SCADAfence

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Техническая документация

Упрощение сегментации сети с платформой SCADAfence

Сложности сегментации сети OT

В не столь отдаленном прошлом жизненно важные системы защищались от внешних угроз в первую очередь через «воздушный зазор», что означало, прерывание связи систем для предотвращения взаимодействия с другими сетями и Интернетом.

Сегодня, в разгар 4-ой индустриальной революции, увеличение возможностей подключения должно, полностью исключив актуальность «воздушного зазора», укрепить предприятия и по-прежнему поддерживать их конкурентоспособность.

Тенденция к увеличению возможностей подключения делает сети OT уязвимыми, подвергая их ряду новых векторов атак. Чтобы снизить эти риски, организации используют технологию межсетевых защитных экранов для реализации сегментации сети.

Реализация процесса сегментации в загруженных внутренних сетях OT отличается от известных методик защиты границ ИТ. Диапазон и сложность подключений значительно выше, и важность производственных процессов значительно больше, чем повседневный офисный трафик, пересекающий корпоративную границу. Это происходит особенно когда развернуто большое количество межсетевых экранов и целью является микро сегментация.

При правильном выполнении сегментация повышает безопасность сети OT, но для того, чтобы сделать эти вложения эффективными еще существуют серьезные проблемы и возможные слабые места, которые необходимо учитывать.

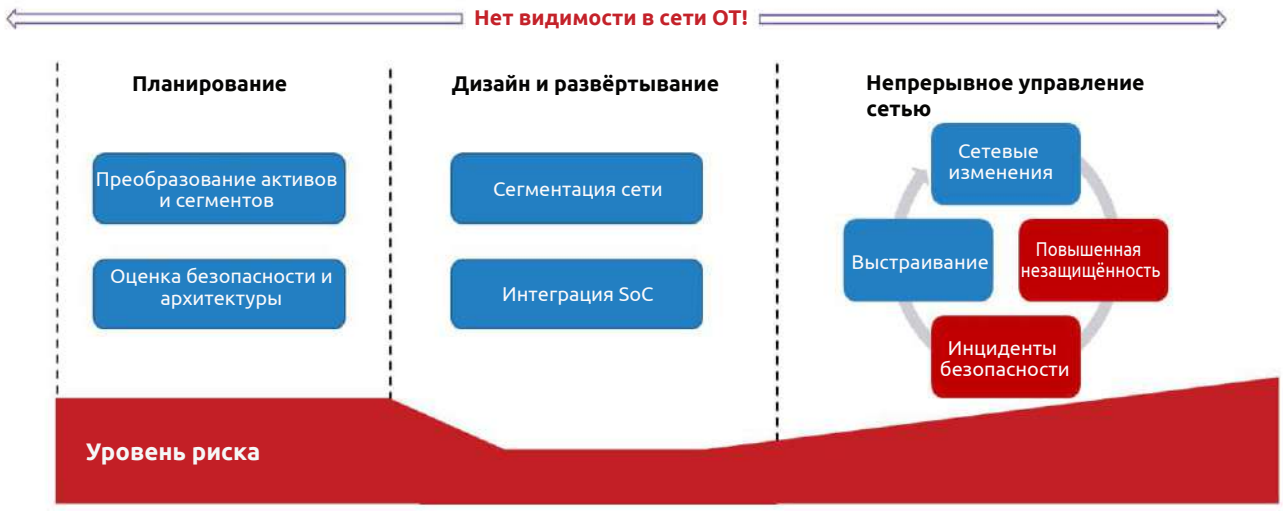

Схема 1: Взаимосвязь между процессом сегментации сети и процессом OT без необходимого уровня прозрачности

Данные сложности в основной массе вызваны недостаточной видимостью сети, зависимостью от мануальных операций и отсутствием взаимосвязи сетевых устройств с запущенными в сети процессами OT.

