ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІНЦЕВИХ ПРОСТРОЇВ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ РІШЕННЯ FORTICLIENT»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 «Кібербезпека»
Освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Цуранов М.О.
(прізвище та ініціали)

Керівник Довженко Н.М.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ВСТУП

Актуальність дослідження. Персональні комп'ютери допомагають нам виконувати роботу. Допомагають правильно планувати час за допомогою додатків календарів, записників і тд. Персональні комп'ютери такі як смартфони, ноутбуки, планшети є кінцевими пристроями для підприємств і компаній в яких працюють співробітники.

Якщо пристрій підключено до мережі, він вважається кінцевою точкою. Зі зростанням популярності BYOD (bring your own device) та IoT (Internet of Things) кількість окремих пристроїв, підключених до мережі організації, може швидко досягати десятків а то і тисяч.

Захист кінцевих точок є важливою частиною кібербезпеки підприємства з кількох причин. Перш за все, у сучасному діловому світі дані є найціннішим активом компанії, і втрата цих даних або доступу до них може поставити весь бізнес під загрозу банкрутства. Підприємствам також доводиться стикатися не лише зі зростанням кількості кінцевих точок, але й із збільшенням кількості типів кінцевих точок. Ці фактори самі по собі ускладнюють забезпечення безпеки кінцевої точки підприємства, також вони ускладнюються політиками віддаленої роботи та BYOD, які роблять захист периметра дедалі недостатнішим і створюють уразливості. Ландшафт загроз також ускладнюється: хакери завжди винаходять нові способи отримати доступ, викрасти інформацію або змусити співробітників надати конфіденційну інформацію. Якщо врахувати вартість перерозподілу ресурсів із бізнес-цілей на боротьбу із загрозами, репутаційні витрати від масштабного порушення та фактичні фінансові витрати від порушень відповідності, і легко зрозуміти, чому захист кінцевих точок стали вважатися обов'язковими.

Тенденція віддаленої роботи співробітників за останні декілька років дуже зросла. Пандемія COVID-19 посприяла збільшенню співробітників які працюють з

дому, а отже збільшився ландшафт атак для зловмисників. Оскільки обсяг і складність загроз кібербезпеці неухильно зростають, зростає потреба в більш досконалих рішеннях безпеки кінцевих точок. Сучасні системи захисту кінцевих точок розроблені для швидкого виявлення, аналізу, блокування та стримування поточних атак. Для цього їм потрібно співпрацювати один з одним та з іншими технологіями безпеки, щоб надати адміністраторам бачення передових загроз, щоб пришвидшити час виявлення та реагування на виправлення. Організації будь-якого розміру піддаються ризику з боку хактивістів, організованої злочинності, а також зловмисних і випадкових внутрішніх загроз. Безпека кінцевих точок часто розглядається як головна лінія кібербезпеки, і це одне з перших місць, де організації прагнуть захистити свої корпоративні мережі.

Розуміння усіх цих загроз а також важливість безпеки кінцевих точок змушують вдосконалювати та розбудовувати захист пристроїв які підключаються до корпоративної мережі.

Об'єкт дослідження – процес забезпечення захисту кінцевих точок корпоративної інформаційної мережі.

Предмет дослідження – технологія захисту кінцевих точок корпоративної інформаційної мережі.

Мета роботи - розробити варіант технології захисту кінцевих точок корпоративної інформаційної мережі.

Наукові завдання:

- дослідити сутність проблеми забезпечення захисту корпоративних кінцевих пристроїв;
- виокремити втрати підприємств через атаки на кінцеві пристрої;
- проаналізувати існуючі актуальні атаки на кінцеві пристрої;
- розробити варіант технології захисту кінцевих точок корпоративної інформаційної мережі.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, моделювання топології системи захисту корпоративних кінцевих пристроїв та розробленя рекомендації щодо захисту.

