Check Point®
SOFTWARE TECHNOLOGIES LTD.

РЕШЕНИЯ CHECK POINT ДЛЯ ЗАЩИТЫ ТЕХНОЛОГИЧЕСКИХ СЕТЕЙ

Введение

Современную организацию трудно представить без информационных систем. Информация, ее сбор, обработка, хранение и передача являются важнейшей частью бизнес-процессов компаний, принадлежащих различным секторам экономики. В связи с чем безопасность информации рассматривается сейчас как важнейшая часть процесса управления рисками. Это в большей степени становится очевидным, когда в организации существует непосредственная связь информационных систем с системами управления производственными процессами, составляющими основной бизнес компании, и, следовательно, областью, где информационный ущерб может стать причиной сбоев или остановки производства, что влечет за собой как репутационные, так и финансовые потери.

Современные промышленные компании и предприятия характеризуются широким использованием автоматизированных систем управления, важнейшей компонентой которых является автоматизированная система управления технологическим процессом (АСУ ТП) — комплекс технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях. Под АСУ ТП обычно понимается целостное решение, обеспечивающее автоматизацию основных операций технологического процесса на производстве в целом или каком-то его участке, выпускающем относительно завершенное изделие.

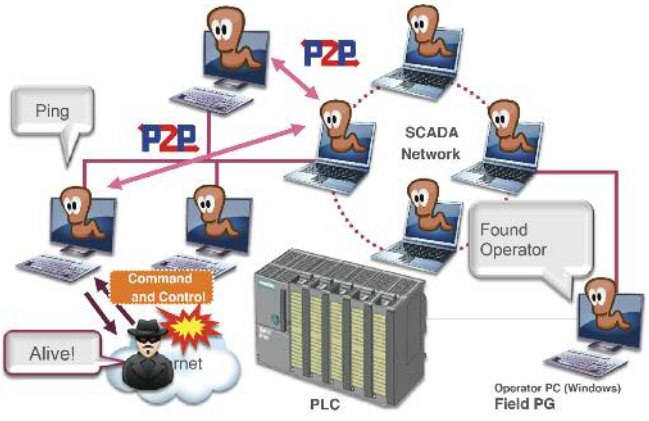
Составными частями АСУ ТП могут быть отдельные системы автоматического управления (САУ) и автоматизированные устройства, связанные в единый комплекс. Такие как системы диспетчерского управления и сбора данных (SCADA), распределенные системы управления (DCS) и другие более мелкие системы управления (например, системы на программируемых логических контроллерах (PLC)). Как правило, АСУ ТП имеет единую систему операторского управления технологическим процессом, средства обработки и архивирования информации о ходе процесса, типовые элементы автоматики: датчики, устройства управления, исполнительные устройства. Для информационной связи всех компонентов системы используются промышленные сети.

Хотя традиционно информационные системы АСУ ТП строились с использованием специальных, достаточно специфических технологий и протоколов обмена информацией, в последнее время наблюдается активный переход таких систем на использование стека протоколов TCP/IP, а также расширение применения операционных систем общего назначения. С одной стороны, это привносит в такие системы большую гибкость и адаптивность, с другой стороны – делает их восприимчивыми как к «классическим» угрозам информационной безопасности, так и угрозам, связанным с уязвимостями специфических протоколов АСУ ТП.

Промышленные предприятия и объекты критичной инфраструктуры находились под пристальным вниманием злоумышленников, и переход АСУ ТП на использование IP-сетей облегчил для них задачу по получению доступа к системам управления, что может привести к катастрофическим последствиям. Яркими примерами атак на АСУ ТП являются инциденты, связанные с атакой Stuxnet на АЭС в иранском Бушере в июне 2010 года, нарушение работы системы управления водоснабжением в Южном Хьюстоне в ноябре того же года и атака в июле 2011, поразившая 29 компаний химического сектора в Италии.

Появление новых векторов атак, связанных с таргетированными действиями, угрозами «нулевого дня», возросший уровень «хактивизма», активное использование злоумышленниками вредоносного ПО, кибервойны, ведущиеся крупными компаниями и правительствами – все это, наряду с традиционными угрозами, требует изменения механизмов и процессов обеспечения информационной безопасности (ИБ) промышленных предприятий.

