ВОЛОКОННО-ОПТИЧЕСКИЕ ТРАНСПОРТНЫЕ СЕТИ: обеспечение конфиденциальности и безопасности

С.Коган, к.т.н., советник генерального директора компании "Т8" по формированию технической стратегии / kogan@t8.ru

УДК 004.056.53, DOI: 10.22184/2070-8963.2022.101.1.66.74

Потребность в передаче больших объемов данных между центрами обработки данных (ЦОДами), в обеспечении высокопроизводительных вычислительных процессов и работы критически важных для бизнеса приложений нарастает. Волоконно-оптические транспортные сети, особенно те, которые обеспечивают взаимодействие между несколькими сайтами с ЦОДами, должны поддерживать высокий уровень безопасности. Традиционно угрозы безопасности исходят от вредоносных программ или хакеров-любителей. Их целями чаще всего являются прибыль от продажи интеллектуальной собственности, финансовая информация и даже вымогательство. В статье рассматриваются технологии защиты данных, а также способы обеспечения безопасности волоконно-оптических транспортных сетей.

Защита данных, передаваемых по волоконно-оптической сети

Для защиты от несанкционированного доступа и кражи данных, передаваемых по волоконно-оптическим сетям, требуется набор технологий, позволяющих устранять угрозы безопасности рентабельным и управляемым образом [1]:

- обеспечение контролируемого доступа к сетевым ресурсам. Физическая защита – самый простой подход к защите конфиденциальных данных. Но такую защиту бывает сложно реализовать. Для предотвращения неправомерного использования информации законными пользователями сети, а также внешними хакерами необходимо обеспечить безопасность сетевой инфраструктуры, управляемый доступ к сети и средства контроля доступа привилегированных пользователей. Сетевые администраторы должны развертывать такое сетевое оборудование от поставщиков, в котором предусмотрены методы обеспечения безопасности;
- наличие эффективной системы обнаружения и предотвращения несанкционированного доступа. По сравнению с другими средами передачи оптоволокно считалось более безопасным из-за трудностей подключения к нему и считывания оптических сигналов. Однако известно, что с использованием новых технологий относительно легко осуществить доступ к данным, передаваемым по оптоволокну:

для этого достаточно простых инструментов, которые подключаются к оптическому волокну и улавливают утечку света, не мешая прохождению сетевого трафика. Этот вид несанкционированного доступа сложно обнаружить, его может выполнить любой хакер, имеющий физический доступ к оптоволокну. В таких условиях возрастает потребность в мерах безопасности при транспортировке данных по волоконно-оптическим сетям, то есть для обеспечения гарантии безопасности недостаточно простого владения оптоволоконными ресурсами. В сетевых устройствах должна быть использована встроенная технология мониторинга безопасности, с тем чтобы выявить несанкционированный доступ путем обнаружения, например, необъяснимого снижения уровня мощности оптического сигнала и немедленного предупреждения сетевого администратора о потенциальном нарушении безопасности;

- возможность шифрования передаваемых данных. Средства контроля доступа к сетевым физическим ресурсам помогут защитить от нежелательного перехвата данных, но они не предотвратят все подобные попытки, поэтому их нужно дополнить защитой с использованием шифрования передаваемых по оптическим каналам данных, которое преобразует данные в нечитаемый криптографический текст и в результате украденное становится бесполезным для злоумышленника.

Шифрование данных, передаваемых по волоконно-оптической сети

В настоящее время шифрование передаваемых по сети данных рассматривается как необходимый способ безопасности для все большего числа приложений.

Шифрование при передаче данных по волоконно-оптическим транспортным сетям уже не считается каким-то экзотическим механизмом, использование которого ограничено секретными организациями или военными. Этот обычный инструмент применяется для обеспечения безопасности рабочих процессов в банках, коммунальных службах, финансовых и государственных учреждениях, на транспорте, а также в других организациях, заинтересованных в надежной передаче данных между сайтами.

