передачи данных и голоса механизмы защиты определяются хорошо известными решениями, такими как межсетевой экран, система предотвращения вторжений и система противодействия атакам класса «распределенный отказ в обслуживании» (DDoS), то для мобильных операторов задача по обеспечению информационной безопасности представляется куда более сложной.

С лавинообразным распространением мобильных устройств и увеличением базы подписчиков операторы все более превращаются из поставщиков базовых сервисов передачи голоса или данных в интернет-провайдеров, что ставит перед ними три главные задачи:

- Поддерживать максимальную пропускную способность и доступность своих сетей;
- Обеспечивать широкий спектр услуг и надлежащий уровень удобства их использования для своих подписчиков;
- Обеспечивать защиту своих мобильных сетей, данных пользователей и их устройств от текущих и перспективных угроз.

Успешное решение этих задач чрезвычайно важно в свете сохранения лояльности клиентов, обеспечения роста бизнеса и поддержания репутации. Однако развитие возможностей мобильных устройств и постоянно растущие запросы пользователей в смысле более быстрого и функционально богатого интернет-сервиса приносит новые риски в сети операторов связи, как традиционные 3G, так и новые 4G.

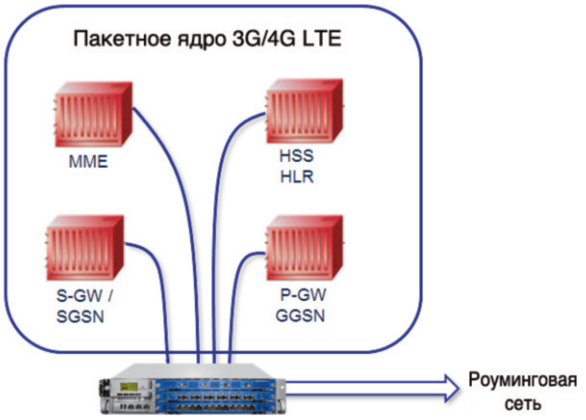
Быстрый рост использования смартфонов и мобильных приложений, приводящий к избыточной сигнальной нагрузке в сетях, оказывает влияние на сетевую производительность, вызывая эффект ненамеренной атаки «отказ в обслуживании». Также возросшее число мобильных устройств и приложений открывает двери новым уязвимостям прикладного уровня. Переход на архитектуру 4G LTE, базирующуюся на протоколе IP, означает, что сети операторов становятся уязвимыми для атак, основанных на IP, из интернета и сетей радиодоступа. Это приносит операторам новые, доселе не существовавшие вызовы, требующие новых подходов в обеспечении безопасности их сетей. Потенциально атакующий может проникнуть в частную опорную сеть оператора и получить доступ к незашифрованному трафику пользователей и сигнальному механизму управления сетью.

Для реализации возможных уязвимостей атакующий может использовать один из трех главных интерфейсов мобильной сетевой инфраструктуры:

- Интерфейс Gi/SGi, осуществляющий сопряжение мобильной сети GPRS / LTE, соединяющей миллионы мобильных устройств с интернетом и другими недо-

веренными сетями, что открывает возможность реализации всего спектра веб-угроз, включая вредоносное ПО, ботнеты, спуфинг, сканирование портов и многое другое;

- Интерфейс S1, соединяющий и проводящий аутентификацию тысяч базовых сотовых станций в мобильной сети;



- Интерфейс Gp/S8, соединяющий мобильные сети партнеров по роумингу мобильного оператора и предоставляющий доступ к внутренним сервисам и данным пакетного ядра.

Дополнительный риск как для сетей 3G, так и 4G происходит из-за увеличения развертывания микросотовых базовых станций публичного доступа в целях создания дополнительной емкости в общественных местах, таких как торговые центры, офисы и т.п. Эти малые устройства, размещенные в общедоступных местах, не могут быть обеспечены надежной физической защитой - такой, какую имеют обычные базовые станции. И это дает атакующим потенциально более легкие точки входа для атак на сеть.