Практичне значення одержаних результатів полягає в розробці варіанта технології захисту корпоративних кінцевих пристроїв на базі Fortinet Forticlient та Forticlient EMS.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на конференції:

1) Всеукраїнська науково-технічна конференція «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р., 130-132 стр.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Аналіз кібератак на кінцеві пристрої корпоративної мережі

Кібератака — це напад, здійснений кіберзлочинцями за допомогою одного чи кількох комп’ютерів проти одного чи кількох комп’ютерів чи мереж. Кібератака може зловмисно вивести комп’ютери з ладу, викрасти дані або використати зламаний комп’ютер як точку запуску для інших атак[1].

Кібератаки на кінцеві пристрої можно поділити на внутрішні та зовнішні[2].

Зовнішніми кібератаками є:

- Phishing(фішинг), spear phishing (таргетований фішинг) та whaling (фішинг таргетований на високопосадовців);
- Malware (шкідливе програмне забезпечення);
- DoS/DDoS (атаки типу відмова в обслуговуванні);
- Advanced Persistent Threat (постійна загроза підвищеної складності);
- Атаки які використовують макроси та скрипти.

Внутрішні кібератаки:

- Компрометація підрядників, третіх компаній;
- Випадкова помилка або розкриття співробітником;
- Компанії які надають послуги, а також вендорів додатків/систем які використовує підприємство.

1.2 Зовнішні кібератаки на кінцеві пристрої корпоративної мережі

Phishing та його різновиди. Фішинг передбачає надсилання зловмисних електронних листів із імовірно надійних джерел якомога більшій кількості людей за умови низького рівня відповіді. Наприклад, фішинговий електронний лист може нібито надійти від PayPal і просити одержувача підтвердити дані свого облікового запису, натиснувши на вкладене посилання, що призводить до встановлення зловмисного програмного забезпечення на комп'ютері жертви. Фішингові електронні листи є знеособленими, надсилаються масово й часто містять орфографічні чи інші помилки, які виявляють їхні зловмисні наміри. Проблема в тому, що не всі помічають ці тонкі натяки. Довірених логотипів і посилань на відомі пункти призначення достатньо, щоб обманом змусити багатьох людей поділитися своїми даними[3].

Spare Phishing – таргетовані фішингові електронні листи які складніше виявити, оскільки вони, здається, надходять із джерел, близьких до цілі. Кіберзлочинці надсилають персоналізовані електронні листи певним особам або групам людей, які мають щось спільне, наприклад співробітникам, які працюють в одному відділі. Фішери використовують Інтернет, найчастіше соціальні мережі, щоб вивчати та збирати інформацію про своїх цілей, тому ці повідомлення можуть адресуватися вам особисто, використовувати знайому мову і тд.

Whaling (вилов китів) - використовує оманливі повідомлення електронної пошти, націлені на керівників високого рівня в організації, таких як генеральні директори, фінансові директори та інші керівники. Такі особи мають доступ до дуже цінної інформації, включаючи комерційні таємниці та паролі до адміністративних облікових записів компанії. Зловмисник надсилає електронні листи з критично важливих для бізнесу питань, видаючи себе за особу чи організацію з законними повноваженнями. Наприклад, зловмисник може надіслати електронного листа генеральному директору з проханням оплатити, видаючи себе за клієнта компанії. Китобійні атаки завжди спрямовані особисто на цільових осіб, часто використовуючи

їхні титул, посаду та номер телефону, які отримані з веб-сайтів компаній, соціальних мереж або преси. Різниця між виловом китів і фішингом полягає в тому, що китобій націлений виключно на високопоставлених осіб в організації, тоді як фішинг зазвичай націлений на категорію осіб з нижчим авторитетом[4].