НЬЮ-ЙОРК,462 W Бродвей Нью-Йорк, NY 10012, США +1-646-475-2173

МЮНХЕН, Schellingstr. 109a80798 Мюнхен, Германия +49-322-2109-7564

ТОКИО, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Токио 103-0023, Япония+81-3-4588-5432

Контакты: info@scadafence.com

Сложности в процессе развёртывания

Высокие риски, связанные с отсутствием видимости. Как правило, проекты сегментации занимают несколько месяцев или даже дольше. Обычно данные проекты включают в себя стадии анализа, планирования и распределения. В это время видимость ОТ сети теряется и не может быть обеспечена надлежащая безопасность. В современной динамичной среде это значит очень долгий срок для возникновения критических событий безопасности.

Неэффективное развёртывание. Поскольку экраны безопасности развернуты во внутренних загруженных сетях, они могут «не видеть» весь опасный трафик. Могут присутствовать удаленные подключения или мошеннические устройства, которые незамеченными обходят межсетевые экраны. Иной раз само местоположение развёртывания выбирается неверно, потому что другая точка пересечения сети может быть гораздо эффективнее. При подобных сценариях у службы безопасности может сложиться ложное чувство безопасности, в то время как требуемый уровень защиты не достигнут.

Отсутствие взаимосвязи с бизнес-процессами. Межсетевые экраны не устанавливают взаимосвязь между видимым IP-адресом и ролями устройства в процессе ОТ. Во внутренних сетях с большим количеством IP и множеством типов трафика приложений это может привести к бесчисленному количеству мануальных (и долгосрочных) манипуляций для понимания шаблонов трафика. Недостаток взаимосвязи подобного рода может привести к непреднамеренной блокировке важных процессов, а с другой стороны, может открыть ненужные порты и создать чрезмерную уязвимость сети. А это делает инвестиции в технологии сегментации неэффективными и в конечном результате создает высокий уровень риска.

Коротко о предоставляемых преимуществах

• Эффективная сегментация путём максимального повышения инвестиционных выгод.

• Предоставляя комплексное решение, охватывает векторные атаки, которые не имеют отношения к дополнениям и межсетевому экрану.

• Тесная связь с операциями ОТ и снижение уровня вмешательств.

• Полная видимость и снижение риска с 1-го дня и способность не создавать слепые зоны в течение длительного времени.

• Осуществляет контроль влияния динамических искажений после этапа развертывания и снижает риск критических событий

• Отслеживает трафик приложений, не сегментированных с помощью межсетевого экрана

НЬЮ-ЙОРК, 462 W Бродвей Нью-Йорк, NY 10012, США +1-646-475-2173

МЮНХЕН, Schellingstr. 109a80798 Мюнхен, Германия +49-322-2109-7564

ТОКИО, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Токио 103-0023, Япония+81-3-4588-5432

Контакты: info@scadafence.com

Сложности после процесса развёртывания

• **Поломки с течением времени.** Со временем сегментация сети «выходит из строя» из-за сетевых изменений, нарушений политики и человеческого фактора. В сеть добавляются новые системы, существующие конфигурации и политики динамично эволюционируют, создавая «пробелы» в политике безопасности.
А это в свою очередь означает, что уровень риска, сниженный проектом сегментации, снова начинает расти с первого же дня после окончания использования межсетевого экрана безопасности.
Если эта ситуация останется незамеченной, то подобное повреждение повлечёт за собой высокий риск серьезных нарушений в системе безопасности.

• **Векторы кибератак.** Зачастую в сетевую инфраструктуру вносятся преднамеренные изменения для того, чтобы обойти безопасность границ. Для сотрудников ИТ и ОТ или внешних провайдеров создаются Бэкдоры, что приводит к новым атакам. Новые подключения из / в Интернет могут устанавливаться бесконтрольно. В качестве примеров векторов атак, угрожающих сети, можно указать внутренних пользователей, USB-устройства, беспроводный доступ, вредоносное заражение через электронную почту.
Для обеспечения безопасности ОТ-сети, они должны контролироваться средствами, отличными от защитных межсетевых экранов.

• **Приложения и системы управления.** На уровне сетевых приложений отображение часто выглядит «плоским». Системы подобные Системе управления производством (СУП) производственные и контроллеры домена, предоставляют доступ ко всем подсетям в организации и не защищаются сегментацией.

