Сеть на основе намерения

Устранение разрыва между бизнесом и ИТ

Введение

Сети находятся в центре неминуемого эволюционного перехода к цифровой экономике. Цифровизация полностью меняет принципы взаимодействия бизнеса с партнерами, сотрудниками и потребителями. Продукты и услуги могут быть кастомизированы, заказаны и отправлены из веб-приложения буквально одним нажатием кнопки. Бизнес-данные собираются, анализируются и передаются практически в реальном времени. Географические границы между компаниями и потребителями размываются. А сеть находится в центре коммуникаций, которые обеспечивают работу приложений, формирующих основу цифровой экономики.

Однако традиционным архитектурам корпоративных сетей и центров обработки данных сложно адаптироваться к требованиям этой динамично развивающейся среды. Приложения перемещаются в общедоступные, частные и гибридные облачные среды и используются по подписке, что размывает границу между непроверенными доменами и сетью предприятия. Благодаря все более широкому использованию программного обеспечения с открытым исходным кодом, контейнеров, микросервисов и процессов разработки agile период от создания концепции до запуска рабочего приложения теперь занимает не месяцы или годы, а считаные дни. Для сотрудников и заказчиков доступ к сети и информации независимо от места, устройства или времени становится чем-то неотъемлемым. И по мере того как Интернет вещей расширяется, к сети подключается все больше датчиков и автономных устройств. В то же время киберугрозы становятся все более сложными для обнаружения и опасными для репутации и финансового благополучия организаций.

Традиционные корпоративные архитектуры сетей и центров обработки данных и операционные процедуры должны развиваться, чтобы соответствовать этим тенденциям. В частности, новая сеть должна:

- поддерживать реализацию инициатив цифрового бизнеса, а не сдерживать их; обладать гибкостью и быстро адаптироваться к меняющимся бизнес-целям;
- быть простой в настройке, эксплуатации и обслуживании независимо от масштаба и сложности (используемые в настоящее время операционные модели не являются масштабируемыми или устойчивыми);
- осуществлять всесторонний мониторинг своей работы, обеспечивать поддержку текущих бизнес-инициатив и соблюдение нормативных требований, выявлять неполадки и рекомендовать меры по их исправлению;
- выявлять и нейтрализовать угрозы безопасности, прежде чем они причинят вред. Мультиоблачные среды, Интернет вещей и широкое использование мобильных устройств создают новые векторы угроз, от которых в сети должна быть предусмотрена надежная и непрерывная защита.

Содержание

Такая ситуация в ИТ-индустрии вызывает растущий интерес к интеллектуальным сетям, которые называют сетями на основе намерения.

Управляемые на основе намерения сети меняют наше представление о проектировании, разработке и эксплуатации сетевых сред. Ранее не существовало инструментов, с помощью которых можно было объявить намерение и преобразовать его в отвечающую поставленным целям конфигурацию на уровне устройства. Для достижения желаемого результата проектировщикам или администраторам сети приходилось настраивать конфигурации отдельных элементов сети. Например: «необходимо, чтобы эти серверы были доступны из этих филиалов, то есть нужно настроить подсеть VLAN и правила безопасности на каждом сетевом устройстве».

Сетевые решения на основе намерения позволяют заменить обычные методы, которые требуют конфигурирования отдельных элементов сети вручную, на обобщенную настройку на основе политики с использованием контроллеров. Таким образом администраторы получают возможность легко «выразить намерение» (желаемый результат) и впоследствии убедиться, что сеть делает именно то, что от нее требуется.

Требования цифровой трансформации в отношении масштаба, гибкости и безопасности сетей предполагают, что поэлементная настройка сети должна быть заменена автоматизированным общесистемным программированием сетевых элементов с применением последовательных политик на основе намерения. Кроме того, непрерывный контекстуальный анализ данных до, во время и после развертывания гарантирует, что сеть выполняет поставленные перед ней задачи и надежно защищена. Непрерывный сбор телеметрии и других видов данных, поступающих из множества различных источников, обеспечивает широкий информационный контекст, позволяющий оптимизировать работу системы и защитить ее.