Barrel Phishing або Double-Barrel Spear Phishing цей тип фішингу відрізняється від більшості прямих фішингів, оскільки ці зловмисники використовують двосторонній підхід, щоб обдурити свої цілі, тоді як прямий фішинг зазвичай включає один електронний лист конкретній особі. Barrel Phishing часто включає два електронні листи. Перший зазвичай безпечний і призначений для встановлення довіри. Другий електронний лист, який може розглядатися як доповнення, містить зловмисне посилання або вкладений файл із начебто невинним запитом. Наприклад, повідомлення 1 може містити: «Привіт. У мене є питання.» У другому електронному листі може бути щось на кшталт: «Знову я. Ви б могли перевірити цей файл на наявність помилок? Це важливо. Взаємодія з посиланням або вкладенням призводить до крадіжки облікових даних, зараження зловмисним програмним забезпеченням або іншого типу зламу[5].

Clone Phishing or Cloning хоча фішинг і Whaling шкідливі, фішинг клонів дещо змінює ситуацію. Клонування фішингу дещо відрізняється від звичайної спроби фішингу. Атака клонування фішингу використовує законний або раніше надісланий електронний лист, який містить вкладення або посилання. Клон — це майже копія оригіналу, де вкладені файли або посилання замінені шкідливим програмним забезпеченням або вірусом. Електронний лист зазвичай підроблено, щоб виглядати так, ніби його надіслав початковий відправник, і стверджувати, що це просте повторне надсилання. Що ще гірше, електронний лист надсилається великій кількості одержувачів, і зловмисник просто чекає, поки жертви натиснуть його. Коли жертва піддається клонованому електронному листу, зловмисник пересилає той самий підроблений електронний лист контактам із папки «Вхідні» жертви. Цей тип атаки

вважається найшкідливішим, оскільки жертвам важко запідозрити підроблену електронну пошту.

Malware (зловмисне програмне забезпечення) – це загальний термін для будь-якого типу зловмисного програмного забезпечення, призначеного для шкоди або використання будь-якого програмованого пристрою, служби чи мережі. Кіберзлочинці зазвичай використовують його для вилучення даних, які вони можуть використовувати для отримання фінансової вигоди. Ці дані можуть варіюватися від фінансових даних до медичних записів, особистих електронних листів і паролів — можливості того, яку інформацію можна зламати, стали безмежними.

Ransomware (програмне забезпечення-вимагач) – це тип зловмисного програмного забезпечення, призначеного для вимагання грошей у своїх жертв, яким блокується або забороняється доступ до даних у їхніх системах. Два найпоширеніші типи програм-вимагачів – це шифрувальники та блокувальники екрана. Шифрувальники, як випливає з назви, шифрують дані в системі, роблячи вміст марним без ключа дешифрування. Блокувальники екрана, з іншого боку, просто блокують доступ до системи за допомогою екрану «блокування», стверджуючи, що система зашифрована. Жертви часто отримують сповіщення на екрані блокування (спільне як для шифраторів, так і для блокувальників екрана) про необхідність придбати криптовалюту, наприклад біткойн, щоб сплатити викуп. Після сплати викупу клієнти отримують ключ розшифровки та можуть спробувати розшифрувати файли. Дешифрування не гарантується, оскільки численні джерела повідомляють про різний ступінь успіху дешифрування після сплати викупу.

Іноді жертви так і не отримують ключі. Деякі атаки встановлюють зловмисне програмне забезпечення на комп’ютерну систему навіть після сплати викупу та оприлюднення даних. Хоча спочатку зосереджувалися переважно на персональних комп’ютерах, шифрувальні програми-вимагачі все більше націлювалися на бізнес-користувачів, оскільки компанії часто платять більше за розблокування критичних систем і відновлення щоденних операцій, ніж окремі особи. Корпоративні програми-

вимагачі або віруси зазвичай починаються зі шкідливого електронного листа. Нічого не підозрюючи користувач відкриває вкладення або клацає на шкідливій або скомпрометованій URL-адресі.