Несмотря на то, что информационный сегмент АСУ ТП традиционно рассматривался как изолированная система, современные тенденции в построении информационной системы предприятия предусматривают интеграцию АСУ ТП с корпоративной сетью для обеспечения сбора информации о состоянии технологических процессов, контроля состояния оборудования и других задач. Использование технологий беспроводного доступа также повышает вероятность несанкционированного подключения непосредственно к сетям АСУ ТП. Кроме того стоит отметить, что для систем АСУ ТП, обычно имеющих длительный жизненный цикл, зачастую невозможна реализация практики поддержания необходимого уровня безопасности с помощью программных «заплаток», выпускаемых производителями операционных систем при обнаружении уязвимостей, так как системы АСУ ТП сертифицируются их производителями только при работе с определенными версиями ОС и программного обеспечения (ПО). В связи с этим существенно возрастает необходимость сегментирования сетей и обеспечения их безопасности за счет использования специализированных средств защиты (таких как средства межсетевого экранирования и обнаружения вторжений с поддержкой протоколов АСУ ТП, средства криптографической защиты каналов связи). Однако



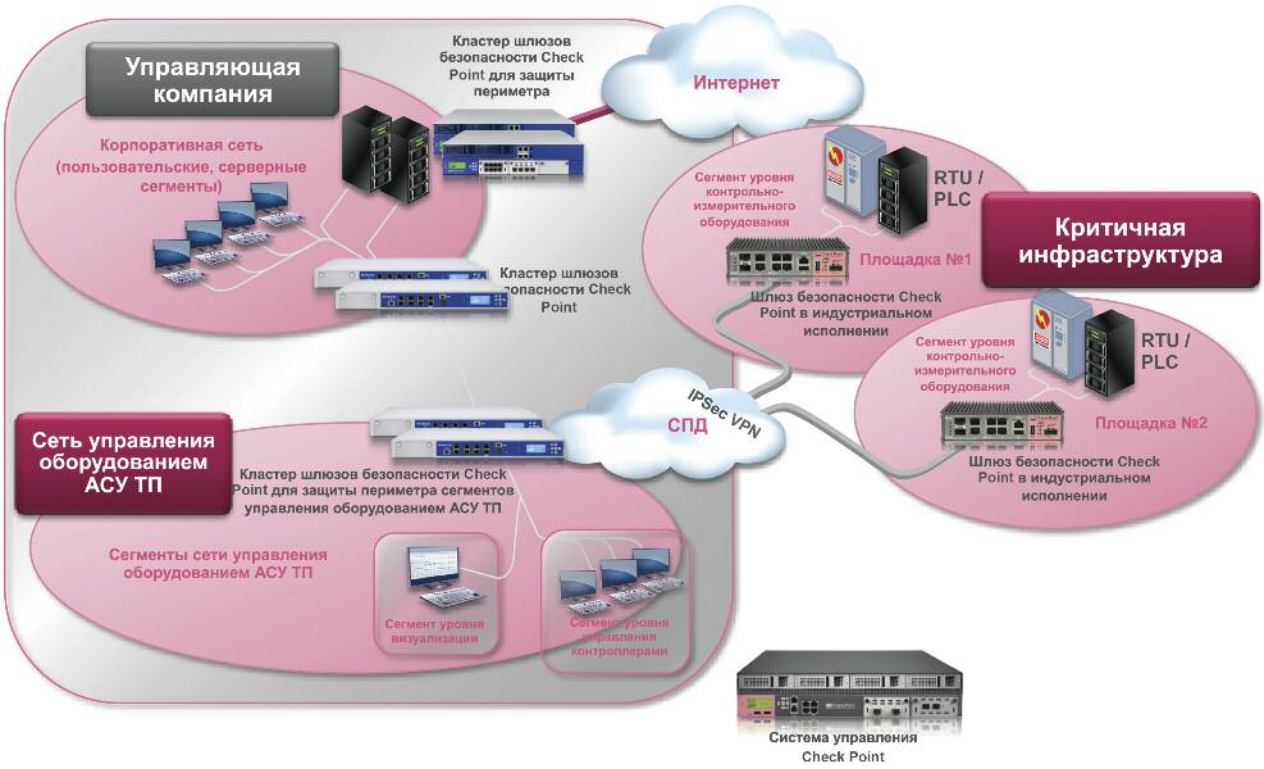
в силу специфики оборудования и ПО АСУ ТП обычные средства ИБ не могут обеспечить необходимый уровень защиты, так как они зачастую не поддерживают специфические технологии и протоколы и не рассчитаны на тяжелые (зачастую экстремальные) условия эксплуатации.

