Межсетевые экраны CheckPoint

В области межсетевых экранов (МЭ) CheckPoint является лидером в отрасли, предоставляя как аппаратные, так и программные решения.

Аппаратные решения предоставляют собой готовые мощные системы для развертывания программных решений Check Point, удовлетворяющие любую потребность в области информационной безопасности. Устройства разработаны на единой архитектуре безопасности, что в итоге, позволяет выполнять все операции по управлению безопасностью с единой, унифицированной консоли управления. Кроме того, благодаря революционной архитектуре "программных блейдов", появляется возможность быстро и гибко расширить функционал безопасности без необходимости добавления нового оборудования.

Решения подразделяются на следующие классы:

1. Устройства класса High End:
   - **линейка устройств Power-1**, которые используя современные технологии ускорения в сочетании с программными блейдами, обеспечивает высокопроизводительную платформу для защиты многогигабитных сред (крупные кампусные сети или центры обработки данных);

   - **интегрированные аппаратные решения (Integrated Appliance Solutions, IAS)**. Являясь программно-аппаратными комплексами, имеют настраиваемые технические характеристики, предоставляя возможность выбора платформ, которые наиболее точно отвечают корпоративным нуждам. Определив требуемый уровень производительности системы безопасности, компания Check Point устанавливает программное обеспечение (VPN-1 UTM, VPN-1 Power, VPN-1 Power VSX, а также Provider-1) на сервер или сверхтонкие серверы IBM, тем самым обеспечивая комплексное решение, включающее техническую поддержку Check Point.

2. Устройства унифицированного управления защитой от угроз:

   - **линейка устройств UTM-1**, обеспечивающие наиболее комплексную защиту сети. Устройства представляют собой универсальные и не требующие сложной настройки решения. Каждое устройство имеет встроенное централизованное

управление, а также возможность включения таких программных блейдов, как: FireWall, VPN, IPS, SSL VPN, защиту от вирусов, программ-шпионов и спама, специализированный межсетевой экран для защиты web-приложений и web-фильтрацию;

- **устройства Check Point UTM-1 Edge.** Обеспечивают всеобъемлющую защиту для филиалов, расширенные возможности соединений и удобное централизованное управление. UTM-1 Edge предоставляют возможности UTM, повышенную надежность и непревзойденную простоту в использовании. Из ключевых свойств UTM-1 Edge следует отметить технологию предотвращения вторжений Check Point SmartDefense (для защиты от известных и неизвестных типов атак), лёгкую организацию безопасных подключений к корпоративной сети с использованием VPN, избыточность в сети и балансировку нагрузки для обеспечения непрерывного соединения, мощную систему управления трафиком, которая назначает приоритеты и распределяет полосу пропускания трафика, централизованную автоматизированную схему распространения обновлений, соответствие стандартам для производственных помещений (по устойчивости к проникновению пыли, тепла, вибрации).

3. Устройства для малого бизнеса:
   - устройства унифицированного управления защитой от угроз Safe@Office.

Данные устройства уже в состоянии поставки обеспечивают интегрированные средства защиты, а также сетевые и коммуникационные возможности. Являясь простым, надежным и доступным решением, Safe@Office используют технологии МЭ аналогичные более дорогим и высокопроизводительным устройствам, также позволяя производить защиту от вирусов на рубеже шлюза, защиту электронных сообщений, web-фильтрацию, контроль доступа к сети, управление трафиком (маршрутизация, QoS), а также организацию VPN и удалённого доступа.

Программный блейд Check Point Firewall благодаря установке на аппаратные платформы клиента обеспечивает необходимую начальную производительность, а также её наращивание, что в свою очередь обеспечивает гибкую масштабируемость решения, отвечающего возрастающим потребностям организации. Наращивая мощность аппаратной платформы, клиент получает возможность без значительных затрат в разы повышать производительность системы безопасности. Будучи функционально аналогичным устанавливаемым на аппаратные решения CheckPoint, программный блейд Check Point Firewall также, и в полной мере, обеспечивает высочайший уровень защиты, с контролем доступа, защитой приложений, аутентификацией и трансляцией сетевых адресов. Поддержка NAC позволяет блокировать доступ для неавторизованных пользователей сети и защищать корпоративные ресурсы. Firewall использует программные блейды для управления безопасностью (Security Management Software Blades), благодаря чему обеспечивается удобное удаленное управление средствами защиты с наивысшей эффективностью.