У цей момент встановлюється агент-вимагач, який починає шифрувати ключові файли на комп'ютері жертви та будь-які прикріплені спільні файли[6]. Після шифрування даних програма-вимагач відображає повідомлення на зараженому пристрої. У повідомленні пояснюється, що сталося і як розплатитися зловмисникам. Якщо жертви заплатять, програма-вимагач дати код для розблокування даних. Підприємство, яке стає жертвою програм-вимагачів, може втратити тисячі доларів у продуктивності та втраті даних.

Зловмисники, які мають доступ до даних, шантажуватимуть жертв, щоб вони сплатили викуп, погрожуючи оприлюднити дані та викрити порушення даних, тож організації, які не платять достатньо швидко, можуть отримати додаткові побічні ефекти, такі як пошкодження бренду та судові процеси. Програми-вимагачі зупиняють продуктивність, тому першим кроком є стримування. Після стримування організація може або відновити з резервних копій, або заплатити викуп. Правоохоронні органи беруть участь у розслідуванні, але відстеження авторів програм-вимагачів вимагає часу на дослідження, що лише затримує відновлення. Аналіз першопричини визначає вразливість, але будь-які затримки у відновленні впливають на продуктивність і дохід бізнесу.

Scareware (залякувальні програми) кіберзлочинці лякають, змушуючи думати, що комп'ютери чи смартфони заражені, щоб переконати жертв придбати підроблену програму. У типовому шахрайському програмному забезпеченні під час перегляду веб-сторінок можно побачити тривожне повідомлення «Увага: ваш комп'ютер заражено!» або «У вас вірус!» Кіберзлочинці використовують ці програми та неетичну рекламну практику, щоб залякати користувачів і змусити їх придбати шахрайські програми.

Worms (черв’яки) – черв’яки мають здатність копіювати себе з машини на машину, як правило, використовуючи певні недоліки безпеки в програмному забезпеченні чи операційній системі, і не вимагають взаємодії користувача для функціонування.

Spyware (Шпигунське програмне забезпечення) – це програма, встановлена на комп’ютері, зазвичай без явного відома власника, яка збирає та передає особисту інформацію чи звички та деталі перегляду Інтернету. Шпигунське програмне забезпечення дозволяє контролювати всі форми зв’язку на цільовому пристрої. Шпигунське програмне забезпечення часто використовується правоохоронними органами, урядовими установами та організаціями з інформаційної безпеки для тестування та моніторингу комунікацій у конфіденційному середовищі або під час розслідування. Але шпигунське програмне забезпечення також доступне для споживачів, дозволяючи покупцям стежити за своєю дружиною, дітьми та співробітниками і тд. *Троянські програми* - маскуються під нешкідливі програми, обманом змушуючи користувачів завантажувати та використовувати їх. Після того, як така програма запущена, вона може викрасти особисті дані, вивести з ладу пристрій, стежити за діяльністю або навіть здійснити атаку.

Adware (Рекламні програми) надсилають користувачам небажану рекламу та зазвичай відображають миготливі рекламні повідомлення або спливаючі вікна, коли виконується певна дія. Програми з рекламним програмним забезпеченням часто встановлюються в обмін на іншу послугу, наприклад, право використовувати іншу програму без плати за неї[7].

*Fileless malware(*Безфайлове зловмисне програмне забезпечення*)* – це тип шкідливого програмного забезпечення, яке використовує законні програми для зараження комп’ютера. Безфайлові атаки на реєстр зловмисних програм не залишають жодних файлів зловмисного програмного забезпечення для сканування та виявлення зловмисних процесів. Він не покладається на файли та не залишає слідів, тому його складно виявити та видалити[8].