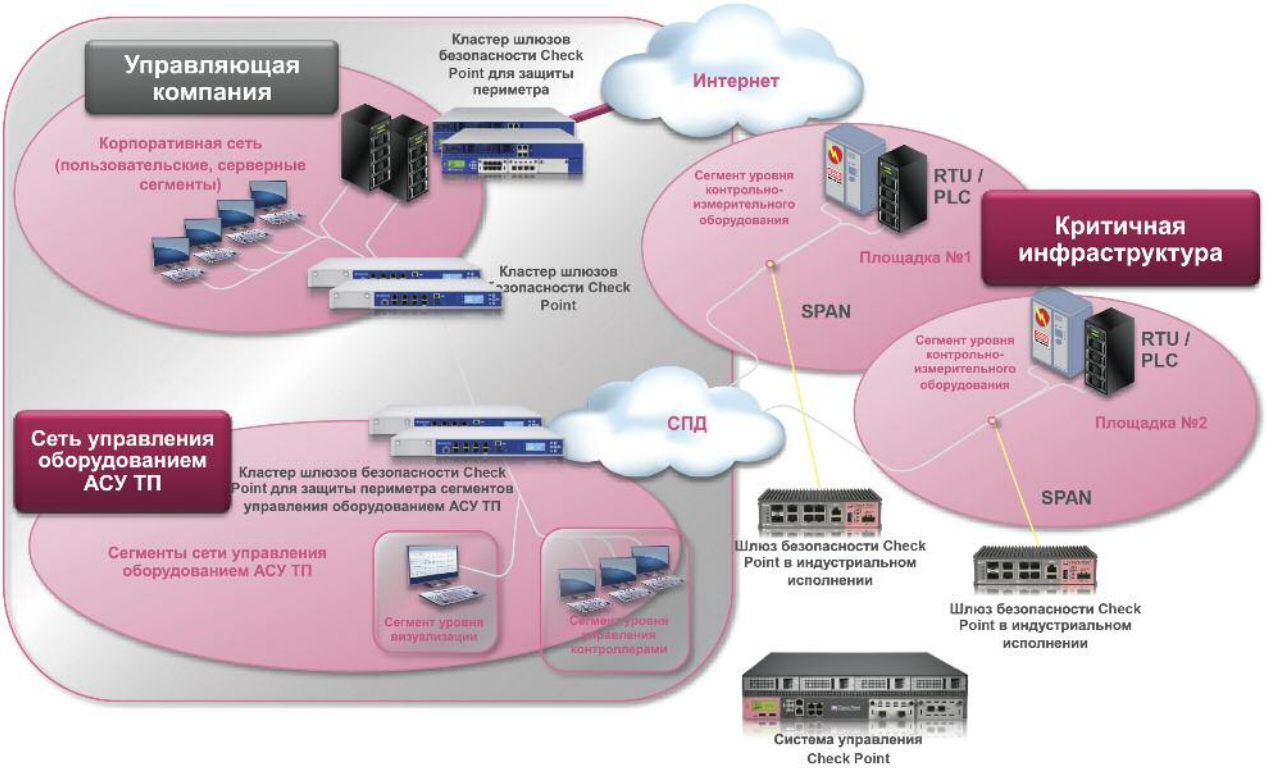
Говоря о современных проблемах, стоящих перед промышленными компаниями, нельзя не упомянуть также и о задачах, связанных с обеспечением соответствия информационных систем требованиям различных регуляторов. Такие требования могут предъявляться как государственными, так и отраслевыми организациями, а также сертификационными органами. Кроме того, существуют регулирующие требования компаний-производителей технологического оборудования, что накладывает дополнительные ограничения на использования тех или иных средств защиты. Соответствие таким требованиям рассматривается предприятиями как одна из важнейших компонент управления рисками и, безусловно, должна оказывать влияние на формирование облика системы ИБ.

При разработке системы защиты АСУ ТП рекомендуется придерживаться системного подхода. Прежде всего должна быть проведена оценка угроз ИБ, проработана архитектура решения, разработана политика безопасности и т.д. Безусловно, при разработке необходимо знать и учитывать специфику работы промышленных систем и особенности работы сетевых протоколов АСУ ТП. Иными словами, неизбежно приходится решать задачу оптимизации со многими ограничениями. Это тем более важно в случае промышленного предприятия, где эффективность функционирования информационной компоненты АСУ ТП влияет на самую сущность бизнеса. Основными факторами, влияющими на решение такой задачи являются:

- необходимость соблюдения параметров производительности системы ИБ как части инфраструктуры АСУ ТП;
- ограничения, связанные со спецификой протоколов АСУ ТП;
- ограничения, связанные с условиями эксплуатации оборудования, особенно в составе критичной инфраструктуры;
- требования регуляторов и производителей решений АСУ ТП;
- необходимость обеспечения гибкости решения с учетом динамики информационных систем (например, появление новых технологий передачи данных, размывание границ системы, связанное с мобильностью сотрудников) и изменения ландшафта угроз.