Каким образом непрерывный мониторинг и автоматическое обнаружение активов решают проблемы сегментации сети

Платформа SCADAfence обеспечивает непрерывный мониторинг сети и автоматическое обнаружение активов. SCADAfence предлагает дополнительный уровень кибер-защиты, помогающей решить вышеупомянутые проблемы и дополняет архитектуру безопасности.

Схема 2: Эффективная сегментация и долгосрочная безопасность

НЬЮ-ЙОРК,462 W Бродвей Нью-Йорк, NY 10012, США +1-646-475-2173

МЮНХЕН, Schellingstr. 109a80798 Мюнхен, Германия +49-322-2109-7564

ТОКИО, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Токио 103-0023, Япония+81-3-4588-5432

Контакты: info@scadafence.com

Решение проблем во время реализации проекта сегментации

• **Виртуализация трафика между сегментами.** Платформа SCADAfence предоставляет «карту сегментов», отображающую все сегменты сети, и «карту воздействия», демонстрирующую связи между логическими группами и различными сегментами сети. Дополнительная автоматизированная визуализация анализа трафика обеспечивает понимание пользователей модели поведения и требований приложений, а также блокирует недостающий трафик, пересекающий межсетевой экран. Благодаря этому немедленно обнаруживаются все попытки пересечь границу / сеть в трафике.

Одновременно это обеспечивает обнаружение всего сетевого трафика и эффективное выполнение процесса сегментации.

• **Автоматическая инвентаризация активов и ее взаимосвязь с процессом ОТ.** Платформа SCADAfence обнаруживает и отображает все объекты сети, включая роли и действия приложений, с использованием национальных промышленных протоколов. А это гарантирует, что правила сегментации внутренних ОТ-сетей, коммуникационных аспектов и важных промышленных приложений, которыми снабжено большинство сетей, будут более чёткими и эффективными.

• **Отчет об автоматической оценке рисков.** Платформа SCADAfence служит в качестве инструмента, используемого для анализа рисков, выявления важных моделей связи и выявления проблем безопасности. Помогает выявлять уязвимости и слабые места системы безопасности, обеспечивать отображение потенциальных векторов атак и помогает определить требования безопасности на основе реальных данных, а не мануальных исследований. И наконец, администратору сети предоставляется подробный отчет о результатах и рекомендациях по корректировке. Данный отчет даёт гарантию, что процесс сегментации устраняет критические сетевые риски и не игнорирует важные проблемы системы безопасности.

• **Снижение рисков с перового дня -** Контролируя сеть, обеспечивая полную видимость и предупреждения о любых аномальных действиях или отклонениях от политики, платформа SCADAfence гарантирует немедленное снижение риска. Помимо этого, снижение рисков не откладывается на месяцы, пока не станут доступны все механизмы безопасности, что позволяет избежать инцидентов сетевой безопасности.

Поддержание чистоты и безопасности сети после развёртывания:

• **Обнаружение изменений и предотвращение инцидентов безопасности.** Сети являются динамичными структурами: активы добавляются, правила межсетевого экрана безопасности могут изменяться для разрешения небезопасные операций, конфигурируются удаленные подключения. Не всё из этого можно просто обнаружить с помощью технологий сегментации. Платформа SCADAfence обеспечивает четкое представление о безопасности и работоспособности сети и отправляет предупреждающие уведомления о любых изменениях и нарушениях политик.

Выравнивание происходит до того, как произойдет следующее нарушение безопасности, а не после него. За счёт мониторинга снижаются риски кибератак и заражений вредоносным ПО, а также сокращается время, необходимое для обработки потенциальных инцидентов.

• **Устранение бэкдоров и поставщиков атак, прорывающихся через межсетевой экран.** Платформа SCADAfence мгновенно обнаруживает вновь созданные соединения и ресурсы, даже если они не видны через входы сегментации. Это предотвращает проникновение сквозь системы безопасности и другие бэкдоры до того, как это будет сделано злоумышленниками.

НЬЮ-ЙОРК, 462 W Бродвей Нью-Йорк, NY 10012, США +1-646-475-2173

МЮНХЕН, Schellingstr. 109a80798 Мюнхен, Германия +49-322-2109-7564

ТОКИО, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Токио 103-0023, Япония+81-3-4588-5432

Контакты: info@scadafence.com

Обеспечение безопасности несегментированных систем. Поскольку управляющие приложения без упомянутой ранее сегментации являются системами не защищёнными межсетевыми экранами, они постоянно контролируются на предмет аномальной активности.