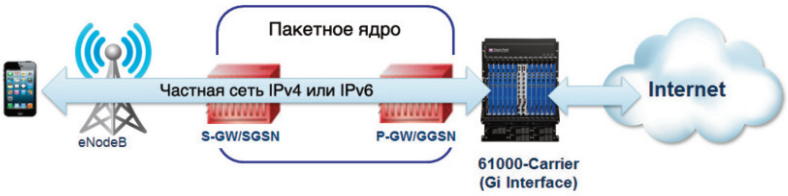
Также проблемой безопасности сетевой архитектуры LTE является возможность нарушения работы протоколов SCTP и Diameter и атаки DDoS между различными элементами мобильной сети. Необходимо помнить, что шлюзы сигнализации данных, мобильное пакетное ядро и сеть радиодоступа – все эти элементы инфраструктуры имеют потенциальные уязвимости.

Решения по безопасности операторов связи компании Check Point предоставляют им единую интегрированную платформу для обеспечения полной защиты сетей 3G и 4G LTE. Основанная на испытанных технологиях, используемых в ведущих телекоммуникационных компаниях по всему миру, решения по защите операторов связи Carrier Security компании Check Point обеспечивают безопасность ваших интерфейсов LTE, защищают мобильное пакетное ядро, позволяют осуществить безопасные соединения в роуминге и поддерживают широкий спектр дополнительных услуг безопасности для клиентов. Все это дает возможность операторам мобильных сетей и провайдерам максимизировать отдачу от инвестиций в инфраструктуру за счет целостной защиты, масштабируемости и возможности предоставлять управляемые сервисы ИБ для клиентов.

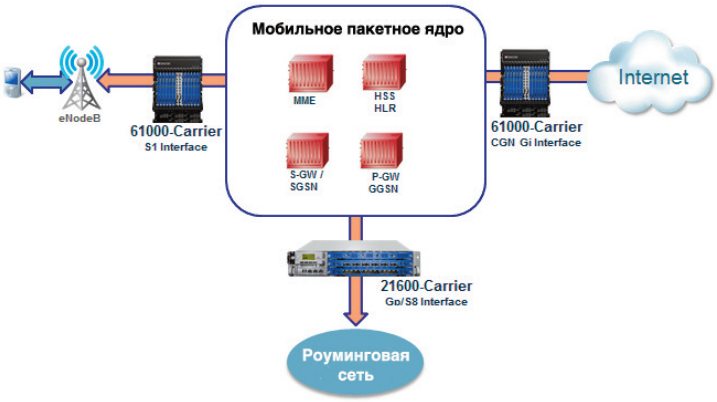
Интегрированная защита всей инфраструктуры оператора связи

Система безопасности оператора связи Check Point 41000 и 61000-Carrier Security System, а также устройства форм–фактора 2U 21700 и 21600-Carrier предлагают масштабируемые решения с оптимальным соотношением цена-качество для телекоммуникационных компаний любого масштаба. Эти решения предоставляют единую, интегрированную платформу для защиты интерфейсов 3G и 4G, соединенных с мобильным пакетным ядром, которая:

- Обеспечивает безопасное соединение тысяч станций 4G LTE (eNodeB) к пакетному ядру, используя технологию IPSec для авторизации и шифрования трафика пользователей;



- Защищает интернет-соединения устройств с помощью масштабируемого межсетевого экрана с NAT операторского класса (CGNAT) для IPv4 (NATP и NAT44(4) со статическим и динамическим распределением портов) и IPv6 (с поддержкой Двойного стека v4/v6 , туннелирования трафика IPv6 поверх IPv4 и IPv4 поверх IPv6, а также NAT46 и NAT64*), поддерживающего до 70 миллионов одновременных сессий;
- Содержит шлюз прикладного уровня для поддержки приложений, не поддерживающих или некорректно работающих с NAT (например, FTP, медиа-протоколы, p2p);
- Обеспечивает безопасность соединений с сетями роуминг-партнеров;
- Обеспечивает полный контроль инфраструктуры безопасности с использованием единых политик, мо-



ниторинга, системного журналирования и отчетов по всем интерфейсам оператора связи.