Возможности политики на основе намерений выходят за рамки управления доступом клиентских устройств или приложений. Они позволяют предоставить пользователям требуемый уровень обслуживания, выставить приоритеты для приложений и определить цепочку сетевых служб, которые должны быть применены к потоку приложений, или даже операционные правила для соглашений об уровне обслуживания, например: «я хочу, чтобы на моих сетевых устройствах были развернуты только золотые образы».

«По мнению Gartner, способность систем управляемой на основе намерения сети повышать адаптивность и доступность сети и применять политики на базе единой цели в нескольких инфраструктурах несет в себе множество преимуществ».

Gartner, 2017 г.

Аналитика инноваций от Gartner: «Сети, основанные на намерении», Эндрю Лернер, Джо Скорупа, Санджин Гангули, 7 февраля 2017 г.

По мнению Cisco, полнофункциональная сеть на основе намерения (рис. 1) должна выполнять следующие основные функции.

- **Перевод.** Функция перевода характеризует намерение. Она позволяет администраторам сети гибко выражать намерение в декларативной форме. Другими словами, задача функции перевода – передать, **какое** поведение сети будет оптимальным для достижения бизнес-целей, а не **как** сетевые элементы должны быть настроены для достижения этого результата.
- **Активация.** Полученное намерение затем необходимо интерпретировать в политики, которые могут быть применены к сети. Функция активации внедряет эти политики в физическую и виртуальную сетевую инфраструктуру с помощью общесетевой автоматизации.
- **Контроль.** Чтобы удостовериться в том, что выраженное намерение реализуется в сети на постоянной основе, функция контроля выполняет непрерывный цикл проверки и верификации. Чтобы проверить соответствие операции намерению, используются контекстные данные, полученные посредством телеметрии.

Рис. 1. Функции сети на основе намерения

В настоящем документе излагается точка зрения Cisco на эволюцию сетевых технологий, в результате которой появилась сеть на основе намерения, описывается архитектура такой сети и ее преимущества для сетевых инженеров и архитекторов. В документе содержится обзор основных функциональных блоков сети на основе намерения и приводятся конкретные примеры для центра обработки данных и корпоративной сети.

Намерение. Устранение разрыва между бизнесом и ИТ

Сегодня настройка работы ИТ-системы в соответствии с требованиями бизнеса требует множества усилий и выполняемых вручную действий. В большинстве случаев процесс является очень ресурсоемким, длительным и часто приводит к ошибкам. Он не отвечает критериям гибкой цифровой бизнес-среды, которая объединяет в себе все большее число систем, устройств, приложений и служб.

Сеть на основе намерения воспринимает задачи бизнеса, переданные в форме бизнес-требований, и переводит их в ИТ-политики, применение которых постоянно контролируется по всей сети. На рис. 2 приведены примеры, демонстрирующие разницу между намерением («что») и реализацией («как»).