Для достижения максимальной производительности на шлюзах безопасности (как программных так и аппаратных) могут быть задействованы блейд Check Point Acceleration and Clustering, который использует передовые технологии SecureXL, CoreXL и ClusterXL. Данные технологии позволяют ускорить функции защиты путём принятия решений на более низком прикладном уровне, распределения трафика между ядрами в многоядерных системах, а также ускорить и повысить надёжность системы за счет кластеризации шлюзов безопасности и распределения нагрузки между ними.

При использовании програмного блейда Check Point Advanced Networking администраторы получат ряд таких сетевых возможностей как: динамическая маршрутизация, поддержка широковещательных сообщений (multicast), качество сервиса (QOS, Quality of Service), отказоустойчивость подключения к Интернет (ISP redundancy), балансировка нагрузки приложений. В совокупности, эти функциональные возможности позволяют быстро и просто развернуть систему безопасности в комплексных и высокоуровневых сетевых средах, например, в центрах обработки данных или крупных предприятиях, когда востребованы производительность и высокая доступность.

Защиту голосового трафика (а также видеоконференций) шлюзы безгопасности смогут обеспечить при включении блейда Check Point Voice over IP. Данный блейд защитит от червей и специфичных для VoIP атак на отказ в обслуживании, которые могут вызвать сбой сервисов IP-телефонии. Данное решение также понижает сложность предоставления услуг VoIP, поскольку исключают проблемы, связанные с несоответствием VoIP и NAT (Network Address Translation).

IPS

Решение Check Point IPS предоставляет исключительные возможности предотвращения вторжений на многогигабитных скоростях, обеспечивая лучшие в отрасли защиту и производительность системы безопасности. Check Point IPS - это надежная защита клиентского ПО, серверов, операционных систем от угроз безопасности, в т.ч. вредоносного ПО, червей и др. Для достижения высочайшего уровня сетевой защиты многоуровневый механизм IPS Threat Detection Engine использует множество различных методов обнаружения и анализа, в том числе: использование сигнатур уязвимостей и попыток их использования, выявление аномалий, анализ протоколов. Механизм IPS способен быстро фильтровать 90% входящего трафика без необходимости проведения глубокого анализа трафика, благодаря чему на наличие атак анализируются лишь соответствующие сегменты трафика, что ведет к понижению расходов и повышению точности.
В решении IPS применяются высокоуровневые средства динамического управления компании Check Point, что позволяет графически отображать только значимую информацию, легко и удобно изолировать данные, требующие дальнейших действий со стороны администратора, а также соответствовать нормативным требованиям и стандартам отчетности. Кроме того, решения Check Point IPS - как программный блейд IPS, так и аппаратное устройство Check Point IPS-1 - управляются с помощью единой консоли управления SmartDashboard IPS, что обеспечивает унифицированное управление средствами IPS.
Программные блейды IPS и IPS SmartEvent представляют новую парадигму динамического управления, которая позволяет соответствовать современной сетевой среде - с высокими объемами трафика, постоянно эволюционирующими угрозами безопасности.
Процессы Check Point управления защитой от угроз позволяют Вам быстро и эффективно реагировать на постоянные изменения, снижая Ваши расходы на управление и обеспечивая быстрое применение обновлений.

Контроль приложений

Библиотека приложений Check Point Application Library обеспечивает сканирование и обнаружение свыше 4 500 приложений и более 50 000 виджетов - независимо от порта, протокола или используемых сетевых технологий. Поскольку интернет-приложения динамически меняются, библиотека приложений Check Point постоянно обновляется. Интеграция библиотеки приложений Check Point Application Library в шлюзы безопасности Check Point позволяет заказчикам безопасно использовать технологии Web 2.0.

DLP

Используя передовые разработки, технологии и процессы, компания Check Point предлагает революционно новый подход к предотвращению потери данных. Решение Check Point позволяет компаниям перейти от инертного обнаружения к активному предотвращению потерь данных. В состав предлагаемого решения входят:

- **система Check Point MultiSpect** представляет собой многофакторный механизм классификации данных - связей между пользователями, типами данных и процессами. Check Point DLP с исключительно высокой точностью проводит идентификацию конфиденциальных данных, в т.ч. персональной идентификационной информации (PII, personally identifiable information), данных на соответствие (HIPAA, SOX, PCI и др.) и конфиденциальной бизнес-информации.
- **система Check Point UserCheck**, помогающая пользователям устранять инциденты информационной безопасности в режиме реального времени. Данная технология предупреждает пользователей о возможном нарушении режима безопасности, позволяет оперативно устранить возникшее нарушение и не допустить утечки данных. Благодаря UserCheck пользователи могут самостоятельно администрировать обработку инцидента безопасности, с возможностью отправки, удаления и проверки запроса по инциденту. Благодаря этому улучшается знание пользователями корпоративных правил работы с информацией и повышается уровень защиты.
- **централизованное управление политиками безопасности,** с помощью которого система DLP управляется централизованно, через единую консоль управления Check Point Security Management. Централизованное управление обеспечивает лучшие контроль и применение политик безопасности, а также дает организациям возможность использования единого хранилища с заданными пользователями и группами, сетевыми объектами, правами доступа и политиками безопасности во всей инфраструктуре безопасности. Унифицированные правила доступа автоматически применяются во всей распределенной инфрастуктуре, обеспечивая защищенный доступ с любого места.

Благодаря предустановленным шаблонам, содержащим широкий спектр встроенных политик и правил безопасности, компании любого размера будут защищены с помощью этого решения с первого же дня его внедрения. Данное решение можно легко и быстро установить на любой шлюз безопасности Check Point (на базе устройств Check Point или на открытые сервера), что позволяет экономить время и средства благодаря использованию имеющейся у Вас инфраструктуры безопасности. Кроме того, для лучшего соответствия требованиям любой сетевой среды заказчика компания Check Point предлагает широкий спектр мощных и высокомасштабируемых устройств DLP-1.

Antivirus & Antimalware

Решение Check Point Antivirus & Anti-Spyware защищает от угроз, передаваемых по протоколам HTTP, FTP, SMTP и POP3. Благодаря постоянно обновляемому списку сигнатур антивирусного и антишпионского ПО и защите на основе обнаружения аномалий, программный блейд Antivirus and Anti-Malware останавливает вирусы и другое вредоносное ПО на рубеже шлюза, с избежанием вмешательства вирусов в работу пользователей. Интерфейсы Check Point содержат средства управления политиками безопасности, регистрации и мониторинга, и обеспечивают все преимущества простого и удобного управления средствами безопасности. В настройках по умолчанию проводится сканирование всех протоколов, однако опции сканирования каждого протокола можно централизованно настроить.

Блейд обеспечивает постоянное сканирование и анализ файлов до их загрузки. Если в ходе сканирования в файле обнаружен вирус, то доставка файла клиенту немедленно прекращается, в итоге, предотвращается заражение вирусом. Кроме того существует возможность определения направления сканирования, которое позволяет обнаружить и

проводить сканирование файлов, перемещающихся в определенном направлении - например, в корпоративную сеть или из нее, или в демилитаризованную зону DMZ. Конфигурация проводится по направлению, не по хосту, что позволяет администраторам безопасности применять более широкие политики безопасности с упрощенными правилами. Можно внести исключения по сканированию - для заданных пользователей или сетевых устройств будет идти беспрепятственная передача файлов.

Endpoint

Check Point Endpoint Security™ - первый и единственный единый клиент, содержащий все необходимые компоненты для комплексной защиты конечных точек сети, обеспечивающий высокий уровень защиты и прозрачный режим функционирования для пользователей. Кроме того, Check Point Endpoint Security является единственным единым клиентом безопасности, обеспечивающим как защиту данных, так и клиента VPN для организации безопасного удаленного доступа.