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





ственным 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 обеспечению безопасности АСУ ТП, являются:

- средства защиты инфраструктуры АСУ ТП, включая решения по ее безопасной сегментации и механизмы построения виртуальных частных сетей (VPN);
- многоуровневая система противодействия современным угрозам;
- система мониторинга и управления ИБ;
- обеспечение соответствия требованиям регуляторов.

Защита инфраструктуры АСУ ТП

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

Говоря об особенностях защиты инфраструктуры АСУ ТП, важно отметить следующие основные факторы, которые необходимо учитывать при ее построении.

Во-первых, в силу длительности эксплуатационного цикла оборудования АСУ ТП и ограничений на обновления его ПО, связанного с сертификационными требованиями производителя, вероятность наличия незакрытых «заплатками» уязвимостей достаточно высока. Это касается как самого ПО, так и протоколов обмена данными. Таким образом, основной фокус в задаче защиты оборудования АСУ ТП смещается в сторону предотвращения несанкционированного доступа к сети АСУ ТП и предотвращения возможного распространения вредоносной активности в случае заражения внутри доверенной сети.

Другой важной задачей является обеспечение надежных и защищенных каналов обмена информацией между объектами АСУ ТП (включая мониторинг оборудования, сбор информации с PLC или RTU, передачу управляющих воздействий и т.п.). Учитывая большое количество объектов и их распределенный характер, необходимо рассматривать применение технологий, позволяющих организовать удаленный защищенный доступ к оборудованию АСУ ТП, таких как виртуальные частные сети (VPN).

И наконец, важным фактором, который необходимо учитывать при планировании, является неблагоприятная среда и режимы работы, в которых будет эксплуатироваться оборудование, обеспечивающее ИБ АСУ ТП. При этом должны быть учтены не только такие факторы, как температура, влажность, воздействие радиации и агрессивные химические среды, но и требования, предъявляемые к надежности и отказоустойчивости оборудования. Это особенно важно в силу того, что надежность системы определяется надежностью самого слабого ее звена и таким звеном не должны оказаться средства ИБ.

АСУ ТП можно логически разделить на три уровня:

- верхний уровень, или уровень визуализации, диспетчеризации и сбора данных;
- средний уровень, или уровень контроллеров;
- нижний уровень, или уровень контрольно-измерительного оборудования.

Рекомендуется для каждого из данных уровней создать отдельные сегменты: сегмент «Уровня визуализации», сегмент «Уровня контроллеров» и сегменты «Уровня контрольно-измерительного оборудования», расположенные на промышленных площадках.

Ниже приведены рекомендации по размещению оборудования системы защиты АСУ ТП.

Для защиты от несанкционированного доступа на границе сегментов АСУ ТП рекомендуется установить следующее оборудование Check Point:

- на границе сегментов «Уровня визуализации» и «Уровня контроллеров» разместить кластер шлюзов безопасности Check Point в отказоустойчивом исполнении;
- на границе сегментов «Уровня контрольно-измерительного оборудования» разместить одиночные шлюзы безопасности Check Point при необходимости, в индустриальном исполнении (для обеспечения непрерывности работы контрольно-измерительного оборудования возможна установка в режиме мониторинга). При необходимости, например, при обнаружении угрозы, шлюз может быть оперативно переведен в режим предотвращения угроз.

Для оптимального планирования политик безопасности должна быть разработана матрица доступа в сегменты критичной инфраструктуры из сегментов «Уровня визуализации» и «Уровня контроллеров», а также из сегментов корпоративной сети в сегмент «Уровня визуализации». Доступ в сегменты критичной инфраструктуры из корпоративной сети должен быть запрещен (или при необходимости максимально ограничен).