Шифрование может быть реализовано тремя основными способами:

- шифрование данных на сервере – легко реализуемый способ, который, между тем, предъявляет дополнительные требования к вычислительным ресурсам сервера, выполняющего шифрование. Многие компании шифруют данные в состоянии покоя, а затем перемещают их между ЦОДами в зашифрованном виде. Сложность реализации этого способа связана с отсутствием возможности централизованного управления, поскольку каждый сервер управляется индивидуально;
- шифрование данных с помощью резервного копирования на магнитную ленту – реализовать также нетрудно. Этот способ иногда используется для аварийного восстановления, но он сложен в управлении, требует более высоких, чем ожидалось, затрат. Кроме того, шифрование неактивных данных не поддерживает многопротокольную связь между ЦОДами в реальном времени, которая необходима предприятиям для обеспечения непрерывности бизнеса и защиты постоянно изменяющихся критически важных данных. В этом случае требуются дополнительные вычислительные ресурсы на сервере резервного копирования, который выполняет шифрование, отбирая ценную вычислительную мощность цифрового процессора у других задач. Кроме того, этот способ не защищает данные, передаваемые через сеть общего пользования (PSTN, WAN), поскольку шифрование реализуется локально;
- шифрование передаваемых по сети данных – наиболее эффективный метод предотвращения нарушений безопасности. Криптографические алгоритмы считаются "сильными" не потому, что их невозможно взломать математически, а потому, что они реализуемы с вычислительной точки зрения. Чем больше времени необходимо затратить для расшифровки сообщения без знания ключа, тем выше надежность алгоритма. Если злоумышленнику требуются годы для расшифровки закодированного сообщения, взламывать код не имеет смысла – информация, скорее всего, утратит актуальность и устареет.

Анализ преимуществ и недостатков разных способов шифрования данных, передаваемых по оптической транспортной сети, представлен на рис.1 [3].

Шифрование передаваемых по оптической транспортной сети данных на более высоких уровнях сетевого стека OSI может быть эффективным в определенных ситуациях, однако подобная процедура обычно оказывается более сложной и дорогой, что приводит к большой загрузке цифровых процессоров (CPU), увеличению задержки и размеров заголовков в передаваемых на более низких уровнях потоках данных.

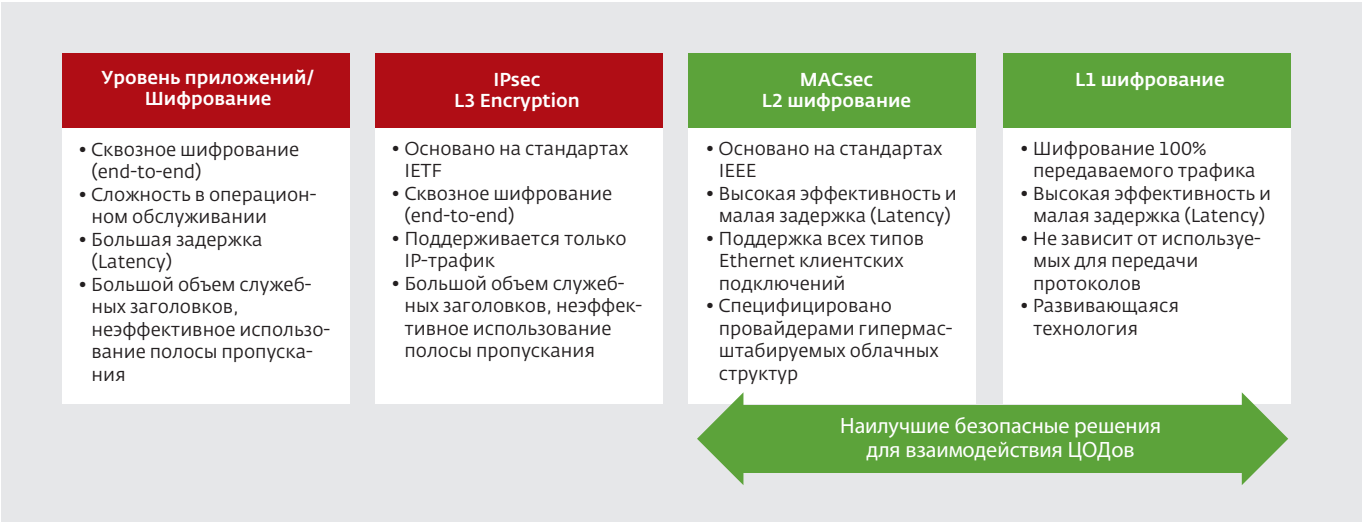

Рис.1. Анализ преимуществ и недостатков разных способов шифрования данных, передаваемых по волоконно-оптической сети