Решение включает в себя следующие модули:
- **межсетевой экран**, блокирующий нежелательный трафик, делает невидимыми для хакеров конечные точки сети и предотвращает заражение компьютеров вредоносным ПО;
- **браузер Check Point WebCheck,** обеспечивающий защиту корпоративных компьютеров от интернет-угроз с одновременно простым и прозрачным режимом функционирования для пользователей;
- **Check Point OneCheck,** предоставляющий удобный доступ ко всем подсистемам защиты конечных точек сети, включая Windows, шифрование содержимого диска ПК (disk encryption), шифрование данных на мобильных носителях (media encryption) и VPN;
- **модуль организации удаленного доступа,** который обеспечивает защищенный удаленный доступ к корпоративным ресурсам благодаря шифрованию и системы аутентификации передаваемых данных. Новая система VPN Auto-Connect обеспечивает непрерывное подключение пользователей при переходе от LAN-подключения к беспроводным и GPRS сетям, а также незаметно для пользователя выбирает правильную конфигурацию удаленного доступа к корпоративной сети;
- модуль программного контроля Program Advisor. Наличие данного модуля, позволяет выбирать и контролировать программы, запускаемые на компьютерах. Средство Program Advisor содержит динамично обновляемую базу данных из свыше миллиона известных программ, в т.ч. вредоносного ПО;
- средства защиты от вирусов и вредоносного ПО, которое позволяет обнаруживать и уничтожать вирусы, шпионское ПО, регистраторы клавиш, программы типа «троянский конь», руткиты и иные вредоносные программы, основанные на комбинировании сигнатур, блокираторах поведения и эвристическом анализе. При этом обеспечиваются высокие скорости обнаружения вредоносных объектов и ежечасное обновление сигнатур;
- **шифрование всего содержимого диска (Full Disk Encryption).** Благодаря сочетанию аутентификации до загрузки и надежного шифрования всего содержимого диска обеспечивается высочайший уровень защиты данных, хранящихся на переносных и настольных компьютерах;
- **модуль управления портами ПК (Port Protection) и шифрование данных на сменных носителях (Media Encryption).** Данный модуль обеспечивает защиту ценных корпоративных данных на сменных носителях путём шифрования съемных носителей (USB-устройств, DVD-дисков и др.) и управлению портами и устройствами, при котором осуществляется контроль над записью, чтением, выполнением;
- **модуль контроля доступа к сети (NAC).** До предоставления доступа к сети клиент безопасности Check Point Endpoint Security применяет комплексную политику контроля доступа к сети и проверяет, установлены ли на рабочей станции самые последние версии антивирусных программ, свежие патчи и обновления ПО, а также требуемые приложения, в т.ч. браузеры и клиенты VPN.
- **модуль поддержки централизованного управления.** Решение Check Point Endpoint Security обеспечивает централизованное развертывание, конфигурирование, управление

политиками безопасности, а также анализ и составление отчетов о событиях системы безопасности конечных точек сети с одной консоли.

Управление

Решение Check Point Security Management является лидирующим на рынке управления системами безопасности. Благодаря тому, что устройства созданы на основе гибкой архитектуры Check Point "программные блейды", компания Check Point впервые в отрасли предлагает высокомасштабируемое решение с единым управлением политиками безопасности сетей, IPS и конечных точек сети.

Единая менеджмент-консоль SmartDashboard охватывает управление следующими компонентами инфраструктуры безопасности от Check Point:

- управление сетевой безопасностью. Управление всеми устройствами безопасности осуществляется через единую политику безопасности, которая централизованно распространяется на все межсетевые экраны сети. Доступ к единой политике предоставлен через интуитивно понятный пользовательский интерфейс, в котором, несмотря на широкие возможности по настройке политик, сам процесс управления происходит просто и прозрачно. Сетевой уровень включает в себя управление:

- правилами межсетевого экрана;
- правилами трансляций сетевых адресов;
- настройками системы предотвращения атак (IPS);
- настройками системы контроля служб IM;
- настройками контент-фильтрации на межсетевых экранах;
- шифрованными туннелями связи (VPN) между шлюзами безопасности (отдельно стоит отметить технологию Check Point по построению VPN в одно нажатие «one-click VPN»);
- правилами приоритезации трафика (QoS);
- правилами межсетевых экранов на конечных рабочих станциях.

Консоль предусматривает ролевое управление с гранулярным распределением прав администраторам безопасности.

- система логирования и контроля состояний. Представляет собой мощную систему управления и агрегирования логов с устройств безопасности. В которой благодаря категоризации поступающих событий и широким возможностям конструктора фильтров, значительно упрощается локализация и поиск неисправностей, оптимизация политик безопасности, а также поиск потенциальных уязвимостей в существующих политиках.

- система управления политиками конечных пользователей. Предоставляет возможность построения необходимого набора политик безопасности для конечных точек (предпочтительна ролевая сегментация групп пользователей на основании LDAP). Такие наборы политик аккумулируются внутри единого клиента безопасности и применяются в зависимости от принадлежности пользователя работающего за рабочей станцией к той или иной ролевой группе. Единый клиент имеет модульную структуру и может состоять из следующих компонент:

- модуль межсетевого экрана;
- модуль разграничения сетей и назначении прав доступа к ним;
- модуль контроля сетевой активности приложений;
- модуль контроля приложений;
- модуль контроля доступа к сети, основывающийся на корпоративных требованиях необходимых обновлений которые должны быть установлены на рабочих станциях;
- модуль antispyware;
- антивирусный модуль.