УДК 004.75

СИСТЕМА ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ЗАЩИТОЙ ОКОНЕЧНЫХ УСТРОЙСТВ В КОРПОРАТИВНОЙ СЕТИ

Мұқанов Мерей Амангелдіұлы
mukanov_merey@mail.ru
Магистрант первого курса специальности системы информационной безопасности им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – PhD Ташенова Ж.М.

Аннотация. Информационная безопастность самих оконечных устройств и данных которые в них хранятся очень важна не только для обычных людей, она также очень важна для корпораций, компаний, государтвенных органов, где каждый пользователь корпоративного доменного оконечного устройства (планшета, ноутбука, персонального компьютера) хранят в них очень важные документы, пользуются программами документооборота корпораций, обмениваются файлами и ведут переписку с помощью корпоративной почты.

Ключевые слова: Web Filter, Endpoint Management Server, Windows.

С 2019 года из-за пандемий COVID-19 спрос на специалистов и на устройств по информационной безопасности вырос, так как все стали работать удалённо и подключаться к корпоративным ресурсом из Интернет пространства. Количество атак в виде DDoS, MITM вырос, так как подключения к Intranet ресурсам из внешнего Интернет пространства увеличился вдвойне. Таким образом информационная безопастность всех оконечных устройств (планшетов, ноутбуков, компьютеров и серверов) в корпоративной сети оказался под большим давлением. Атаки из внешних Интернет ресурсов можно заблокировать с помощью Next Generation Firewall и управлять ими с помощью централизованного отдельного устройства как Controller. Мониторить и вовремя выявлять такие виды атак можно с помощью SIEM систем и анализатора сетевого трафика. Это очень эффективно, информационно безопастно и надёжно. А что делать с атаками направленными с самих оконечных устройств? Как их мониторить? Как избежать и вовремя выявлять такие виды атак? И самое главное, как централизованно управлять информационной безопасностью всех оконечных устройств в корпоративной сети? На эти вопросы можно ответить одной фразой: антивирусная система.

Антивирусная система защищает все виды оконечных устройтсв в корпоративной сети от вредоносных кодов, сплойтных программ, нежелательных файлов, опасных вирусов, нагружающего оконечное устройтсво сетевого трафика. С помощью антивирусной системы

можно защитить оконечные устройства точечным образом, установив программу антивирусной системы на каждое оконечное устройтсво. После окончания установки антивируса на персональный компьютер, сервер, ноутбук или на планшет мы можем считать что это устройтсво защищено от любых видов угроз. Этот метод очень хорошо подходит для одного человека или для предприятий малого объёма, где количество оконечных устройств не повышает 10-15 устройств. Для корпоративных сетей, где количество оконечных устройств превышает 50 устройств метод точечной защиты очень неудобен. Чтобы на каждое устройство установить антивирусную программу инженер информационной безопасности должен будет потратить немало своего и рабочего времени. Такой метод установки и защиты оконечных устройств будет останавливать работу сотрудников в корпоративной сети. Для таких предприятий необходим гибкий метод защиты оконечных устройств с централизованным управлением антивирусных программ в устройствах.

Существует множество видов антивирусных программ, которые обеспечивают гибкую работу с оконечными устройствами и с централизованным управлением системой, и та, которая подходит для моего проекта, будет зависеть от ряда факторов, таких как, сколько оконечных устройств необходимо одновременно защитить в корпоративной сети и какие виды защиты нужно обеспечить для этих устройств.

FortiClient Endpoint Management Server (FortiClient EMS) – это решение для управления безопасностью, которое обеспечивает масштабируемое и централизованное управление несколькими конечными точками (компьютерами, ноутбуками, планшетами, серверами). FortiClient EMS обеспечивает эффективное и действенное администрирование конечных точек, на которых работает FortiClient. Он обеспечивает видимость всей сети для безопасного обмена информацией и назначения политик безопасности для конечных точек. Он предназначен для обеспечения максимальной эффективности работы и включает автоматизированные функции управления устройствами и устранения неполадок. FortiClient EMS также работает с расширением FortiClient Web Filter для обеспечения веб-фильтрации для пользователей Google Chromebook.

FortiClient EMS очень хорошо вписывается в малые и крупные предприятия, которые развертывают FortiClient на конечных точках и/или обеспечивают веб-фильтрацию для пользователей Google Chromebook. Преимущества развертывания FortiClient EMS включают в себя:

- Удаленное развертывание программного обеспечения FortiClient на конечных точках с Windows и MacOS;
- Обновление профилей конечных пользователей вне зависимости от места доступа;
- Администрирование подключений к конечной точке FortiClient, например, прием, отключение и блокировка подключений;
- Управление и мониторинг конечных точек, таких как информация о состоянии, системе и подписи;
- Выявление устаревших версий программного обеспечения FortiClient;
- Определение правил веб-фильтрации в профиле и удаленное развертывание профиля в расширении FortiClient Web Filter на конечных точках Google Chromebook.