Кроме того, могут возникнуть проблемы с совместимостью сетевых уровней OSI. Более низкие уровни OSI модели более предпочтительны для шифрования данных, которое становится проще в реализации. Следует учитывать, что шифрование на самом нижнем из возможных уровней OSI защищает также информацию на вышележащих уровнях.

Реализация эффективного шифрования и управления ключами шифрования данных, передаваемых на уровне L1/OTN сети OTN/DWDM, является важным компонентом общей стратегии многоуровневой защиты критически важных бизнес-данных и обеспечивает снижение затрат на постоянное управление безопасностью на сетях взаимодействия между ЦОДами.

Основные преимущества уровня L1/OTN (МСЭ G.709) заключаются в следующем [4]:

- сокращение затрат на транспортировку данных. Благодаря возможности передачи нескольких клиентов на одной длине волны технология OTN/DWDM предоставляет экономичный механизм заполнения оптических каналов (длин волн) систем с разделением каналов по длине волны оптического излучения (WDM) сервисными потоками;
- эффективное использование пропускной способности и гибкость сетевых решений. Стандарты OTN обеспечивают эффективное использование пропускной способности и поддерживают высокую скорость передачи данных по каждому оптическому каналу на сетях DWDM, оснащенных во многих случаях многосвязными гибкими средствами кросс-коммутации и ввода/вывода оптических каналов на фотонном уровне (например, в узлах ROADM), а также кросс-коммутации и ввода/вывода каналов OTN на электрическом уровне (например, в узлах с централизованной матрицей OTN кросс-коммутации);
- детерминизм. Стандарты OTN позволяют выделять настраиваемую скорость передачи для каждой услуги, их группы или сегмента сети. Каждому клиентскому сервисному потоку гарантируется определенная пропускная способность соединения (скорость передачи, задержка, низкочастотные и высокочастотные дрожания, надежность), а также отсутствие конфликтов между одновременно предоставляемыми услугами или пользователями;
- виртуализация сетевых операций. Благодаря разбивке сети с OTN-коммутацией на частные сетевые сегменты, клиент получает выделенный набор сетевых ресурсов, не зависящий от остальной сети. При использовании функционала сегментирования сети (Slicing) каждый арендатор сети имеет доступ только к тем выделенным ему ресурсам, которые связаны с его частным сегментом, и не имеет доступа к ресурсам, относящимся к другим арендаторам;
- гибкость. Сети OTN/DWDM предоставляют операторам возможность использовать технологии, необходимые для удовлетворения требований к передаче данных, а также новые технологии (например, новые клиентские сигналы и соединения), удовлетворяя запросы бизнеса;

- безопасная модель. Сети OTN обеспечивают высокий уровень конфиденциальности и безопасности путем жесткой сегментации трафика по выделенным цепям. Такое разделение сетевого трафика затрудняет перехват данных, передаваемых между узлами по каналам, структурированным в соответствии с OTN рекомендациями МСЭ-Т (например, G.709). Поскольку сети с кросс-коммутацией OTN разделяют все приложения и арендаторов, то благодаря функциональности Slicing арендаторы могут эффективно противостоять атакам хакеров, получивших доступ к одному сегменту сети, предотвращая их доступ к другим сегментам;
- надежность и простота операций. Административные данные сети OTN/DWDM передаются по отдельному каналу (например, по оптическому сервисному каналу на отдельной длине волны за пределами полосы группового сигнала DWDM), который изолирован от каналов, по которым передаются данные пользовательских приложений. Через интерфейсный порт клиента значительно сложнее получить доступ к настройкам сети OTN.