Как использовать платформу SCADAfence в проекте сетевой сегментации

Платформа SCADAfence используется для планирования проекта сегментации, благодаря чему сокращается время реализации проекта, а следовательно, и его стоимость, и предоставляется более надёжное решение для сегментации.

Выполните следующие шаги для успешной реализации процесса сегментации:

• Подключите систему к сети для обеспечения анализа сетевого трафика. Инвентаризация активов и карты сетевых подключений создадутся автоматически.

• Для того, чтобы увидеть, какие подсети используются в настоящее время, используйте карту топологии подсети. Убедитесь, что вы видите все подсети.

• Для того, чтобы определить трафик между приложениями, операциями ОТ и сайтами, используйте карту подверженности сети атакам и изучите уровень связи между группами.

• Для того, чтобы связать операции ОТ с сетевым трафиком и быстро определить характер взаимодействия, используйте автоматическую инвентаризацию активов (включая автоматически определяемые роли устройств).

• Для того, чтобы выполнить оценку рисков безопасности на основе фактического сетевого трафика, используйте отображения оценки угроз, карту подверженности и отчеты о безопасности.

• Используйте карту подверженности атакам и внутренние предупреждения о подключении к Интернету для обнаружения исходящих подключений. Изучите следующее вопросы:
A. Являются ли эти подключения авторизованными.
B. Пересекают ли соединения точки пересечения границы / межсетевого экрана.
Используйте карты подверженности атакам для определения связи между подсетями. Подсети, не требующие связи между собой, должны быть разделены в рамках проекта сегментации.

• Решите какие подсети должны взаимодействовать между собой. Постарайтесь максимально ограничить возможности подключений, а если вы даёте разрешение на подключение, то ограничьте разрешенное состояние.

• Результат операции используйте как руководство по сегментации.

• По окончанию проекта сегментации используйте этот же способ, чтобы убедиться, что сегментация остаётся успешной, а защита находится на прежнем уровне в течение долгого времени.

• После реализации проекта сегментации используйте системные предупреждения об аномальном трафике, новом устройстве и новом подключении для обнаружения любого ухудшения ситуации с безопасностью и предотвращения инцидентов безопасности.

НЬЮ-ЙОРК, 462 W Бродвей Нью-Йорк, NY 10012, США +1-646-475-2173

МЮНХЕН, Schellingstr. 109a80798 Мюнхен, Германия +49-322-2109-7564

ТОКИО, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Токио 103-0023, Япония+81-3-4588-5432

Контакты: info@scadafence.com

О платформе SCADAfence

Платформа SCADAfence является мировым технологическим лидером в области кибербезопасности OT и IoT (Интернет вещей). Платформа SCADAfence даёт возможность организациям, использующим сложные сети OT, воспользоваться преимуществами промышленных ИТ за счет снижения кибер рисков и устранения операционных угроз. Бесперебойно работающая платформа предлагает лучшую в своем классе точность мониторинга, обнаружение активов и управление с минимальным количеством ложных срабатываний, обеспечивая при этом широкую функциональность для крупных сетей. Удостоенная в 2020 году награды «Cool Vendor» от Gartner, платформа SCADAfence, обеспечивает безопасность и прозрачность самым сложным сетям OT в мире, включая крупнейшее производственное предприятие в Европе. SCADAfence гарантирует безопасность и надёжность организациям, работающим в таких отраслях как критически важные инфраструктуры, производство и управление зданиями. Для получения дополнительной информации посетите www.scadafence.com

НЬЮ-ЙОРК,462 W Бродвей Нью-Йорк, NY 10012, США +1-646-475-2173

МЮНХЕН, Schellingstr. 109a80798 Мюнхен, Германия +49-322-2109-7564

ТОКИО, Clip Nihonbashi, 3-3-3 Nihonbashi-Honcho Chuo-ku, Токио 103-0023, Япония+81-3-4588-5432

Контакты: info@scadafence.com