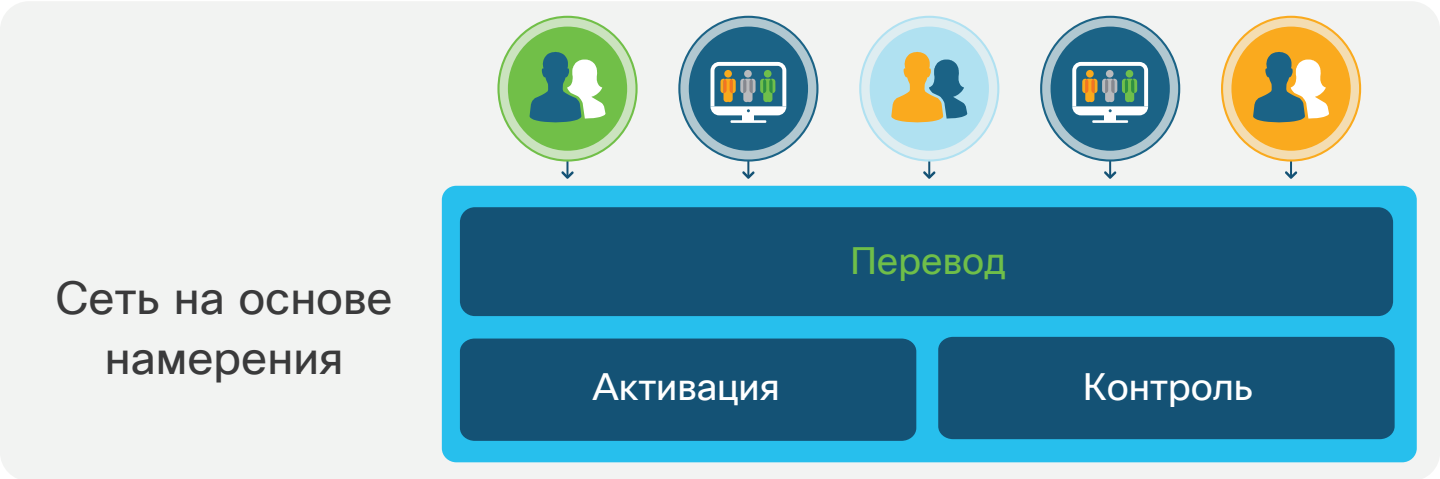
Рис. 2. Примеры выражения намерения

В сети на основе намерения администратор говорит «что делать», а система определяет «как». – Зевс Керравала

Функциональные блоки корпоративной сети на основе намерения

Сеть на основе намерения строится на трех основных функциональных блоках (рис. 3): восприятие выраженного намерения, автоматизация развертывания выраженного намерения по всей сетевой инфраструктуре и контроль за реализацией выраженного намерения.

Рис. 3. Функциональные блоки управляемых на основе намерения сетей



Перевод

В модели сетей на основе намерения задача перевода включает в себя несколько функций. Один или несколько администраторов или их группа могут охарактеризовать свое намерение. Намерение может быть передано через удобный графический пользовательский интерфейс, абстрактную модель (например, YANG или JSON/XML), которая интуитивно понятна и связана с бизнес-целями, или даже определенный синтаксис или язык. Намерение может определяться разработчиками приложений как часть непрерывного процесса интеграции/доставки (CI/CD). А в будущем даже, вероятно, сможет передаваться посредством речевого воспроизведения текста, когда администратор устно выражает намерение и система на основе намерения выполняет указания и предоставляет устную или другую обратную связь. Подход, основанный на намерении, отличается от традиционных сетевых архитектур именно этими обобщенными указаниями, передаваемыми сети в форме бизнес-требований.

Другая функция перевода заключается в переработке намерения в общую политику на основе модели (MBP), часто с помощью архитектуры на основе контроллера. Намерение, выраженное посредством различных инструментов ввода, которые могут находиться в разных сетевых доменах, переводится в такие стандартные политики MBP. Это является основой автоматизации сети и применения комплексных проверок на согласованность и целостность.

Серьезной задачей является переход от традиционной сети к сети, управляемой на основе намерения. В этом случае в существующей сети уже есть действующие политики. Но оператор сети может не иметь всей необходимой информации о развернутых в настоящее время политиках. Поэтому необходимо выполнить автоматическое обнаружение хостов и политик и определить действующие политики, чтобы предоставить администратору полную информацию. После этого выбранные администратором политики автоматически развертываются в управляемой на основе намерения сети.

Активация

Функции активации обеспечивают применение производных политик MBP в соответствующих сетевых доменах. В управляемой на основе намерения сети физические и виртуальные сетевые функции в различных операционных доменах (центр обработки данных, WAN, филиалы, комплексы зданий) могут контролироваться одной или несколькими группами администраторов. Функция оркестрации сети на основе намерения позволяет применять политики MBP в релевантных доменах. Это означает, что действие политики может быть ограничено определенной частью сети.

В блоке активации также могут использоваться дополнительные функции для выполнения дальнейшей настройки устройств. Для создания соответствующей конфигурации устройства контроллер домена может соотносить информацию об элементах сети, их функциях и топологии с правилами применяемой политики MBP. До программирования сетевых элементов могут использоваться дополнительные проверки на согласованность на уровне конфигурации на основе стандартных API (например, сетевого протокола конфигурации [NETCONF], YANG или передачи состояния представления [REST]).