Обеспечение безопасности при взаимодействии между ЦОДами

Многие угрозы безопасности для ЦОДов являются внутренними и исходят от законных пользователей, зачастую и сотрудники ведут себя ненадлежащим образом. Внутренняя угроза не ограничивается взломом сетевых устройств. Можно, например, подвергать оптическое волокно изгибу до тех пор, пока оно не начнет пропускать свет. Утекающие из кабеля световые импульсы можно обнаружить оптическим фотодетектором, закрепленным вокруг оптического волокна, не мешая при этом передаваемому по оптическому кабелю сетевому трафику. Такая сложно обнаруживаемая атака по силам любому человеку, имеющему физический доступ к корпоративным помещениям.

По мере увеличения объемов трафика, передаваемого при подключении к ЦОДам предприятий, потребность в эффективных способах защиты передачи критически важных данных нарастает. Для обеспечения безопасности ЦОДов, включающих несколько сайтов, технических средств противодействия, например, антивирусных программ и сетевых экранов (firewalls), используемых внутри центра обработки данных, может оказаться недостаточно. Понадобится систематический и целостный подход, предусматривающий комплексную и скоординированную контратаку.

Для обеспечения безопасности взаимодействия ЦОДов применяются следующие три способа противодействия угрозам кражи информации [2]:

- предотвращение – обеспечение безопасности сетевой инфраструктуры. Для профилактики неправомерного применения информации законными пользователями центра обработки данных и/или внешними хакерами следует обеспечить не только управляемый доступ к сети, но и средства контроля доступа привилегированных пользователей. Администраторы ЦОДов должны иметь в виду, что в полученном от поставщиков и развернутом на сети оборудовании должно быть предусмотрено не только использование методов безопасности, но и возможность управления ими;
- обнаружение – в сетевых устройствах должна быть предусмотрена встроенная технология мониторинга безопасности, с тем чтобы обнаруживать несанкционированное подключение к сети, даже если обмен трафиком, проходящим через сеть взаимодействия между ЦОДами, не нарушается. Имеется в виду возможность обнаружения несанкционированного подключения злоумышленников к оптическому волокну и немедленного предупреждения администратора о потенциальных или уже состоявшихся нарушениях безопасности;
- подавление – наиболее эффективный метод устранения нарушений безопасности – шифрование данных. В этом случае украденные данные становятся бесполезными для злоумышленника.

Обеспечение безопасности на сети общего пользования

Защита данных, передаваемых по сети общего пользования (PSTN, WAN), обеспечивается путем их шифрования на физическом уровне в реальном времени. Корпоративные пользователи могут создавать между собой безопасные, масштабируемые, высокопроизводительные соединения в пределах частного облачного сетевого образования на основе зашифрованных каналов L1/OTN, организуемых по оптоволокну с использованием технологии DWDM. Шифрование каналов уровня L1/OTN на волоконно-оптической транспортной сети гарантирует, что весь трафик, проходящий по сети, зашифрован, поскольку обеспечивается совместная, конвергентная передача трафика LAN (Local Area Network), SAN (Storage Area Network) и HPC (High-Performance Computing) поверх единой физической волоконно-оптической среды и значительно упрощается управление безопасной сетевой

инфраструктурой. Нормативные требования соблюдаются даже в том случае, если устаревшие приложения более высокого уровня не должны быть выведены из эксплуатации в течение нескольких лет.

Применительно к системам обмена данными между ЦОДами с каналами со сверхмалой задержкой и высокой пропускной способностью обеспечивается их шифрование с поддержкой всех протоколов и приложений более высоких уровней OSI (Open Systems Interconnection), зеркалирования данных, возможности изменения местоположения виртуальных машин VM (Virtual Machine) и виртуализации средств хранения данных.

Особенности шифрования данных, передаваемых по транспортной сети:

- осуществляется с помощью специального оптического транспортного оборудования, выполняющего шифрование в реальном времени на скорости передачи данных между удаленными узлами;
- не требует от серверов выделения дополнительных вычислительных ресурсов;
- поддерживает централизованное управление, необходимое для контроля и управления устройствами шифрования.