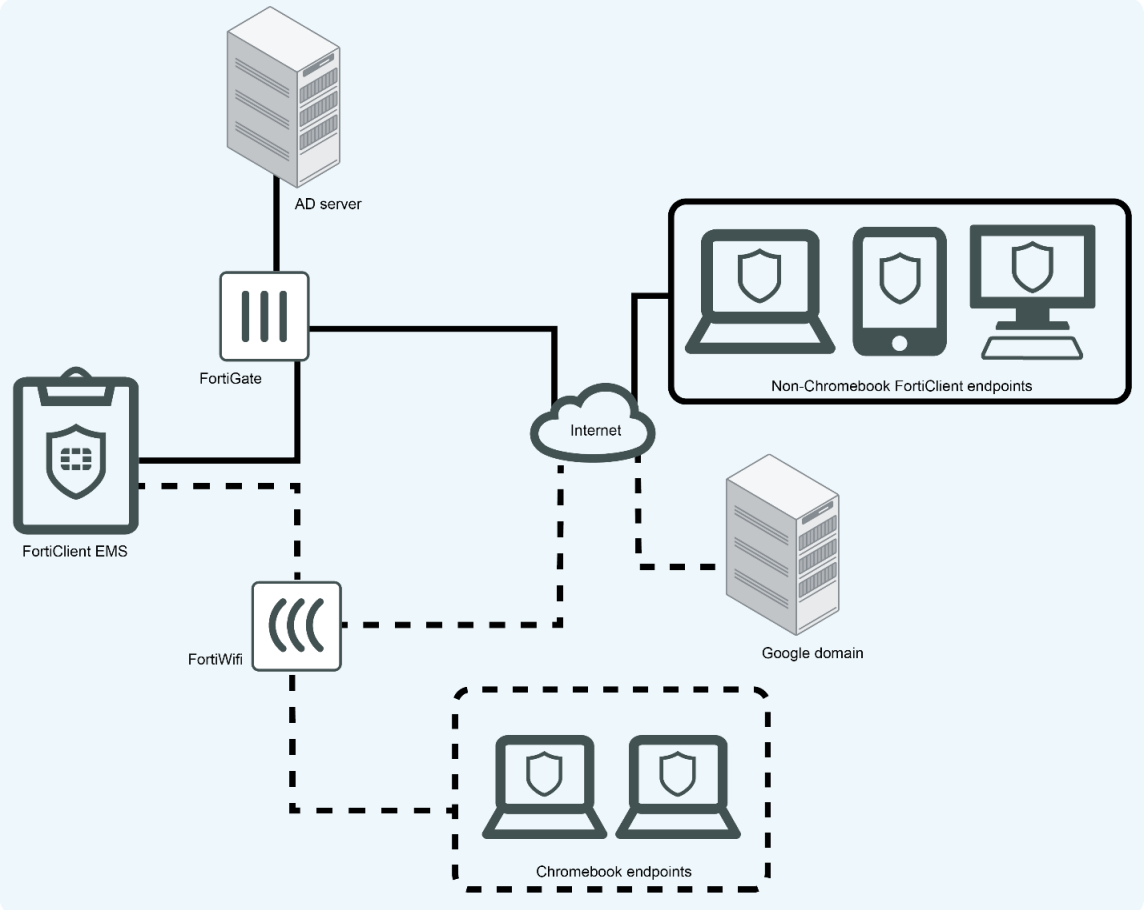
FortiClient EMS предоставляет инфраструктуру для установки и управления программным обеспечением FortiClient на конечных точках. FortiClient защищает конечные точки от вирусов, угроз и рисков.

FortiClient EMS также предоставляет инфраструктуру для установки и управления расширением FortiClient Web Filter на конечных точках Google Chromebook. FortiClient защищает пользователей конечных точек, работая с FortiClient EMS для фильтрации просмотра веб-контента пользователями конечных точек на Google Chromebook.

В следующей таблице перечислены компоненты FortiClient EMS:

Компонент	Описание
FortiClient EMS	Управляет FortiClient на конечных точках, которые подключаются к корпоративной сети. Управляет расширением FortiClient Web Filter, установленным на конечных точках Google Chromebook, которые подключены к домену Google.
База данных	Сохраняет профили безопасности и события. Также хранит информацию о пользователе, полученную из консоли администратора Google для Chromebook. FortiClient EMS устанавливается вместе с базой данных SQL.
FortiClient	Помогает обеспечить безопасность и защиту конечных точек. Он работает на серверах, настольных и портативных компьютерах, которые нужно защищать.
Расширение Web Filter FortiClient	Взаимодействует с FortiClient EMS и обеспечивает веб-фильтрацию на конечных точках.

На схеме пунктирными линиями показано, как различные компоненты подключаются для управления конечными точками Windows, MacOS и Linux с помощью FortiClient EMS. Пунктирные линии показывают, как используются компоненты для управления конечными точками Chromebook с помощью FortiClient EMS.



FortiClient EMS позволяет:

- Создание и применение профилей безопасности;
- Управление развертыванием, конфигурацией и обновлениями;
- Управление профилями безопасности с интегрированной консоли управления;
- Выполнить комплексную установку компонентов безопасности и настроить профили;
- Мониторинг активности конечных точек в Интернете.

Заключение

Основываясь на выше сказанные теорий, применение централизованной защиты конечных устройств в корпоративной сети, где количество конечных устройств превышает 50, очень удобен, гибок для управления, информационно безопасно, а также правильный подход к единому требованию информационной безопасности. В нашем случае для этой цели будет использоваться программное обеспечение FortiClient EMS, так как он имеет расширенные функций защиты конечных устройств в корпоративной сети Web Filtering, Chromebook, Advanced Antivirus Protection, поддерживает все используемые в конечных устройствах операционные системы Windows, MacOS, Linux, Windows Server.

Список использованных источников

1. Григорьев А.Н., Мускатиньев А.Ю., Иванов П.Ю., Организация антивирусной защиты автоматизированных информационных систем органов внутренних дел, 2016. С. 38-57.
2. Алексеев П.П., Антивирусы. Настраиваем защиту компьютера от вирусов / П.П. Алексеев. – Москва: Наука и техника, 2013. – 80 с.
3. Анастасия Сапрыкина. Обеспечение безопасности удалённых рабочих мест при помощи продуктов Fortinet. https://www.anti-malware.ru/practice/solutions/securing-remote-workstations-with-fortinet-products, 2020.