



АНАЛИЗ СЕТЕВЫХ ОБЛАЧНЫХ СИСТЕМ СЕРТИФИКАЦИИ CISCO

Чебыкин Андрей Михайлович

студент, ФГБОУ ВО Кубанский государственный аграрный университет имени И.Т. Трубилина, РФ, г. Краснодар

Сергеев Александр Эдуардович

научный руководитель, канд. физ.-мат. наук ФГБОУ ВО Кубанский государственный аграрный университет имени И.Т. Трубилина, РФ, г. Краснодар

Аннотация. В статье рассматривается процесс анализа основных концепций облачных систем сертификации в сетевых устройствах Cisco.

Cisco запускает платформу Cloud Controls в открытом доступе, которая внедряет сертификацию безопасности на устройствах Cisco. Новые технологии позволяют предоставить широкой группе людей удобное и безопасное обеспечение компаний сертификатами.

Сертификат - электронный документ, который идентифицирует физическое или юридическое лицо, сервер или другую организацию и связывает эту организацию с открытым ключом. Самозаверяющий сертификат подписывается его создателем. Сертификаты могут быть самозаверяющими или подписанными цифровой подписью внешним центром сертификации. Цифровой сертификат, подписанный центром сертификации, считается отраслевым стандартом и более безопасным, чем самозаверяющий сертификат.

Сертификаты используются в сети для обеспечения безопасного доступа. Сертификаты идентифицируют узел Cisco ISE с конечной точкой и обеспечивают связь между этой конечной точкой и узлом Cisco ISE.

Сама технология называется Cisco Cloud Controls Framework, которая внедрена в новые сетевые устройства и может быть поставлена с обновлениями системы на текущие уже эксплуатируемые платформы. Cloud Controls Framework помогает экономить значительные ресурсы, позволяя организациям гораздо эффективнее получать сертификаты облачной безопасности. Cisco Cloud Controls Framework предлагает подход «build-once-use-many» для получения самого широкого спектра международных и национальных сертификатов облачной безопасности, таких как SOC 2, ISO и FedRAMP.

Cloud Controls Framework представляет собой всеобъемлющий набор международных и национальных стандартов к соблюдению требований безопасности и сертификации, объединенных в одну структуру. Это позволяет администраторам убедиться, что облачные продукты и сервисы соответствуют требованиям безопасности и конфиденциальности благодаря упрощенной рационализированной стратегии соответствия требованиям и управления рисками, что позволяет сэкономить значительные ресурсы.

Удовлетворение быстро меняющихся требований к сертификациям и стандартам безопасности по всему миру становится все более важным, но также и чрезвычайно сложным, требующим больших ресурсов и времени для поставщиков облачного программного обеспечения.

Cloud Controls Framework содержит руководство по внедрению средств контроля и артефакты аудита, необходимые для демонстрации операционной эффективности средств контроля.

Компании, получающие услуги SaaS стараются обеспечить безопасность, доступность и конфиденциальность для своих клиентов. В то время как получение глобальных сертификатов безопасности стало для многих важным условием ведения бизнеса, данная технология является отличной возможностью реализации сертификатов. Многие организации с трудом поспевают за этим ресурсоемким и трудоемким процессом.

По мере роста сложности рыночного спроса поставщики SaaS нуждаются в эффективном способе упрощения и оптимизации усилий по получению сертификатов безопасности. Они ищут методы и инструменты, которые помогут им начать свой путь к облачному соответствию требованиям и расширить доступ к глобальному рынку. Стратегический подход к соблюдению требований и управлению рисками так же важен для успеха организации, как и ее продуктовая стратегия.

Cisco Cloud Controls Framework V1.0 охватывает рамки соответствия требованиям безопасности и стандарты сертификации.

Наряду с элементами управления безопасностью мы также предоставляем "описания", руководства для пользователей, чтобы они понимали, как внедрять необходимые средства контроля, и "артефакты аудита", которые включают примеры того, что аудиторы обычно запрашивают при тестировании операционной эффективности средств контроля. Соответствующие описания фреймворка и вспомогательные артефакты аудита дают вам рекомендации по обзору, оценке и адаптации в соответствии с вашими потребностями, одновременно интегрируя Cisco CCF в режим соответствия требованиям вашей организации.

Спрос компаний на глобальные сертификаты безопасности SaaS постоянно растет, как и риски безопасности, с которыми сталкиваются технологические компании и компании интернет-услуг.

Cisco Cloud Application Centric Infrastructure автоматизирует управление сквозным подключением, а также применение согласованных политик безопасности для приложений, работающих в локальных центрах обработки данных и на гибридных облачных системах.

Cisco Cloud ACI - комплексное решение, которое использует возможности сетевого подключения гибридных облачных систем для предоставления клиентам упрощенных операций, согласованной сетевой политики и видимости в нескольких локальных центрах обработки данных и облаке гибридных облачных систем.

С помощью этого решения клиенты могут распространить свои сетевые политики Cisco Cloud ACI на гибридных облачных системах. Чтобы устранить основные риски по обеспечению безопасности, организации внедряют решение для автоматизации управления безопасностью и реагирования сбора данных об операциях безопасности, создают обоснования для обнаружения изменений конфигурации безопасности и организуют пользовательские разрешения рабочего процесса для их проверки.

Это обеспечивает необходимую видимость для активного сетевого мониторинга и возможность исправления результатов.

Прежде чем переносить данные или рабочие нагрузки в облако, облачные и технологические команды могут рассмотреть следующие средства управления облачной безопасностью в своих приложениях, сетях, рабочих нагрузках и инфраструктуре:

- защита рабочей нагрузки. Когда элементы управления устанавливают базовые ограничения и минимальные конфигурации для защиты развертывания;
- сегментация, разграничение доступов внутри определенных локальных сегментов сети организации;
- управление нарушениями доступов извне. Эти средства управления регулируют ландшафт уязвимостей с помощью специализированных сервисов для повышения устойчивости к уязвимостям и атакам программ внутри сети. Организации могут сосредоточиться на выявлении и оценке облачных активов на протяжении всего их жизненного цикла и на разных уровнях архитектуры.

Такой подход к миграции в облако, основанный на обеспечении безопасности, может помочь повысить устойчивость и целостность технологий для компаний и их клиентов.