Выбор метода шифрования и управление ключами шифрования данных

Волоконно-оптические транспортные системы могут быть защищены от киберугроз за счет:

- надежного шифрования данных и правильного выбора ключей шифрования. Основой шифрования на уровне L1/OTN в международной практике является использование алгоритма (шифра) AES-256 (Advanced Encryption Standard). В AES (Advanced Encryption Standard) предусмотрен симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм широко используется и может быть реализован на аппаратном и программном уровнях. Предполагается, что AES-256 останется актуальным в течение десятилетий. Однако шифр AES-256 нужно дополнять надежными и качественными ключами. Взаимодействие и управление ключами планируются таким образом, чтобы избежать снижения эффективности системы [5].

  В Российской Федерации в качестве стандарта рекомендована технология, представленная в ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования". Это блочный шифр с 256-битным ключом и 32 циклами (называемыми раундами) преобразования, в котором использованы 64-битные блоки данных.

  В 2015 году алгоритмы шифрования "Кузнечик" и "Магма", упомянутые в ГОСТ 28147-89, были опубликованы как часть ГОСТ Р 34.12-2015 "Криптографическая защита информации. Блочные шифры (19.06.2015)" и ГОСТ Р 34.13-2015 "Криптографическая защита информации. Режимы работы блочных шифров (19.06.2015)". В 2020 году алгоритм "Магма" был опубликован в виде RFC 8891 GOST R 34.12-2015 (Block Cipher Magma, September 2020). При использовании алгоритма "Магма" длина шифруемого блока составляет 64 бита, а длина ключа шифрования – 256 бит. Подлежащий зашифровыванию блок данных длиной 64 бита разделяется на два равных сегмента по 32 бита каждый – правый и левый. Далее выполняется тридцать две итерации с использованием итерационных ключей, получаемых из исходного 256-битного ключа шифрования [6];
- устойчивого дизайна сети, включающего в себя надежную конструкцию оборудования, наличие резервирования, а также возможности по локализации и устранению неисправностей. Высокая надежность систем очень важна для обеспечения безопасности сетевых решений;
- независимой сертификации. Органы по стандартизации, такие как National Institute of Standards and Technology (NIST, USA), Common Criteria и др., разработали методы подтверждения безопасности сети. Федеральная служба безопасности Российской Федерации предоставляет государственную услугу по сертификации средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации в помещениях и технических средствах, а также технических средств обеспечения безопасности и (или) защиты информации. Меры по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена определены Указом Президента РФ № 351 от 17 марта 2008 года. Сертификация независимым органом означает для конечного пользователя то, что подход к безопасности проверен и заслуживает доверия.

Для обеспечения передачи зашифрованных данных требуется правильное управление ключами шифрования. Неправильное управление ключами шифрования может лишить авторизованных клиентов доступа к системе или вызвать прерывание трафика между ЦОДами, что, в свою очередь, оказывает влияние на работу критически важных бизнес-приложений предприятия. По этой причине администраторам центров обработки данных требуется безопасное зашифрованное решение для сетей взаимодействия ЦОДов с комплексным управлением соответствующими ключами шифрования на протяжении всего их жизненного цикла.

Устойчивость ключа должна соответствовать стойкости шифра. Каждый подход к сетевой безопасности будет настолько эффективен, насколько силен более слабый из этих двух элементов. Признано, что для обеспечения защиты от атак при наличии квантовых компьютеров требуется не менее чем 192-битный ключ.

Алгоритмы с симметричным шифрованием, такие как AES-256, используют двустороннюю функцию передачи и генератор случайных чисел для создания ключа. Эта стратегия проста в вычислительном отношении и результативна, поскольку угадывание ключа усложняется. При асимметричном алгоритме ключи шифрования вычисляются с использованием односторонней передачи, что требует больших вычислительных ресурсов и более сложного программного обеспечения. Результаты сравнения эффективности симметричного и асимметричного алгоритмов шифрования отражены на рис.2 [7].