Компания Check Point является единственным производителем, предлагающим решения по инспекции всех протоколов LTE, включая GTP, SCTP и Diameter. Это позволяет реализовать беспрецедентную интегрированную систему безопасности сетей LTE, защищая от атак DDoS, сигнального шторма, сканирования портов, спуфинга и атак овербиллинга, усовершенствованного вредоносного ПО, а также обеспечить безопасность данных пользователей.

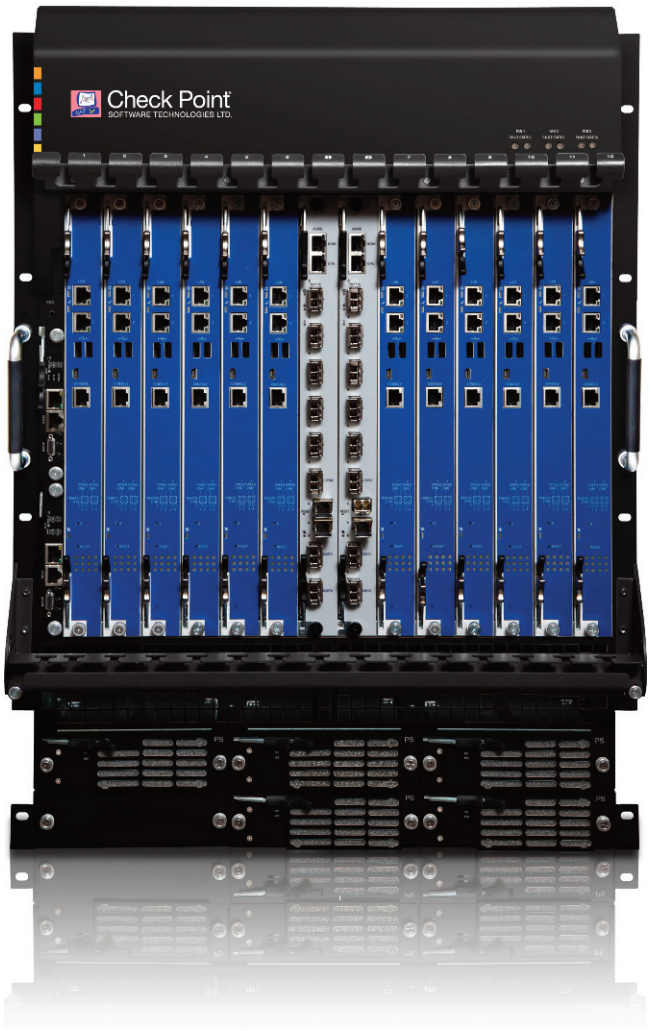
Уникальная производительность

Система безопасности Check Point 61000-Carrier Security System на сегодняшний день обеспечивает пропускную способность межсетевого экрана до 400 Гбит/с, а в будущем будет доведена до 1 Тбит/с. Кроме того, возможность поддержки до 70 миллионов конкурентных сессий и 600 000 сессий в секунду обеспечивает этому решению беспрецедентные характеристики производительности в сетях 3G и 4G LTE. Устройство 21700-Carrier предоставляет наилучшую в своем классе производительность мобильной безопасности, обеспечивая пропускную способность IPSec 50 Гбит/с и свыше 15 Гбит/с при инспекции протоколов GTP, SCTP и Diameter, а также беспрецедентную масштабируемость, характеристики обслуживания и плотность портов.

Непрерывность бизнеса, надежность и потенциал роста

Решения по безопасности операторов связи Check Point Carrier Security обеспечивают непрерывность бизнеса и удобство в обслуживании за счет такого функционала, как блоки питания с горячей заменой, избыточные дисковые массивы RAID с горячей заменой, резервные вентиляторы. Также решение позволяет легко развернуть и настроить дополнительные функции защиты, используя архитектуру программных модулей Check Point's Software Blade Architecture™.

