УДК 004.7

Аленченко В.В.,
студент магистратуры
2 курс, факультет «Отдел магистратуры»
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара
Плетеный Д.С.,
студент магистратуры
2 курс, факультет «Отдел магистратуры»
Поволжский государственный университет телекоммуникаций и информатики
Россия, г. Самара
Научный руководитель: Трошин Александр Викторович

СЕТИ УПРАВЛЯЕМЫЕ НА ОСНОВЕ НАМЕРЕНИЙ (IDN)

Аннотация: *в статье рассматривается способ внедрения в цифровую среду и бизнес процессы, сетей управляемых на основе намерений.*

Ключевые слова: *автоматизация, намерения, искусственный интеллект, активно, внедрение, метод, устранение, доступ, архитектура, сеть.*

Annotation: *the article discusses the method of introducing intentionally managed networks into the digital environment and business processes.*

Key words: *automation, intentions, artificial intelligence, active, method, implementation, elimination, access, architecture, network.*

Концепция IDN

Зачастую из-за отсутствия комплексных механизмов автоматизации управление конфигурацией традиционных сетей требует затрат огромного количества времени и ресурсов, что в условиях динамично развивающейся

цифровой среды заметно тормозит не только внедрение новых технологий, но и бизнес-процессы. Решить эти проблемы способны сети, управляемые на основе намерений, или Intent-Driven Networking (IDN). Эта технологическая концепция помогает компаниям сменить пассивную систему технического обслуживания на активную — то есть перейти от сети, зависящей от квалификации специалистов, к автоматизированной сети на базе искусственного интеллекта.

Внедрение намерений

Работу с сетями на основе намерений можно сравнить с управлением беспилотным автомобилем, когда все, что вам нужно для прибытия в определенный пункт, — это ввести место назначения. Точно так же, используя это новое технологическое решение, сетевому администратору нужно только описать в бизнес-терминах задачи и KPI для сети, а также пропустить это описание через искусственный интеллект, а остальное сеть сделает сама.

Используя искусственный интеллект, анализ больших данных и облачные технологии, IDN может в секунды или минуты выполнять задачи, на которые раньше целая армии IT-специалистов тратила часы и дни: в зависимости от заданных бизнес-намерений сеть автоматически конфигурирует все устройства и выполняет необходимые подключения, производит непрерывный мониторинг процессов с автоматической перенастройкой в соответствии с указанными параметрами, моментально реагирует на изменившиеся потребности компании, эффективно находит и устраняет неполадки, обнаруживает и изолирует угрозы, а еще она постоянно обучается.

Ключевые принципы IDN

Одна из главных особенностей IDN — это предиктивный анализ, благодаря которому сеть самостоятельно прогнозирует сбои и ошибки и заранее оптимизирует процессы, чтобы предотвратить их. Полная автоматизация жизненного цикла сетевых сервисов и упрощение сети с точки зрения архитектуры, протоколов, базовых станций и технического обслуживания позволяет компаниям сократить операционные расходы на 80%. IDN-решения

поддерживают широкополосную связь — это обеспечивает массовый доступ, низкое значение задержки и высокую пропускную способность. Открытый интерфейс прикладного программирования делает возможным подключение сети к сторонним платформам на базе больших данных и облачных вычислений. Наконец, IDN-решения способны сократить среднее время обнаружения угроз безопасности и реагирования на них на 90% вне зависимости от их источника, а технология искусственного интеллекта автоматически выявляет любые аномалии и принимает активные меры по быстрой защите сети.

IDN-решениями от Huawei уже успели воспользоваться несколько игроков глобального рынка, часть из которых входит в Топ-20 по версии рейтинга Forbes Global 2000. Если до недавних пор при возникновении сбоев головной офис компаний вынужден был направлять специалистов в один из тысяч филиалов для их решения, то IDN-решения позволили устранять эти проблемы дистанционно и в кратчайшие сроки.

Пока число компаний в мире, которые используют сети, управляемые на основе намерений, еще немного, ведь сама технология совсем молода. Но, судя по уже имеющимся результатам и потенциальным возможностям можно без преувеличения сказать, что за этим решением будущее корпоративных сетей. Компании, использующие IDN и другие технологии, основанные этих принципах, смогут моментально адаптировать свои сети к меняющимся потребностям бизнеса, обеспечивая высокое качество обслуживания клиентов, повышая операционную эффективность, эффективно внедряя новые технологии и объединяя тем самым цифровой и физический мир

В качестве итогового тезиса вышеприведённых двух пунктов данной главы, хотелось бы сформулировать, что IBN может стать важнейшим этапом эволюции сетевых технологий. Его основное назначение - помощь компаниям в оптимизации эксплуатации сетей и повышение их доступности. Конечно, переход на новую технологию потребует некоторые время, но ожидания того, что концепция IBN постепенно придет на смену традиционному подходу – вполне рациональны.

Вывод

Важными аспектами активного поиска угроз являются выяснение путей их проникновения в сети предприятий и принятие мер по предотвращению атак в будущем. Важно выявлять уязвимости внутри инфраструктуры предприятия. Правильно выполненная кампания по активному поиску угроз может выявить неправильно сконфигурированный сервер или нарушение политики безопасности, которое в обязательном порядке необходимо устранить. Иногда хорошо выполненные мероприятия активного поиска угроз могут не выявлять уязвимости. Однако это будет значить то, что для организации в ближайшем будущем нет повода волноваться за сохранность конфиденциальных данных.

Использованные источники:

1. Романов, С.В. Маршрутизация в беспроводных самоорганизующихся сетях. Иерархические и гибридные протоколы: / Прозоров Д.Е., Трубин И.С., Лесников В.А., Жолобов А.Н., Романов С.В. – Киров: ПРИП ФГБОУ ВПО «ВятГУ», 2013. — 100 с.
2. Threat Hunting Report [Электронный ресурс]. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/pdfs/cybersecurity-series-2019-threat-hunting-ru.pdf
3. Блог Cisco в России и СНГ [Электронный ресурс]. URL: https://gblogs.cisco.com/ru/
4. Васильев, Д.С. Протоколы маршрутизации в MANET / Д.С. Васильев, А.В. Абилов // Электросвязь. — 2014. — № 11. — С. 52–54.
5. Калашников С.К. История «болезней» VPN // Журнал сетевых решений, 2013. - № 11.