Использование централизованного управления ключами имеет ряд преимуществ:

- лучшее шифрование и масштабирование. Ключи создаются централизованно и безопасно отправляются для шифрования и дешифрования. В этом случае освобождаются ресурсы цифрового процессора, можно использовать более надежные и сложные ключи;
- единая точка доверия. Ключи находятся в ограниченном количестве мест, что снижает угрозу доступа к ключам;
- адекватное применение политик. Администраторы легко применяют стандарты и политики по всей сети;
- оптимизированное администрирование. Обновления выполняются один раз и передаются по всей сети, что позволяет обеспечить принудительную многопользовательскую синхронизированную ротацию ключей;

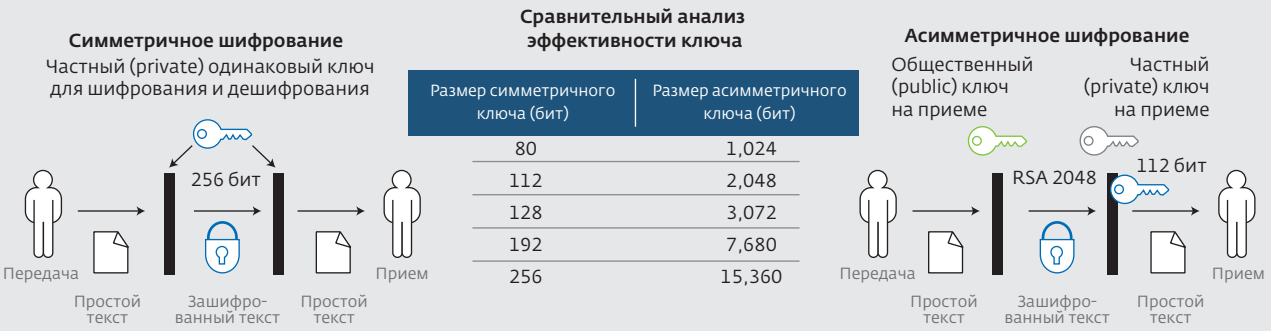

Рис.2. Сравнение эффективности симметричного и асимметричного алгоритмов шифрования

- единый аудит и исправление. Аудит сетевой безопасности и соблюдение политик упрощаются за счет ведения журналов аудита, содержащих все действия, связанные с ключами. Анализ журналов позволяет проводить профилактические работы.

Пример обеспечения безопасности на волоконно-оптической транспортной сети

Ниже представлен пример мер по обеспечению безопасности на волоконно-оптических транспортных сетях OTN/DWDM [8].

1. Конфигурации сети для работы в безопасном режиме:
   - открываются только основные логические и физические порты, необходимые для управления системой;
   - функции отладки программного обеспечения отключаются;
   - сервисы встроенной операционной системы отключаются, запрещается любой интерактивный доступ к операционной системе;
   - используются и поддерживаются только безопасные протоколы управления сетевыми элементами, например простой протокол управления сетью SNMPv3.
2. Аутентификация и авторизация пользователя:
   - механизм авторизации контроля доступа обеспечивает совместимое разделение обязанностей между управлением сетевыми элементами и предоставлением услуг (соединений) с шифрованием (криптографической обработкой);
   - криптографические функции реализованы в транспондерах/мукспондерах с функцией шифрования полезной нагрузки оптических каналов (активизируются при необходимости);
   - криптографические функции реализованы в используемом протоколе управления SNMPv3, который сертифицирован на предмет удовлетворения требований FIPS 140-2 level 2;
   - процедуры и технические аспекты реализуются согласно положениям ISO 15408, которые должны соблюдаться на всем жизненном цикле сетевого оборудования, включая процессы документирования, соответствия методологии безопасной разработки программного обеспечения, а также тестирования и выпуска продукта.
3. Обеспечение безопасности при подключении системы централизованного управления сетью:
   - использование физического интерфейса с функцией шифрования для подключения интерфейса SNMPv3, обеспечивающего взаимодействие сетевых элементов с централизованной системой управления сетью. Доступ к функциям управления возможен только после того, как пользователь успешно идентифицирован, аутентифицирован и авторизован в соответствии с его ролью;
   - конфигурирование и активизация интерфейса системы управления (SNMPv3), аутентификация его параметров и других установок, связанных с безопасностью;
   - начальная настройка ключей для интерфейса управления SNMPv3;
   - для уменьшения угрозы атак отключаются (блокируются):
     - доступ для других интерфейсов системы централизованной системы управления;