Решения могут управляться как с помощью интегрированных средств управления безопасностью, так и с помощью единой системы менеджмента. Это упрощает сложную задачу управления в среде крупных провайдеров. Всеобъемлющая централизованная система управления позволяет контролировать все шлюзы Check Point, развернутые на мобильных сетевых интерфейсах, а усовершенствованная система анализа журналов дает возможность наблюдения в реальном времени за



миллиардами записей, сделанных в различные промежутки времени и в разных доменах управления.

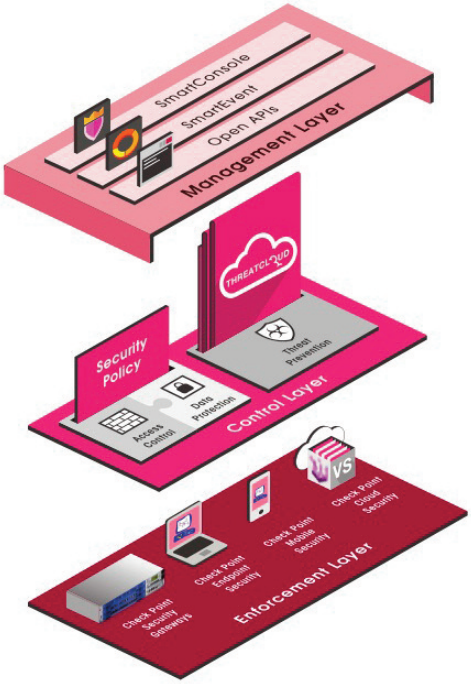
Использование Виртуальных Систем на платформе Check Point 61000-Carrier позволяет организации консолидировать до 250 виртуализованных шлюзов безопасности на одной аппаратной платформе. Это позволяет снизить себестоимость решения и предложить клиентам кастомизированные решения ИБ на базе виртуальных систем, использующих архитектуру программных модулей Software Blade. Такое решение позволяет бесшовно наращивать производительность системы, просто добавляя дополнительные Виртуальные Системы и аппаратные модули, равномерно распределяя трафик по всему шасси.

Безопасность технологий виртуализации сетей

Появление и последующий взрывной рост решений виртуализации, широкое использование облачных ресурсов наряду с повышением эффективности информационных систем принесли с собой и рост рисков, связанных с их применением. Технологии, связанные с созданием гибкой сетевой архитектуры, – программно-определяемые сети (SDN) и виртуализация сетевых функций (NVF), – дающие небывалую гибкость, также изменили и спектр угроз, создавая новые уязвимости и влияя на соответствие требованиям регуляторов. Для того чтобы адресовать эти риски, компания Check Point разработала пути интеграции своих решений с различными архитектурами SDN и NVF, давая возможность применения в программно-определяемых и виртуализованных сетевых средах различных сервисов по обеспечению многоуровневой защиты.

Технология SDN позволяет упростить развертывание и работу инфраструктуры, давая возможность вашей информационной системе (сети оператора или центру обработки данных) быстро меняться в соответствии с меняющимися требованиями. Но с такой же скоростью должны изменяться и сервисы безопасности. Интегрируя свои решения с различными решениями SDN, компания Check Point позволяет автоматически осуществлять провижининг сервисов безопасности через управление облачными системами. Это делает возможным безопасное и масштабируемое их развертывание и позволяет вам безопасно наращивать число приложений и сервисов в вашей сети.

Основу гибкости решений Check Point составляет уникальная адаптивная архитектура безопасности SDP (software-defined protection, программно-определяемая защита), представляющая собой новую парадигму – практический подход к реализации модульной и динамической инфраструктуры безопасности. Архитектура SDP делит инфраструктуру безопасности на три взаимосвязанных слоя:



- Уровень Применения (Enforcement Layer) – основан на физических, виртуальных или хостовых точках применения политик безопасности, осуществляет сегментацию сети и исполнение логики защиты в высокопроизводительных средах.
- Уровень Контроля (Control Layer) – анализирует различные источники информации об угрозах и создает защитные механизмы и политики, которые будут исполняться на Уровне Применения.
- Уровень Управления (Management Layer) – управляет инфраструктурой и обеспечивает высокий уровень быстроты реагирования для всей архитектуры.