Контроль

В сети на основе намерения контроль является важнейшей функцией. Сеть постоянно отслеживает, достигаются ли требуемые результаты, используя контекстуальный анализ данных для проверки того, что намерение действительно реализуется. Функция контроля в сети на основе намерения включает в себя три основных компонента, которые также приведены на рис. 4.

- **Отслеживание поведения системы управляемой на основе намерения сети до, во время и после развертывания.** Проверка реализации выраженного намерения в сети на постоянной основе. Это требует постоянного наблюдения за статусом сетевых элементов и событий. С помощью телеметрии на основе намерения измеряется степень реализации выраженного намерения. Эти данные собираются и непрерывно передаются блоку функций контроля управляемой на основе намерения сети. Алгоритмы контроля, начиная с формальных математических моделей и заканчивая методами, основанными на телеметрии и машинном обучении, гарантируют, что состояние и поведение сети соответствуют выраженному намерению как на уровне доменов, так и на междоменном уровне.
- **Получение аналитических выводов (корреляция событий и использование машинного обучения и искусственного интеллекта [ML/AI]) для проверки, изучения и прогнозирования работы сети.** В дополнение к проверке текущего состояния сети и его соответствия выраженному намерению функции контроля выполняют более глубокий анализ поведения сети на основе намерения. Например, они могут предсказать нарушения в реализации выраженного намерения до внесения планируемых изменений, определить или спрогнозировать тенденции, выявить аномалии, предсказать и проверить производительность сети на системном уровне.
- **Использование замкнутого цикла для реализации мер по корректировке и оптимизации работы сети.** Обнаруженные аномалии, нарушения и несоблюдение соглашения об уровне обслуживания (при выраженном намерении) могут быть программно исправлены в масштабе всей системы через обращение к функциональному блоку активации. Таким образом, в сети на основе намерения применяется механизм автоматизации для исправления любого нарушения политики на основе намерения и для непрерывной оптимизации, гарантирующей реализацию выраженного намерения в любой момент времени. Обратите внимание, что в зависимости от политики меры могут приниматься автоматически или сообщаться администратору в виде рекомендаций. В последнем случае решение об их исполнении принимает администратор.

Рис. 4. Три основных компонента блока контроля

Основные различия в архитектуре, функциональных блоках и результатах между традиционной сетью и сетью на основе намерения приведены в таблице 1 ниже.

Таблица 1. Сравнение традиционных сетей и сетей на основе намерения

Возможности	Традиционная сеть	Сеть на основе намерения
Архитектура	▪ Управление на уровне устройств ▪ Однонаправленная конфигурация ▪ Непрограммируемые устройства ▪ Фрагментарная безопасность сети	▪ Централизованное управление всей сетью ▪ Автоматическая конфигурация замкнутого цикла и контроль ▪ Программируемые физические и виртуализированные инфраструктуры ▪ Встроенные функции обеспечения безопасности по всей архитектуре ▪ API-ориентированная, на основе модели ▪ Открытый стек программного и аппаратного обеспечения
Перевод	▪ Интерпретация и перевод, требующие от администратора специальных знаний	▪ Да, с помощью системных функций восприятия и перевода намерения
Верификация намерения	▪ Не поддерживается	▪ Да, проверки на целостность и согласованность
Поддержка политик	▪ Ограниченная, политики реализуются через команды устройств	▪ Политики на основе намерений с использованием моделей
Активация	▪ Ограниченная (сценарии), на уровне устройств	▪ Автоматизированная, в масштабе всей сети с использованием контроллеров
Телеметрия	▪ Ограниченная поддержка	▪ Всесторонняя поддержка
Контроль	▪ Ручной, на уровне устройств	▪ Автоматизированный, полная аналитика с использованием AI/ML или формальных методов
Цикл обратной связи	▪ На основе ручного контроля администратором	▪ Да, автоматизированные меры, запускаемые администратором или блоком системной активации
Результаты	▪ Несмотря на приложение максимума усилий для выполнения требований бизнеса, результат ограниченный ▪ Сложная система, рост которой ведет к увеличению затрат на управление	▪ Непрерывный контроль за работой сети в соответствии с бизнес-целями ▪ Упрощенное, эффективное управление в масштабе