26–28 АПРЕЛЯ 2022

ПРИ ПОДДЕРЖКЕ ПРАВИТЕЛЬСТВА САНКТ-ПЕТЕРБУРГА

ЖКХ РОССИИ

XVIII МЕЖДУНАРОДНАЯ ВЫСТАВКА

- ЭНЕРГО- И РЕСУРСОСБЕРЕГАЮЩИЕ ТЕХНОЛОГИИ
- ЭКСПЛУАТАЦИЯ ЖИЛИЩНОГО ФОНДА. КАПИТАЛЬНЫЙ И ТЕКУЩИЙ РЕМОНТ
- СИСТЕМЫ КОММУНИКАЦИИ, БЕЗОПАСНОСТИ И КОНТРОЛЯ
- ВНУТРИДОМОВЫЕ ИНЖЕНЕРНЫЕ СИСТЕМЫ
- АВТОМАТИЗАЦИЯ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. УСЛУГИ ДЛЯ ЖКХ.
- БЛАГОУСТРОЙСТВО ГОРОДСКИХ И ПРИДОМОВЫХ ТЕРРИТОРИЙ
- СОВРЕМЕННЫЕ СТРОИТЕЛЬНЫЕ МАТЕРИАЛЫ, ТЕХНОЛОГИИ И ОБОРУДОВАНИЕ
- КОММУНАЛЬНАЯ ТЕХНИКА
- РЕСТАВРАЦИЯ И СОХРАНЕНИЕ ОБЪЕКТОВ КУЛЬТУРНОГО НАСЛЕДИЯ
- ВОДОСНАБЖЕНИЕ, ВОДООТВЕДЕНИЕ, ПОДГОТОВКА И ОЧИСТКА ВОДЫ

ВЫСТАВОЧНАЯ ПРОГРАММА | КОНГРЕССНАЯ ПРОГРАММА | ОРГАНИЗАЦИЯ ДЕЛОВЫХ ВСТРЕЧ

КОНГРЕССНО-ВЫСТАВОЧНЫЙ ЦЕНТР
EXPOFORUM
РОССИЯ, САНКТ-ПЕТЕРБУРГ, ПЕТЕРБУРГСКОЕ ШОССЕ, 64/1

тел./факс: +7 (812) 240 40 40 (доб. 2172, 2161)
gkh@expoforum.ru, GKH.EXPOFORUM.RU

6+

- функция отладки программного обеспечения и связанные с этой функциональностью базовые сервисы встроенной операционной системы;
- в процессе настройки и ввода системы в эксплуатацию пользователям могут быть назначены разные роли. Они могут применяться для обеспечения доступа к сетевым элементам через систему централизованного управления сетью.

3. Защита от несанкционированного доступа к оптическим каналам:
   - наличие встроенной функциональности, которая позволяет измерять уровень оптической мощности в контрольных точках и идентифицировать оптические каналы (длины волн) в контрольных точках по маршруту прохождения тракта (канала) по волоконно-оптической сети;
   - использование дополнительных точек измерения уровня оптической мощности для автоматического обнаружения несанкционированного доступа к волоконно-оптической сети. Если уровень оптической мощности между двумя последовательными измерениями в точке контроля значительно отличается (например, уровень оптической мощности сигнала ниже относительно номинального значения), то формируется сигнал аварии, чтобы предупредить оператора о риске потенциального несанкционированного доступа. При отсутствии такой функциональности несанкционированный доступ на фотонном уровне сети, приводящий к ослаблению уровня оптической мощности сигнала на несколько дБ, может остаться незамеченным оператором и/или пользователями, поскольку сеть и услуги могут продолжать функционировать без проблем и предоставлять качественные сервисы (соединения).