DoS/DDoS (відмова в обслуговуванні/розподілена відмова в обслуговуванні). — це тактика перевантаження комп'ютера або мережі, щоб зробити їх недоступними. Зловмисники досягають цього, надсилаючи більше трафіку, ніж ціль може обробити, спричиняючи її збій, що робить її нездатною надавати послуги своїм звичайним користувачам. Ця атака здійснюється з одного атакуючого комп'ютеру. Сьогодні такая проста атака як відмова в обслуговуванні (DoS) майже не використвується зловмисниками, тому що можливості обробки данних сучасних розподілених систем здатні витримати такі атаки без великої втрати в продуктивності. Розподілена атака типу «відмова в обслуговуванні» (DDoS) виникає, коли група систем переповнює сервер шахрайським трафіком. Згодом сервер перевантажується, через що він або виходить з ладу, або перестає відповідати навіть на законні запити. DDoS-атака запускається з численних скомпрометованих пристроїв, які часто розповсюджуються по всьому світу в так званих ботнетах. Загалом DoS- і DDoS-атаки можна розділити на три типи:

- Об'ємні атаки. Включає затоплення UDP, затоплення ICMP та інші затоплення підроблених пакетів. Метою атаки є перенасичення смуги пропускання атакуваного сайту, а величина вимірюється в бітах на секунду;
- Атаки на протокол. Включає SYN-флуд, фрагментовані пакетні атаки, Ping of Death, Smurf DDoS тощо. Цей тип атаки споживає фактичні ресурси сервера або проміжного комунікаційного обладнання, такого як брандмауери та балансувальники навантаження, і вимірюється в пакетах за секунду;
- Атаки рівня додатків. Включає атаки з низьким і повільним доступом, затоплення GET/POST, атаки, спрямовані на вразливості Apache, Windows або OpenBSD тощо. Ці атаки, що складаються із, здавалося б, законних і невинних запитів, мають на меті призвести до збою веб-сервера, а величина вимірюється в запитах за секунду.

APT (Advanced Persistent Threat - постійна загроза підвищеної складності) — це широкий термін, який використовується для опису кампанії атаки, під час якої

зловмисник або група зловмисників встановлює незаконну довгострокову присутність у мережі з метою вилучення дуже конфіденційних даних. Метами цих нападів, які дуже ретельно вибираються та досліджуються, зазвичай є великі підприємства чи урядові мережі[9].

Наслідки таких вторгнень величезні й включають: крадіжку інтелектуальної власності (наприклад, комерційної таємниці чи патентів); крадіжку конфіденційної інформації (наприклад, особисті дані співробітників і користувачів); саботування критичної організаційної інфраструктури (наприклад, видалення бази даних); повне захоплення сайту. Виконання атаки APT вимагає більше ресурсів, ніж стандартна атака веб-додатків. Зазвичай злочинцями є групи досвідчених кіберзлочинців, які мають значну фінансову підтримку.

Деякі атаки APT фінансуються урядом і використовуються як зброя кібервійни. Зловмисники використовують багатоетапні атаки на мережу організації, які проводяться протягом тривалого часу. Атаки APT можуть тривати місяцями або роками, залишаючись непоміченими у мережі та постійно збираючи конфіденційну або цінну інформацію. Вони неймовірно складні та різноманітні, тому їх важко виявити та усунути, але є загальні характеристики прогресивних атак із постійною загрозою, які можна визначити, щоб підготуватися до атак і захиститися від них. Основні фази чи етапи постійної загрози підвищенної сладності можно виділити наступним чином:

1. *Початковий доступ*. Групи APT починають свою кампанію з отримання доступу до мережі через одну з трьох поверхонь атаки: веб-системи, мережі або користувачі. Зазвичай вони отримують доступ через зловмисне завантаження, пошук і використання вразливостей додатків, прогалини в інструментах безпеки та, як правило, через фішинг, націлений на співробітників із привілейованими обліковими записами. Мета — заразити ціль шкідливим програмним забезпеченням.