Сеть на основе намерения в мультидоменных средах

Управление сетевой инфраструктурой предприятия может осуществляться в разных доменах – операционные задачи могут различаться в комплексе зданий и филиалах, WAN, центре обработки данных и облаке. Приложения, размещенные в центре обработки данных или облаке, а также клиентские устройства могут иметь свои собственные операционные процедуры и рассматриваться как домены. Предполагается, что в сети на основе намерения один или несколько доменов управляются контроллером, который обеспечивает целостное представление инфраструктуры и поддерживает согласованное состояние сети (конфигураций, образов ПО и т. д.).

В системах на основе намерения сетевая инфраструктура представляется в виде доменов. Перевод и оркестрация применяются к доменам, позволяя определять параметры общесетевой политики на основе намерений в комплексе зданий и филиалах, WAN, центре обработки данных и облаке. Функция оркестрации позволяет внедрить полученные политики в соответствующие домены, а также ограничить применение некоторых политик при проектировании. Задача автоматического перевода политик на основе модели в конфигурации для конкретных устройств и создания их экземпляров в сетевой инфраструктуре выполняется доменными контроллерами. Для обеспечения соблюдения политики на основе выраженного намерения функции контроля управляемой на основе намерения сети могут применяться к определенному домену. Кроме того, функции контроля работают на междоменном уровне, проверяя соответствие результата выраженному намерению в масштабе всей сети (от приложения к приложению, независимо от того, где они размещены).

На рис. 5 показаны дополнительные функциональные элементы блоков перевода, активации и контроля управляемой на основе намерения сети и их связь с различными доменами инфраструктуры. Рисунок также иллюстрирует цикл обратной связи, через который аналитические данные, собранные блоком контроля, отправляются обратно в блок активации в целях постоянной оптимизации работы сети.

Рис. 5. Модель сети на основе намерения и функциональные элементы

Преимущества сети на основе намерения

Сети на основе намерения гарантируют ряд преимуществ для руководителей компаний и ИТ-отделов. В частности, это увеличение возможностей бизнеса и эксплуатационной эффективности, соблюдение нормативных требований и обеспечение безопасности на высоком уровне, непрерывный контроль за работой ИТ-инфраструктуры в соответствии с бизнес-целями и снижение рисков.

Увеличение возможностей бизнеса

Абстрагирование, полностью автоматизированный характер управляемой на основе намерения сети и поддержка открытых API-интерфейсов гарантируют, что сеть в состоянии реагировать на динамическую среду цифровой экономики. Новые приложения можно быстро развернуть в нужном месте сети (центре обработки данных предприятия, виртуальном частном облаке (VPC)) или даже использовать по модели «как услуга». Возможность системы на основе намерения абстрактно понимать намерение нового приложения упрощает процесс развертывания такого приложения и его защиту. Комплексные проверки на целостность, автоматическая конфигурация сетевых политик для приложений и постоянный контроль за работой сети позволяют сетевым специалистам разрабатывать приложения в сжатые сроки.

Повышенная эксплуатационная эффективность

Функциональные возможности управляемой на основе намерения сети открывают перспективы повышения эксплуатационной эффективности и сокращения операционных расходов. Предполагается, что проектирование сетей, ввод в эксплуатацию, тестирование и устранение неполадок будут происходить гораздо быстрее. Сеть на основе намерения предлагает полную поддержку моделей: администраторы сети могут просто выразить намерение, которое будет легко переведено в политики на основе модели. После превращения намерения в модель могут использоваться комплексные проверки на согласованность и целостность для подтверждения того, что новое намерение согласуется с ранее выраженным или что намерения, выраженные различными группами администраторов, не противоречат друг другу. Перевод политик на основе модели в стандартные конфигурации сетевых элементов может выполняться полностью автоматически, что способствует согласованной работе сети. Таким образом управляемая на основе намерения сеть предполагает значительное упрощение традиционного процесса ручного конфигурирования, когда определение политики для каждого сетевого элемента архитектуры выполняется с помощью интерфейса командной строки (CLI). Обычно этот ручной процесс повторялся каждый раз, когда к сети подключалось новое приложение или устройство. Он также должен был обеспечить проверку любых изменений конфигурации, чтобы не происходило нарушений правил предыдущих политик.