Комбинируя высокопроизводительный Уровень Применения с быстро перестраивающимся динамическим программным Уровнем Контроля, архитектура SDP обеспечивает не только надежность в работе, но и возможность проактивно предотвращать инциденты безопасности при быстро меняющемся спектре угроз.

Созданная на перспективу, архитектура SDP поддерживает традиционные требования сетевой безопасности и контроля доступа, равно как и механизмы защиты от угроз, необходимых для современного предприятия, включая такие новые технологии, как мобильные вычисления и программно-определяемые сети SDN.

Решения Check Point позволяют обезопасить ваши системы от угроз, давая возможность контролировать трафик как в традиционном направлении «входящий-исходящий», так и трафик внутри вашей информационной системы (например, внутри центра обработки данных). Вы легко можете определять политики безопасности, которые смогут динамически меняться в физической или виртуальной среде вашей сети.

Используя решения Check Point, вы сможете в полной мере реализовать абсолютно новый подход к развертыванию, провижинингу и управлению всего спектра сервисов безопасности, обеспечивая защиту от современных угроз в физических, виртуальных и облачных средах.

Построение виртуальных частных сетей

Эффективность бизнеса современной компании в значительной мере зависит от качества функционирования информационной инфраструктуры. Работа сотрудников из территориально распределенных подразделений в едином информационном пространстве позволяет оптимизировать их взаимодействие, повышать эффективность бизнес-процессов. Особенно остро эта проблема стоит в свете постоянно растущего числа мобильных пользователей, которые могут находиться в любой точке мира и использовать самый

широкий спектр оборудования. Однако создание собственной телекоммуникационной сети, объединяющей подобных пользователей в компании, требует значительных капиталовложений, а ее эксплуатация – существенных непрофильных затрат. Поэтому большим спросом пользуется услуга по организации виртуальной частной сети (VPN, Virtual Private Network) предприятия, которую предлагают все современные операторы связи. Информация в такой сети передается по каналам общего пользования, а необходимая защищенность достигается на уровне протоколов информационного обмена.

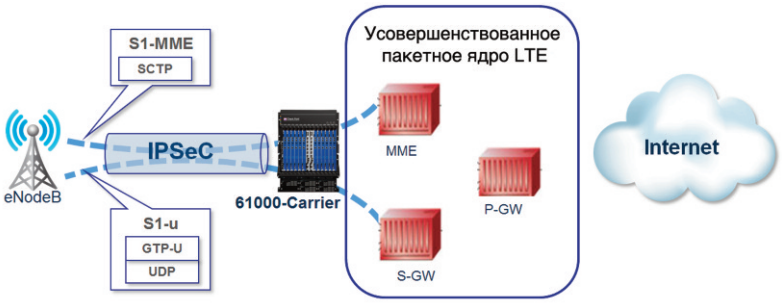
Во многих случаях экономически более целесообразно воспользоваться услугой поддержки VPN, предоставляемой оператором связи, который принимает на себя все вопросы технического и административного обеспечения бесперебойности ее работы. При этом клиент избавляется от необходимости приобретения, настройки и обслуживания телекоммуникационного оборудования, переносит эксплуатационные расходы на оператора.

Компания Check Point предоставляет в распоряжение своих заказчиков программный модуль Check Point IPSec VPN Software Blade, позволяющий организовать безопасное подключение к корпоративным сетям удаленных и мобильных пользователей, филиальных офисов и бизнес-партнеров. Программный модуль содержит в себе интегрированный контроль доступа, аутентификацию и криптозащиту для гарантии безопасности сетевых соединений поверх интернет.