2. *Перше проникнення та розгортання шкідливого програмного забезпечення.* Отримавши доступ, зловмисники компрометують проникнуту систему,

встановлюючи бекдор-оболонку, троян, замаскований під законне програмне забезпечення, або інше шкідливе програмне забезпечення, яке дозволяє їм отримати доступ до мережі та віддалено керувати проникнутою системою. Важливою віхою є встановлення вихідного з'єднання з їхньою системою управління. APT можуть використовувати вдосконалені методи зловмисного програмного забезпечення, такі як шифрування, обфускація або переписування коду, щоб приховати свою діяльність.

3. *Розширення доступу та горизонтальне переміщення.* Зловмисники використовують перше проникнення, щоб зібрати більше інформації про цільову мережу. Вони можуть використовувати атаки грубої сили або використовувати інші вразливості, які вони виявляють у мережі, щоб отримати глибший доступ і контролювати додаткові, більш чутливі системи. Зловмисники встановлюють додаткові бекдори та створюють тунелі, що дозволяє їм здійснювати бічний рух по мережі та переміщувати дані за бажанням.

4. *Інсценування нападу.* Розширивши свою присутність, зловмисники ідентифікують дані або активи, які їм потрібні, і передають їх у безпечне місце всередині мережі, зазвичай зашифровані та стиснуті для підготовки до викрадання. Цей етап може зайняти деякий час, оскільки зловмисники продовжують компрометувати більш чутливі системи та переносити їхні дані в безпечне сховище.

5. *Ексфільтрація або нанесення пошкоджень*. Нарешті зловмисники готуються передати дані за межі системи. Вони часто проводять «атаку білим шумом», таку як атака розподіленої відмови в обслуговуванні (DDoS), щоб відволікти команди безпеки під час передачі даних за межі периметра мережі. Після цього вони вживатимуть заходів для видалення судово-медичних доказів передачі даних. Залежно від мети атаки, у цей момент група APT може завдати величезної шкоди, виснаживши організацію або захопивши критично важливі активи, такі як веб-сайти чи центри обробки даних.

6. *Подальші напади.* Якщо APT-атака передбачала тихе викрадання даних, яке не було виявлено, зловмисники залишатимуться в мережі та чекатимуть

додаткових можливостей атаки. З часом вони можуть зібрати додаткові конфіденційні дані та повторити процес. Вони також прагнуть створити бекдори, які важко виявити, щоб навіть якщо їх спіймали, була змога відновити доступ до системи в майбутньому.

Атаки які використовують макроси. Макроси — це програми спеціального призначення, які використовуються для автоматизації процедур у більшій програмі чи програмному забезпеченні. Макроси є досить потужним і простим способом автоматизації простих завдань Microsoft Office. Вони допомогли трохи полегшити роботу повсякденного офісного працівника, але вони також відкрити соковиту поверхню для атаки. Зазвичай макрос складається з ряду команд і дій, написаних спеціальною мовою макросів або стандартною мовою програмування. Ці команди автоматично виконуватимуться програмою, коли відбудеться певний тригер. Макроси широко реалізовані в Office Suites, щоб дозволити автоматизувати типові завдання та процедури. Різні пакети використовують різні мови макросів, але деякі помітні згадки включають Visual Basic для програм (MS Office), LibreOffice Basic (LibreOffice) і OpenOffice Basic (OpenOffice). Більшість мов макросів Office мають досить широкі можливості та доступ до різних ресурсів. Наприклад, макроси MS Office (написані на VBA) можуть запускати виконувані файли та використовувати мережеві можливості. Як і будь-яка інша програма, що дозволяє виконувати настроювані сценарії у фоновому режимі, зловмисники можуть використовувати пакети Office для запуску зловмисного коду та компрометації жертв. Зазвичай макрозловмисне програмне забезпечення діє як завантажувач у ланцюжку зараження та завантажує та виконує інше корисне навантаження перед припиненням. Зловмисне програмне забезпечення буде вбудовано – як ви вже здогадалися – у файл Office і імплантовано десь, щоб жертва могла отримати до нього доступ, скажімо, у звичайний файловий ресурс або за допомогою електронної пошти. Після відкриття файлу зловмисне програмне забезпечення буде запущено. Це називається Spearphishing Macro Attack, і воно було поширеним протягом дуже тривалого часу. Одним із пам’ятних прикладів макрозловмисного програмного забезпечення є вірус Melissa, який вперше з’явився в