Благодаря механизмам абстрагирования и автоматизации модель на основе намерения также поддерживает масштабируемость цифровой сетевой архитектуры. В частности, намерения и политики обычно определяются на уровне группы. Упрощение операционной модели достигается благодаря группировке приложений, устройств и пользователей и выражению намерения для связанных с ними групп. По мере приема на работу новых сотрудников или распространения приложений новые оконечные устройства могут создаваться в рамках существующих групп, и в них будут применяться ранее выраженное намерение и политики. Кроме того, эффективность стандартизированных и автоматизированных процессов управляемой на основе намерения сети изначально выше, чем традиционных, выполняемых вручную процессов.

Благодаря модели замкнутого цикла сеть на основе намерения также значительно упрощает сценарии устранения неполадок, которые во многих сетях бывают очень сложными. Поскольку процессы контроля постоянно проверяют соответствие конфигурации сети намерению, они могут выявить потенциальные проблемы еще до их возникновения, а также быстро и эффективно определить их причину.

При этом стандартные модификации для устранения часто повторяющихся проблем могут быть автоматизированы с сохранением интеграции с системами управления ИТ-услугами (ITSM), что потенциально означает существенную экономию эксплуатационных расходов. Управляемая на основе намерения сеть может трансформировать административную базу знаний (обычно она используется службой технической поддержки или является базой данных для управления конфигурациями) в системную базу знаний или базу знаний на основе машинного обучения, в которой предварительно одобренные изменения становятся основой автоматизации с замкнутым циклом.

Согласованность работы сети с бизнес-целями

Системы на основе намерений позволяют программировать работу сети через обобщенные указания, передаваемые сети в форме бизнес-требований: **что делать** вместо **как**. Это гарантирует, что работа сети всегда соответствует бизнес-операциям. Ранее перевод бизнес-целей в конфигурации устройств являлся процессом, выполняемым высококвалифицированным специалистом. Например, бизнес-цель «работа приложения X критически важна для бизнеса» требовала фильтрации трафика приложения X, настройки политики качества обслуживания (QoS) на всех соответствующих участках сети и, соответственно, глубоких знаний о каждом сетевом элементе. В управляемой на основе намерения сети то же самое выраженное намерение переводится в политику и настройка сетевых элементов выполняется полностью автоматически. Встроенный в управляемую на основе намерения сеть механизм обратной связи проверяет, выполняются ли переведенные из намерения политики, и, если сеть отклоняется от реализации выраженного намерения, автоматически настраивает конфигурацию сети.

Улучшенное соблюдение нормативных требований и обеспечение безопасности

Улучшенные решения в области безопасности и быстрое сдерживание угроз — важнейшие преимущества сетей на основе намерения. Каждый функциональный блок управляемой на основе намерения сети помогает значительно повысить общий уровень безопасности и соблюдение нормативных требований. Основной задачей управляемой на основе намерений сети должен быть непрерывный контроль за намерениями, связанными с политиками безопасности и соблюдением нормативных требований. Эта задача выполняется путем встраивания решений безопасности в каждый функциональный участок управляемой на основе намерения сети и строгого контроля за соблюдением политик и сдерживания угроз. Политики безопасности могут назначаться группой по обеспечению безопасности операций независимо от других административных групп. Функциональные проверки на целостность позволяют убедиться, что политики не противоречат друг другу. Благодаря непрерывной телеметрии и функции контроля всегда доступна актуальная картина состояния сети, что имеет важное значение для обеспечения безопасности и составления отчетов о соответствии нормативным требованиям. Передовые методы сегментации поддерживают доступность основных активов и предотвращают горизонтальное распространение вирусов между оконечными устройствами, пользователями и приложениями.