Отличительными особенностями решения Check Point являются:

- Централизованная система управления «site-to-site» VPN и VPN для удаленного доступа;
- Повышенная защита IPSec VPN от атак «отказ в обслуживании», в том числе направленных против механизма обмена ключевой информацией IKE;
- Возможность применять политики безопасности в зависимости от уровня шифрования;
- Поддержка различных режимов создания VPN удаленного доступа для поддержки мобильных пользователей, использующих различные типы соединения (включая IPSec VPN, SSL VPN и L2TP);
- Поддержка различных методов построения VPN, включая VPN, базирующиеся на маршрутизации и базирующиеся на доменах;
- Простая активация и настройка VPN на любом шлюзе Check Point;
- Централизованное системное журналирование и отчеты в рамках единой консоли.

Другой важной областью применения IPSec VPN в информационной системе оператора связи является организация защищенных соединений между базовыми станциями и пакетным ядром. Это решение является рекомендованной 3GPP опцией для операторов мобильной связи при соединении в опорных LTE сетях. При этом очевидно, что оператор связи должен использовать решения, позволяющие ему обеспечить как надежность и гибкость соединения, так и потенциал масштабирования



при развитии сети. Ожидаемое увеличение трафика LTE и рост требований по полосе пропускания диктуют провайдерам выбирать решения с производительностью операторского класса, для того, чтобы соответствовать стандартам безопасности 3GPP.

Важными преимуществами решения Check Point в этом случае являются:

- Функциональная совместимость с любыми решениями инфраструктуры публичных ключей PKI сторонних производителей при использовании аутентификации по сертификатам для базовых станций eNodeB на уровне управления с узлом управления мобильностью MME (Mobile Management Entity) и на уровне данных со шлюзом сервиса S-GW (Serving Gateway). Предотвращение неавторизованного доступа базовых станций в пакетное ядро;
- Использование ESP и IKEv2 для обеспечения конфиденциальности и целостности с применением алгоритмов криптозащиты AES, SHA-1 или TripleDES. Защита от прослушивания и подделки данных на уровне управления (S1-MME) и в пользовательском трафике (S1-u);
- Беспрецедентная производительность с использованием протокола IPSec – от 30 Гбит/с на устройствах размера 2U до 56 Гбит/с на модульном шасси (измерено на реальном IMIX трафике S1 мобильных сетей);
- Поддержка до 50 000 туннелей IPSec на устройстве Check Point 61000;
- Быстрый провижининг IPSec для удаленных базовых станций eNodeB.

Система управления сервисами безопасности

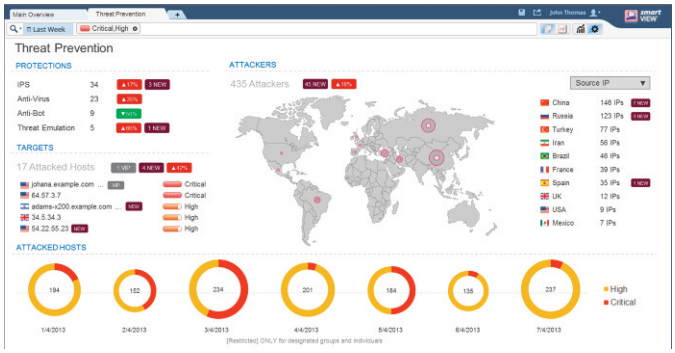
Стремительное развитие рынка телекоммуникаций требует от его участников постоянного поиска конкурентных преимуществ, способных как привлечь внимание новых подписчиков, так и повысить лояльность суще-

ствующих клиентов. Так на рынок выходят дополнительные сервисы, предлагаемые провайдерами для своих заказчиков. При таком подходе клиенту предлагается оформить подписку на полный комплекс услуг, связанный с тем или иным сервисом, что делает простым внедрение заказчиком того или иного функционала без необходимости устанавливать свои собственные системы и содержать свой собственный штат специалистов. Кроме того, данный подход позволяет клиенту получить функциональную гибкость и в случае необходимости легко изменять параметры предоставления сервиса. Такая концепция предоставления услуг получила название «управляемых сервисов» (managed services).