Заключение

Задачи по обеспечению безопасности передачи данных по волоконно-оптическим транспортным сетям OTN/DWDM необходимо решать на всех этапах жизненного цикла и уровнях обслуживания сетевой инфраструктуры – от развертывания и конфигурирования сети для обеспечения ее работы в "безопасном режиме" до выполнения соответствующих требований при подключении системы централизованного управления сетью, от аутентификации и авторизации пользователей до защиты от несанкционированного доступа к оптическим каналам (длинам волн) фотонного уровня DWDM и к соединениям на уровне электронной OTN кросс-коммутации каналов. Эти задачи особенно актуальны на фоне развития перспективных сетей мобильной связи 5G и особого внимания, которое уделяется безопасности функционирования волоконно-оптических транспортных сетей и взаимодействия между ЦОДами [9].

ЛИТЕРАТУРА

1. Secure optical transport with the 1830 Photonic Service Switch, WPNOKIA, 2017. https://onestore.nokia.com/asset/194463/?_ga=2.138203632.1750884051.1630610354-730815896.1614834341&_gac=1.188960345.1629996919.CjwKCAjw95yJBhAgEiwAmRrutLq2akjG-60J5Abd0N 6ARSKYrvnZ8diJ0_ATu1qn5zlbisi3v_aVEYhoCaxUQAvD_BwE
2. Data Center Connect Security. A comprehensive approach to preventing, detecting and mitigating data security risks. Strategic White Paper, Alcatel-Lucent / NOKIA, 2012.
3. Security Strategies for Data Center Interconnect, LightWave, 2017. https://www.lightwaveonline.com/data-center/data-center-interconnectivity/article/16673869/security-strategies-for-data-center-interconnect
4. Ciena. Оптическая транспортная сеть. Руководство эксперта по оптическим транспортным сетям, 2014. https://media.ciena.com/documents/Ciena+Experts+Guide+to+OTN_ru_RU.pdf
5. NOKIA Secure Optical Transport: Not All Solutions Are Equal. March 20, 2017. https://www.lightwaveonline.com/business/earnings-statements/article/16673373/secure-optical-transport-not-all-solutions-are-equal
6. Русская "Магма". Как работает отечественный алгоритм блочного шифрования, 2019. https://xakep.ru/2018/05/10/working-with-magma/
7. Secure optical transport brochure, NOKIA. https://onestore.nokia.com/asset/200776?_ga=2.104331968.1750884051.1630610354-730815896.1614834341&_gac=1.153158474.1629996919.CjwKCAjw95yJBhAgEiwAmRrutLq2akjG60J5Abd0N 6ARSKYrvnZ8diJ0_ATu1qn5zlbisi3v_aVEYhoCaxUQAvD_BwE
8. NOKIA Security Target Nokia 1830 Photonic Service Switch, 2017. anssi-cible-cc-2017_58en.pdf); BEST PRACTICES RESEARCH. Aggregation Router (SAR), 1830 Photonic Service Switch (PSS), 9500 Microwave (pdfslide.net)
9. NOKIA 5G Security Risks and Mitigation Measures. WP. 2021. Whitepaper-5G-security-Nokia-STC-March-31-2021.pdf

26–28 АПРЕЛЯ 2022

КЛЮЧЕВАЯ ПЛОЩАДКА СФЕРЫ ТЭК

РОССИЙСКИЙ МЕЖДУНАРОДНЫЙ

РМЭФ

ЭНЕРГЕТИЧЕСКИЙ ФОРУМ

XXIX МЕЖДУНАРОДНАЯ ВЫСТАВКА

ЭНЕРГЕТИКА И ЭЛЕКТРОТЕХНИКА

18+

КОНГРЕССНО-ВЫСТАВОЧНЫЙ ЦЕНТР
ЭКСПОФОРУМ
САНКТ-ПЕТЕРБУРГ, ПЕТЕРБУРГСКОЕ ШОССЕ, 64/1

ENERGYFORUM.RU
rief@expoforum.ru
+7 (812) 240 40 40, доб.2626

EXPOFORUM

ENERGETIKA-RESTEC.RU
energo@restec.ru
+7 (812) 303 88 68

РЕСТЭК®
выставочное объединение