Автоматизация управления сетью Fortinet Security Fabric

Быстрое внедрение цифровых инноваций сделало сети и их безопасность намного более сложными и уязвимыми. Несмотря на то, что злонамеренные кибератаки остаются серьезной проблемой, 48% всех нарушений в прошлом году происходили из неопасных источников, которые можно было предотвратить. Более того, 75% сбоев сети и проблем с производительностью являются результатом ошибки неправильной конфигурации. В этой связи стратегия безопасности сети, которая ставит во главу угла автоматизацию, может помочь уменьшить одну из основных причин кибер-рисков и простоев - человеческий фактор и неправильную конфигурацию.

Центр управления Fortinet Fabric Management Center (состоящий из FortiManager и FortiAnalyzer), являющийся ключевой частью Security Fabric, упрощает операции, связанные с вышеперечисленными вызовами на малых, средних или крупных предприятиях.

Основные варианты использования центра управления Fortinet Fabric:

- **Централизованное управление**
- **Автоматизация сети и оркестровка**
- **Аналитика Security Fabric**

Сложность сетевых операций

Проблемы, связанные со все более сложной и естественно фрагментированной инфраструктурой, по-прежнему вызывают рост кибер-событий и сбоев в работе сетей. Слишком много точечных продуктов, развернутых на большинстве предприятий, почти всегда работают изолированно со своими собственными консолями управления и средами автоматизации, которые являются узкими и актуальными только для этого одного продукта. Следовательно, группы сетевых операций редко имеют четкое и полное представление о том, какие элементы управления и конфигурации установлены в инфраструктуре. Что еще более важно, им не хватает полной видимости сети для обнаружения аномалий.

Интегрированная архитектура сетевой безопасности с возможностями сетевой автоматизации может легко устранить сложную проблему для операторов сети. Центр управления Fortinet Fabric включает FortiManager в сочетании с FortiAnalyzer для решения трех ключевых вариантов использования для эффективных сетевых операций:

- Централизованное управление
- Автоматизация сети и оркестровка
- Аналитика Security Fabric

Централизованное управление

Когда дело доходит до сетевой безопасности, разрозненные ИТ продукты обычно не могут обмениваться данными об угрозах или координировать ответные меры в рамках инфраструктуры организации. Этот критический недостаток кибербезопасности часто усугубляется нехваткой квалифицированного персонала службы безопасности для управления широким ассортиментом отдельных продуктов. Но даже в крупных организациях со специализированным персоналом по ИТ-безопасности все еще возникают трудности с мониторингом сети для отслеживания текущей ситуации - какие устройства подключены, у кого есть доступ к сети и какие ресурсы требуются для каких приложений и рабочих процессов.

Решение для централизованного управления с единой информационной панелью, такое как Fabric Management Center, обеспечивает оптимизированную видимость, снижающую сложность. Он позволяет группам сетевых операций отслеживать перемещение данных и выявлять аномальную активность, упрощает оптимизацию решения и централизует управление межсетевыми экранами нового поколения (NGFW) и другими инструментами безопасности из одного места. Он также упрощает операции для администраторов и персонала с ограниченными ресурсами, требуя меньше человеко-часов при одновременном снижении совокупной стоимости владения (TCO).

Управление устройствами

- Поддерживает централизованное управление с помощью единой консоли через NGFW, программно-определяемую проводную сеть (SD-WAN), программно-определяемую сеть филиала (SD-Branch) и другие варианты использования;
- Масштабирование для поддержки управления более чем 100 000 устройств Fortinet.

Конфигурация предприятия и управление изменениями

- Поддерживает схему организации высокой доступности до пяти географически распределенных устройств;
- Позволяет создавать административные домены для лучшего разделения сетей.

Видимость

- Предоставляет расширенные отчеты и информационные панели для операций и безопасности;
- Предоставляет инструменты для планирования отчетов.

Сетевая автоматизация и оркестровка

Все чаще используются автоматизация и оркестровка, особенно на предприятиях со сложной инфраструктурой. Такие компании ищут способы консолидации управления конфигурацией и изменениями для обеспечения безопасности в сложных гибридных сетях и, что наиболее важно, в таких сценариях использования, как NGFW, SD-WAN и многие другие.

Операционным группам необходимо активно отслеживать аномалии, поскольку предприятия все чаще используют удаленную работу. Они также должны выявлять нарушения с доступом к виртуальной частной сети (VPN) в режиме реального времени. Этого невозможно достичь, если имеющиеся инструменты не интегрированы и не автоматизированы. Центр управления Fortinet Fabric обеспечивает автоматизацию и оркестровку в сложных инфраструктурах с помощью соединителей, средств автоматизации и предупреждений в реальном времени о любых сбоях в сети.

Развертывание и обслуживание

- Предоставляет интерфейс прикладного программирования (API), который позволяет управлять развертыванием Fortinet и интегрироваться с внешними системами обеспечения, мониторинга, инвентаризации и управления изменениями;
- Включает поддержку интерфейса командной строки (CLI) с помощью примеров сценариев.