Информационная безопасность является для современных предприятий и организаций одной из важнейших областей информационных технологий. Быстро меняющиеся требования к информационному обеспечению бизнеса вызывают быстрое изменение информационной инфраструктуры компании, а также быстрое изменение ландшафта угроз. И эти угрозы требуют адекватных и своевременных средств защиты. К сожалению, не всякая компания может позволить себе самостоятельно и в надлежащем объеме решать проблемы обеспечения ИБ. Высокие издержки на поддержание средств защиты в надлежащем состоянии, постоянное изменение и усложнение угроз и требуемые затраты на их исследование, затраты на штат выделенных специалистов ИБ и мероприятия по постоянному контролю состояния безопасности не всегда приемлемы с точки зрения бизнеса. Поэтому все чаще компании обращают свое внимание на модель получения сервиса ИБ от своего оператора связи, выступающего как провайдер управляемых сервисов безопасности MSSP (managed security service provider). И рынок таких услуг постоянно растет. По прогнозам Gartner объем рынка аутсорсинга сервиса в области ИБ может вырасти с 13.7 миллионов долларов США в 2014 году до 21.5 миллиона долларов США в 2017.

Решения по безопасности операторов связи Check Point Carrier Security позволяют предложить вашим клиентам дополнительные сервисы информационной безопасности, такие как система предотвращения вторжений, антивирус, фильтрация URL, контроль приложений и антибот, реализованные непосредственно на шлюзе. Кроме того, операторы мобильной связи и сервис-провайдеры могут обеспечивать дополнительные услуги для мобильных подписчиков на основе идентификационной информации, что позволяет осуществлять дифференцированный подход к таким сервисам.

Компания Check Point предлагает провайдерам MSSP полный спектр решений для покрытия всех потенциальных категорий клиентов: предприятий, компаний малого и среднего бизнеса и мобильных пользователей. В их распоряжении находятся различные опции реализации защиты информации, такие как устройства, размещаемые на площадке заказчика, виртуальные шлюзы на оборудовании провайдера или облачный сервис с используемым решением Capsule для мобильных пользователей. Все это позволяет обеспечить защиту предприятия любого масштаба на всех уровнях, будь то периметр организации, отделение, центр обработки данных или мобильные пользователи.



Все средства защиты и точки применения политик Check Point управляются с помощью единой унифицированной консоли управления безопасностью, обладающей высокой степенью масштабируемости и дающей возможность управлять десятками миллионов объектов, сохраняя сверхбыстрое время отклика пользовательского интерфейса.

R:80

Основной платформой для такой системы управления может служить платформа R80 компании Check Point, специально спроектированная с учетом специфики MSSP и обладающая беспрецедентной масштабируемостью, возможностью обслуживать различных клиентов в рамках одной платформы и автоматизировать операции по управлению настройками ИБ с учетом делегации полномочий. Система поддерживает до 10 миллионов объектов политик на домен управления, позволяет организовать конкурентную работу одновременно 200 администраторам и способна хранить информацию о 15 миллиардах событий.

Платформа R80 реализует концепцию многодоменного управления, позволяя администраторам определять политики безопасности для каждого домена безопасности, выделяя отдельные домены для каждого клиента, сохраняя при этом разделение полномочий между администраторами провайдера и собственными администраторами ИБ клиента. В этом случае для предотвращения угроз, управления доступом и защиты данных каждый администратор получает возможность работы с удобным представлением политик безопасности, входящих в зону его ответственности.

Хорошо известно, что политики управления доступом и защиты данных являются специфическими для каждой организации и постоянно изменяются в зависимости от появления новых пользователей, приложений и новых бизнес-процессов. Для поддержки таких изменений в

бизнес-процессах система управления безопасностью Check Point предоставляет программные интерфейсы, позволяющие организациям проводить интеграцию с другими системами, такими как системы управления сетями, CRM, системы сопровождения запросов на поддержку, системы управления идентификационной информацией или системы управления облачными решениями. Открытый интерфейс к внешним системам позволяет системе управления «понимать» изменения в окружении и координировать политики безопасности в соответствии с ними.