Многоуровневая система противодействия современным угрозам

Как было отмечено ранее, угрозы информационной безопасности АСУ ТП включают в себя в основном сложные таргетированные атаки, использующие информацию о специфике работы индустриальных систем и протоколов и направленные на определенные цели в этих системах. Для создания благоприятных условий для атаки злоумышленники часто используют вирусы и другое вредоносное ПО. В связи с этим для обеспечения ИБ промышленных информационных систем недостаточно использовать традиционные межсетевые экраны и системы предотвращения вторжений, которые могут оказаться неэффективными в противодействии таким атакам, особенно, если таковые направлены против специфических протоколов обмена информацией, таких как SCADA.

Компания Check Point рекомендует на всех шлюзах безопасности системы защиты сетей АСУ ТП использовать системы обнаружения вторжений Check Point IPS с поддержкой специализированных протоколов (SCADA),

таких как Modbus, DNP3, ICCP, S7 (Siemens), Control Area networks, Control information protocol, DeviceNet, ControlNet, OPC, Profibus, а на кластере шлюзов безопасности Check Point для защиты периметра сегментов управления оборудованием АСУ ТП, кроме программных модулей **Firewall**, **IPS**, **IPSec VPN** Software Blades (компонентов, отвечающих за межсетевое экранирование, предотвращение вторжений и организацию VPN-взаимодействия), использовать следующие программные модули:

- **Application Control** – модуль, отвечающий за контроль приложений на предмет легитимности, позволяющий осуществлять анализ специализированных протоколов АСУ ТП до уровня команд (более 500 команд). Поддержка дополнительных протоколов осуществляется по запросу;

- **AntiMalware** – модуль, отвечающий за выявление и уничтожение различного рода вредоносных программ;

- **Anti-bot** – модуль, отвечающий за защиту от ботов, обнаруживающий зараженные хосты и предотвращающий взаимодействие бота с командным центром;

- **Identity Awareness** – модуль, позволяющий использовать идентификационную информацию пользователей при создании комплексных политик безопасности.

Специализированные платформы для защиты критичной инфраструктуры

Для удовлетворения специфических требований по защите сегментов сетей критичной инфраструктуры компания Check Point предлагает линейку специализированных устройств для защиты АСУ ТП – шлюзы безопасности Check Point в индустриальном исполнении:

- 1200R - Специализированное решение для применения в промышленных и SCADA сетях;
- IAS U1 - Специализированное устройство Check Point для защиты критичных систем (Smart Grid);
- Интегрированный модуль безопасности в коммутатор Siemens / RuggedCom 1500 Switch.

Все эти устройства, представляющие собой специализированные решения для применения в промышленных и SCADA сетях, предоставляют следующие функциональные возможности:

- поддержка специализированных протоколов в модуле межсетевого экранирования (написание политик с учетом SCADA протоколов) и в модуле предотвращения вторжений IPS:
  - анализ SCADA протоколов с учетом направления коммуникации;
  - обнаружение специализированных эксплоитов, использующих уязвимости SCADA протоколов;
  - для Modbus возможность настройки политики до уровня конкретных команд (например, read/write/get);
  - постоянное совершенствование сигнатур;
  - централизованное обновление в режиме online и offline;
- отсутствие движущихся частей — безвентиляторный дизайн с использованием SSD накопителей и отсутствием внутренних кабельных соединений;
- защита от вибрации;
- гибкие варианты монтажа устройства;
- различные опции по питанию – AC и DC;
- поддержка различных сценариев установки в сеть – L3 «в разрыв», L2 в режиме моста и в режиме зеркалируемого трафика, что позволяет поэтапно внедрять решение от стадии мониторинга до полного контроля проходящего трафика;
- Поддержка следующих протоколов АСУ ТП: Modbus, DNP3, ICCP, UCA 2.0 and IEC 61850 standards, Control Area networks, Control information protocol, DeviceNet, ControlNet, OPC, Profibus.

Устройство Check Point 1200R

Check Point 1200R – это устройство, осуществляющее защиту от угроз следующего поколения (Next Generation Threat Prevention, NGTP) для сверхкритичной инфраструктуры и АСУ ТП. Check Point 1200R позволяет защитить протоколы и оборудование АСУ ТП и включает в себя следующие модули: Firewall, IPS, Application Control, Antivirus и Anti-Bot. Данное устройство работает

в агрессивных средах и соответствует индустриальным стандартам IEEE 1613, IEC 61850-3 по температуре, вибрациям и воздействиям электромагнитного излучения. Высокая производительность (пропускная способность в режиме межсетевого экрана при смешанном трафике 700 Мбит/с и 60 Мбит/с в режиме IPS, пропускная способность VPN 450 Мбит/с) и централизованное управление являются преимуществами простого решения «все в одном».