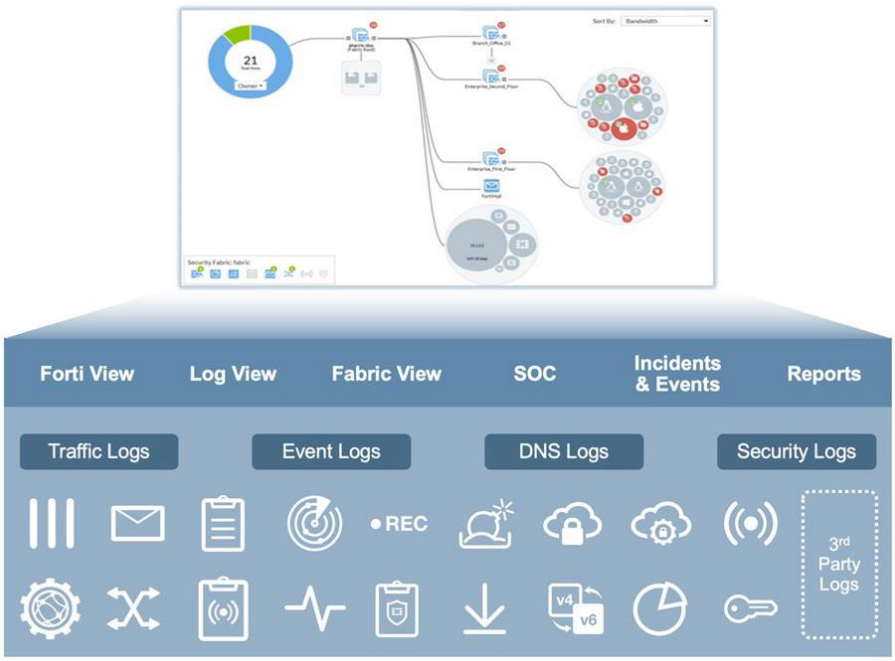
Сетевая интеграция

- Коннекторы Fortinet Fabric обеспечивают интеграцию для управления политиками в единой консоли в нескольких программно-определяемых сетях (SDN), на облачных и партнерских технологических платформах;
- Включает службу распространения Fortinet, которая действует в качестве шлюза для обновления и анализа угроз для всех развернутых устройств Fortinet.

Рабочий процесс и оркестровка

- Обеспечивает быстрое и автоматическое реагирование с помощью инструмента автоматизации FortiOS - простого способа определения действий на триггерах;
- Обеспечивает взаимодействие с существующими инструментами управления и аналитики.

Аналитика Fortinet Fabric



Наблюдение за сетью в реальном времени - непростая задача, особенно с учетом того, что предприятия добавляют все большее количество отдельных ИТ продуктов к и без того сложной инфраструктуре. По мере того, как сетевые группы объединяют такие продукты и используют FortiOS для предотвращения вторжений (IPS), VPN, NGFW, SD-WAN, SD-Branch и других функций, они могут легко обмениваться данными телеметрии между всеми развертываниями и обеспечивать видимость аномалий в реальном времени.

Решение FortiAnalyzer от Fabric Management Center позволяет организациям применять аналитику угроз FortiGuard Labs для выявления проблем в режиме реального времени. FortiAnalyzer помогает коррелировать аналитические данные об угрозах в Security Fabric, используя встроенный механизм аналитики. Он применяет оценку рисков для определения приоритетов аномалий и делится результатами по всей инфраструктуре. Управление этими основными аналитическими возможностями осуществляется с помощью единой консоли FortiManager.

Кроме того, аналитический механизм обеспечивает визуализацию Security Fabric в реальном времени. Эти визуализации позволяют операционным группам выявлять и исследовать любые сетевые риски в режиме реального времени. FortiAnalyzer также поставляется со встроенными панелями мониторинга и отчетами, которые можно легко настроить. Эти функции включают в себя более 700 наборов данных для облегчения адаптации - сложные запросы, оптимизированные для ответов в реальном времени.

Расширенная отчетность

- Поддерживает передовые стандарты безопасности, такие как стандарты Национального института стандартов и технологий (NIST) и Центра интернет-безопасности (CIS).
- Включает отчет о рейтинге безопасности, основанный на сотнях передовых методов обеспечения безопасности Fortinet.

Видимость на основе ролей

- Предлагает целевые информационные панели для ключевых заинтересованных сторон предприятия, включая ИТ-директора, директора по информационным технологиям, архитектора сети и архитектора безопасности;
- Включает панель оценки безопасности для операций безопасности (SecOps).

Серверная часть Security Fabric

- Интегрируется в операционную систему FortiOS и может использоваться для представления топологии и других представлений;
- Использует инструмент автоматизации в FortiAnalyzer и организует ответы в FortiOS.

Повышение значения безопасности на предприятии

Центр управления Fortinet Fabric обеспечивает организацию информационной безопасности корпоративного класса, помогая сетевым командам реализовать ведущие в отрасли преимущества:

Повышает эффективность. Благодаря единому представлению FortiManager помогает предприятиям упростить надзор за инфраструктурой безопасности и автоматизировать реагирование на потенциальные проблемы.

Снижает риск. Функции отслеживания и отчетности Fortinet помогают организациям обеспечивать соблюдение законов о конфиденциальности, стандартов безопасности и отраслевых норм, снижая при этом риски, связанные со штрафами и судебными издержками в случае нарушения. FortiAnalyzer отслеживает активность угроз в реальном времени, упрощает оценку рисков, обнаруживает потенциальные проблемы и помогает смягчить их.

Снижает совокупную стоимость владения. Как часть архитектуры Fortinet Security Fabric, Fabric Management Center помогает снизить совокупную стоимость владения за счет объединения разрозненных функций управления безопасностью. FortiAnalyzer предоставляет преимущества расширенной аналитики и возможностей автоматизации без необходимости добавления дорогостоящих отдельных решений сторонних производителей.