Прозрачность является неотъемлемой частью надежной системы безопасности. В этой связи от системы управления требуется обеспечить как полную ситуативную информированность, так и возможности по реагированию на инциденты. Система Check Point SmartEvent выполняет анализ больших объемов данных и производит корреляцию событий в реальном времени. Это дает возможность получать консолидированную и коррелированную картину инцидента на основе информации из различных источников. Таким образом, создается точная картина события, что помогает ответственным за реагирование на инциденты определить необходимые действия, которые надо предпринять для защиты сети.

Анализ события безопасности представляет результаты в виде индикаторов угроз, которые могут быть переданы в систему ThreatCloud для блокировки угроз в реальном времени. Автоматические механизмы реагирования могут обеспечить сдерживание угрозы, предоставляя возможность предпринять необходимые действия перед возобновлением штатной работы.

Соответствие требованиям регуляторов

Соответствие требованиям регуляторов (compliance) рассматривается организациями как одна из важнейших областей управления рисками. Несоответствие корпорации таким требованиям может вылиться в значительные потери – вплоть до отзыва лицензий на деятельность. Поэтому компании прилагают серьезные усилия для обеспечения соответствия требованиям и ищут эффективные решения по управлению этим процессом.

Понимая это, компания Check Point предлагает организациям решение по контролю за соответствием требованиям регуляторов – модуль Compliance Software Blade, первый встроенный в систему безопасности полностью автоматический сервис такого рода. Решение позволяет обеспечить всестороннюю проверку настроек всех модулей безопасности относительно заданных требований. Система позволяет легко получить отчет о соответствии требованиям при подготовке к аудиту и рекомендации по изменению настроек, основанные на лучших практиках.

Также решение предоставляет возможность анализа влияния предполагаемых изменений конфигурации всех модулей системы безопасности на соответствие требованиям регуляторов в реальном времени.

Компания Check Point уделяет особое внимание сертификации своих продуктов и решений в соответствии с требованиями регулирующих органов РФ. Межсетевой экран компании Check Point традиционно сертифицируется по требованиям 3 класса ФСТЭК, ведется сертификация основных версий также на НДВ по 4 уровню контроля, сертифицируются компоненты системы предотвращения вторжений, антивируса. Система построения виртуальных сетей VPN имеет возможность использования отечественного алгоритма криптозащиты ГОСТ, что подтверждено документами сертифицирующих органов.

Превратите безопасность в двигатель

Учитывая тот факт, что информация является краеугольным камнем бизнеса, современные организации не могут позволить себе игнорировать вопросы безопасности. Без надлежащей политики безопасности как сама компания, так и ее клиенты подвергаются риску. Понимая потенциальные угрозы и уязвимости, создайте надежный план, соотнесенный с вашим бизнесом, и убедитесь, что механизмы защиты интегрированы в вашу IT-инфраструктуру. Тогда вы можете превратить безопасность в двигатель бизнеса, а не в его тормоз.

SECURITY CHECKUP

Сделайте проактивный шаг – убедитесь, что ваша организация защищена. Подпишитесь на CHECK POINT'S SECURITY CHECKUP – бесплатную онлайн-проверку, которая поможет выявить потенциальные риски вашей сети.

http://www.checkpoint.com/campaigns/securitycheckup/index.html

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Международная штаб-квартира

Check Point Software Technologies, Ltd.

5 Ha'Solelim Street, Tel Aviv 67897, Israel

Телефон: + 972-3-753-4555 • Факс: + 972-3-575-9256 • Эл. почта: info@checkpoint.com

•

Представительство в России и СНГ

Check Point Software Technologies (Russia) ООО

109240, Москва, ул. Николоямская, д. 13, стр. 17

Тел./факс: +7 495 967 7444 • http://rus.checkpoint.com

Материал подготовлен компанией RRC, официальным дистрибьютором Check Point в России и СНГ.
119331, Москва, Проспект Вернадского, д.29, офис 903. Тел.: +7 495 956 1717