Наличие USB-портов позволяет администратору подключать совместимые 3G или 4G-модемы сторонних производителей и создавать дополнительные WAN-соединения для резервирования каналов связи для максимальной надежности.

Среднее время наработки на отказ Check Point 1200R составляет около 300,000 часов, а рабочий диапазон по температуре и влажности: от -40 до 75°C, 20%-90%.

Устройство соответствует требованиям IEEE 1613, IEC 61850-3, CE, EN 55024, EN 55022, EN 61000-3, EN 61000-4, CB, IEC 60950 и UL 60950.

Устройство Check Point IAS U1

Представляет собой многофункциональное устройство, обладающее полным функционалом Software Blades – R7X/R77 с производительностью до 3 Гб/с в режиме межсетевого экрана и до 2 Гб/с в режиме IPS (Default IPS profile). IAS U1 имеет встроенные сетевые интерфейсы 2x 10/100/100-BaseT и 4x10/100-BaseT, а наличие 3 слотов расширения для интерфейсных модулей (в том числе волоконно-оптических) позволяет достичь высокой плотности портов для устройства такого класса.

Check Point IAS U1 также имеет 2 интерфейса USB и интерфейсы для подключения консоли, клавиатуры и монитора и полностью интегрируется в систему централизованного мультидоменного управления Smart Center/Multi Domain.

Рабочий диапазон по температуре и влажности: от -20 до 70°C, 20%-95%.

Устройство соответствует требованиям IEEE 1613 и IEC 61850-3.

Интегрированный модуль в коммутатор Siemens/RuggedCom 1500 Switch

Представляет собой решение Check Point R75.40, интегрированное в модуль RuggedApe. Наличие прямого доступа к шине по интерфейсу GigE позволяет обойтись без применения лишних кабелей, а наличие дополнительных интерфейсов (1xGigE и 2xUSB) на внешней панели дает дополнительную гибкость применения.

Рабочий диапазон по температуре и влажности: от -40 до 70°C, 50%-95%.

Устройство соответствует требованиям IEC 61800-3 и EN 61000-6-2.

Построение виртуальных частных сетей

Так как каналы связи с промышленными площадками зачастую проходят по неконтролируемой территории, следует применять шифрование передаваемых данных. Рекомендуется построение сети VPN между кластером шлюзов безопасности Check Point для защиты периметра сегментов управления оборудованием АСУ ТП и шлюзами безопасности Check Point промышленных площадок.

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.

Система мониторинга и управления ИБ

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.

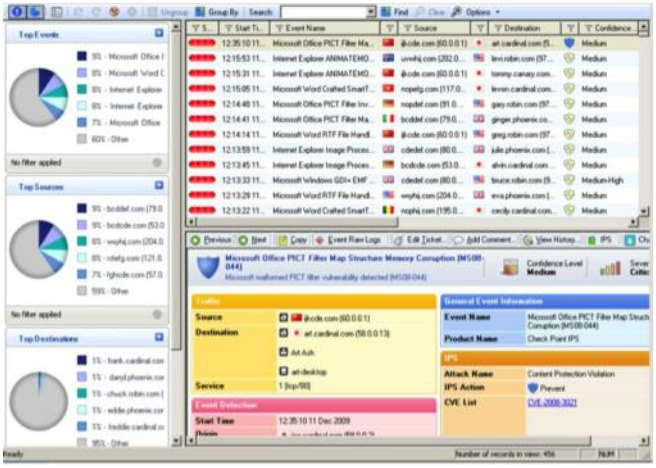
Единая платформа управления Check Point поддерживает распределенные информационные системы и является безопасным инструментом управления, соответствуя стандартам безопасности NERC-CIP (US) и EPCIP (EU). В централизованной системе управления Check Point Security Management администраторы могут создавать политики безопасности для разных объектов – локальной сети, удаленных филиалов, объектов АСУ ТП. С помощью созданного для масштабных сетей и основанного на профилях подхода к управлению SmartProvisioning™ администраторы могут определять единый профиль безопасности и применять его к тысячам устройств, многократно уменьшая время на установку и расходы на обслуживание.

Система управления поддерживает сегментацию предприятия, позволяя администраторам определять политики безопасности для каждого домена безопасности, сохраняя при этом разделение полномочий. 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, дающие организациям возможность 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.

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