Снижение рисков

Абстрагирование, автоматизация и контроль управляемых на основе намерения сетей открывают возможности снижения общих операционных рисков при предоставлении связи пользователям и приложениям или при подключении устройств. В системе на основе намерений ручные процессы с использованием интерфейса командной строки (CLI), которые часто приводят к ошибкам, сводятся к минимуму. Рассмотрим, например, фильтрацию трафика в сети. Обычно для фильтрации трафика в масштабе всей сети как в целях контроля трафика (гарантированная полоса пропускания, определение пути), так и в целях безопасности используются списки контроля доступа (ACL). Со временем списки ACL растут, и внесение в них каких-либо изменений увеличивает риск создания уязвимости в системе безопасности или нарушения предыдущих политик. Используемые в управляемой на основе намерения сети прогнозируемые и последовательные политики на основе намерений, проверки на целостность и согласованность (например, с помощью формальных математических методов) и стандартизированный перевод намерения в конфигурации сетевых элементов повышают согласованность работы сети, даже когда сетью управляют несколько групп администраторов и в ней используются самые разные технологии.

Кроме того, благодаря прогнозированию воздействия модификаций на состояние сети в рамках всей системы в сетях на основе намерения значительно снижается риск возникновения перебоев в их работе. Рассмотрим ситуацию, при которой основной сегмент функционирует нормально, а дополнительный сегмент, используемый только в случаях аварийного восстановления, — нет. Система управляемой на основе намерения сети сможет определить такие скрытые нерабочие конфигурации и уведомить о них администратора (или исправить их автоматически), что позволяет избежать возможных перебоев в работе сети.

«Мы считаем, что внедрение полнофункциональной, управляемой на основе намерения сети позволит компаниям разворачивать сетевую инфраструктуру на 50–90 % быстрее. При этом количество простоев и их продолжительность сократится по меньшей мере на 50 %».

Gartner, 2017 г.

Аналитика инноваций от Gartner: «Сети, основанные на намерении», Эндрю Лернер, Джо Скорупа, Санджин Гангули, 7 февраля 2017 г.

Переход на сеть на основе намерения

Для многих организаций переход на сеть на основе намерения потребует внедрения новых технологий и внесения изменений в существующие процессы. Весь потенциал управляемой на основе намерения сети проявляется при ее развертывании во всех сетевых доменах, включая центр обработки данных, комплекс зданий, филиал и WAN.

Различные ИТ-разработчики занимаются реализацией возможностей сетей на основе намерения. Поэтому многие функциональные блоки модели на основе намерения уже доступны и обеспечивают значительные преимущества своим пользователям. В рамках долгосрочной стратегии развития системы на основе намерения многие фундаментальные элементы, включая программно-определяемые сети, инструменты виртуализации и аналитики, могут быть развернуты уже сегодня. Внедрение управляемой на основе намерения сети может быть значительно упрощено и ускорено путем использования автоматического обнаружения хостов и политик в текущей сети организации с последующим предоставлением информации о них администратору. После анализа имеющихся политик выбранные политики активируются в управляемой на основе намерения сети.

Cisco помогает ИТ-компаниям внедрить полнофункциональную сеть на основе намерения. Для построения сети используются открытые платформы Cisco для центров обработки данных и корпоративных сетей, а также технологии других поставщиков, участвующих в экосистеме Cisco.

В центрах обработки данных ориентированная на приложения архитектура Cisco® (Cisco ACI™) реализует автоматизированную сетевую фабрику на основе политик, отвечающую за фазы перевода и активации в системе на основе намерения, а механизм Cisco Network Assurance Engine контролирует работу сети центра обработки данных.

В корпоративной сети архитектура цифровых сетей Cisco (Cisco DNA™) предлагает подобные сервисы для сред комплекса зданий, филиалов и WAN. Так обеспечивается внедрение функциональных возможностей перевода, активации и контроля в проводные и беспроводные сети, программно-определяемый доступ и программно-определяемые домены глобальной сети. Механизм Cisco Identity Services Engine также обеспечивает применение политик на основе идентификации и предоставляет подробный контекст.

Переход на сетевую модель на основе намерения уже начался!

Дополнительная информация

Узнать больше о сетях на основе намерения можно здесь: https://www.cisco.com/c/ru_ru/solutions/enterprise-networks/intent-based-networking.html

C11-740210-00 01/18