1999 році. Зловмисне програмне забезпечення було вбудовано у файл MS Word і після відкриття надсилало електронний лист до перших 50 контактів в адресній книзі жертви. Хоча це не завдало великої шкоди окремим користувачам (окрім випадкового спричинення кількох поштових служб до DDOS), загальна вартість завданих збитків була оцінена в 80 мільйонів доларів, а зловмисник був засуджений до 20 місяців у федеральній в'язниці. Але це не означає, що макроатаки підманного фішингу є пережитком минулих днів. Згідно з даними, зібраними Cofense Intelligence [10], протягом серпня 2018 року шкідливі макроси, вбудовані у файли MS Office, становили 45% усіх проаналізованих механізмів доставки шкідливого програмного забезпечення. Більше того, незважаючи на, здавалося б, аматорський характер таких атак, зловмисне програмне забезпечення використовувалося для доставки деяких із найбільш шкідливих корисних навантажень у обігу, зокрема Geodo, Chanitor, AZORult та інших. Методології підводного фішингу також використовувалися в комплексних атаках APT різними групами, у тому числі кількома, які, як вважають, мають зв'язки зі шпигунськими агентствами. Під час деяких складніших атак законні офісні файли замінювалися шкідливими, на перший погляд ідентичними.

Одним із основних ризиків макровірусів є їх здатність швидко поширюватися. Після запуску зловмисне програмне забезпечення може вставлятися в інші файли Office на комп'ютері жертви або навіть у самі шаблони файлів Office, що робить кожен документ, створений на комп'ютері, скомпрометованим. У міру поширення зловмисного програмного забезпечення стає все більше легітимних файлів під загрозу, і збільшується можливість помилок користувачів. Крім того, оскільки макроси написані на макро-мові та виконуються як частина більшої програми, вони значною мірою сумісні між платформами, що робить їх поширення ще простішим. Макрошкідливе програмне забезпечення відносно легко обфускувати. Інструменти обфускації легко доступні в Інтернеті, а фрагменти зловмисного коду можна навіть вилучити з вихідного коду макросу та сховати в інших компонентах файлу, таких як текстові мітки, клітинки Excel тощо, щоб уникнути виявлення. Макрозагрози можуть

бути створені для існування «безфайлово», тобто вони нічого не записують на диск і використовують лише звичайні інструменти для запуску коду безпосередньо в пам’яті. Ця техніка набула популярності в останні роки. Двійкові файли, бібліотеки та сценарії можна використовувати виключно для створення повністю безфайлового шкідливого програмного забезпечення або об’єднати з традиційними методами для створення гібридних векторів атак, які записують деякі файли на жорсткий диск. Низький поріг входу. Як і в багатьох методологіях виконання користувачами, макроатаки мають низький поріг входу для успішного виконання. Макрошкідливі програми досить прості в експлуатації та потребують мінімальних налаштувань для конкретних жертв (якщо такі є), в обмін на те, що вони сильно залежать від методів соціальної інженерії.

Атаки які використовують скрипти. Далі буде розглянуто приклад етапів виконання PowerShell скриптів який використовується в MS Windows як самої розповсюдженної операційної системи. PowerShell — це мова сценаріїв розроблений Microsoft, щоб забезпечити кращий інтерфейс для системних адміністраторів, щоб спростити й автоматизувати адміністративні завдання. У атаках за допомогою PowerShell скриптів можна виділити наступні етапи:

1. *Обхід заборони виконання.* Microsoft обмежує сценарії PowerShell політикою виконання, щоб запобігти випадковому виконанню користувачами сценаріїв, які вони не повинні виконувати. Ці обмеження також допомагають запобігти запуску шкідливих сценаріїв у кампаніях соціальної інженерії. Параметром політики виконання за замовчуванням є Restricted. Ця політика за замовчуванням дозволяє користувачам запускати лише інтерактивні сеанси PowerShell і окремі команди, незалежно від походження сценаріїв або від того, чи вони підписані та надійні. Організації встановлюють різні політики для задоволення своїх потреб. Однак зловмисники використовують різні методи, щоб обійти політику виконання. Ось найпоширеніші обхідні шляхи:

- Вивести сценарій за допомогою Echo і передати його в стандартний вхід PowerShell – щоб виконати цей обхід, потрібно передати сценарій у стандартний вхід PowerShell за допомогою команди echo або type. Ця техніка не змінює конфігурації та не вимагає запису на диск.
- Вивести сценарій за допомогою Echo і передати його в інтерактивну консоль PowerShell — це найпростіший обхід, який буде корисним для запуску сценаріїв в інтерактивній консолі. Щоб виконати цей обхід, потрібно скопіювати та вставити сценарій PowerShell в інтерактивну консоль. Ця техніка не змінює конфігурації та не вимагає запису на диск. Однак, ця техніка, буде обмежена привілеями користувача від якого буде запущений скрипт.
- Завантаження сценарія за URL-адресою та передача виразу виклику для його виконання. У цій техніці можливо завантажити сценарій PowerShell з Інтернету та виконати його без запису на диск і зміни конфігурацій.
- Читання сценарію із файлу та передача його стандартній команді Windows «type» або команді PowerShell «get-content», щоб прочитати сценарій із диска та передати його до стандартного вводу PowerShell. Для цього обходу потрібно буде записати сценарій на диск, але конфігурація не зміниться. Щоб уникнути запису на диск, можно прочитати сценарій з мережевого ресурсу.
- Використання перемикача «Command» — цей обхід схожий на обхід за допомогою інтерактивної консолі, але не потребує використання інтерактивної консолі. Недоліком цього обходу є те, що складні сценарії зазвичай призводять до помилок читання цих сценаріїв. Цей обхід не призведе до змін конфігурації або запису на диск.
- Використання перемикача «EncodeCommand» — ця техніка дуже схожа на обхід «використання перемикача «Command», тільки в цьому випадку сценарії надаються як рядки, закодовані Unicode або base64. Це допомагає уникнути помилок читання сценаріїв, які зазвичай трапляються під час використання перемикача

«Command». Під час використання цього обходу не буде жодних змін у конфігурації чи запису на диск.

- Використання команди «Invoke-Command» — цей обхід можна використовувати для виконання команд у віддалених системах, де ввімкнено віддалене керування PowerShell. Зазвичай це виконується за допомогою інтерактивної консолі або однорядкової команди з перемикачем «Command». Цей обхід не призведе до змін конфігурації або запису на диск.
- Використання команди «Invoke-Expression» — цей обхід зазвичай виконується за допомогою інтерактивної консолі та не призводить до змін конфігурації чи запису на диск.
- Використання прапорця політики виконання «Bypass» — коли цей прапорець використовується, нічого не блокується та не буде попереджень чи підказок. Він використовується, коли зловмисник виконує сценарії з файлу. Це не призведе до змін конфігурації під час запису на диск.
- Використання прапору політики виконання «Unrestricted» — коли використовується цей прапор, він завантажує всі файли конфігурації та запускає всі сценарії. Під час запуску непідписаних сценаріїв, завантажених з Інтернету, зловмиснику буде запропоновано надати дозволи. Цей обхід не призведе до змін конфігурації запису на диск.
- Використання прапору політики виконання «‘Remote-Signed» — це політика за замовчуванням для серверів Windows. Цей прапорець не потребує цифрового підпису на сценаріях, написаних на локальному комп’ютері. Коли він використовується, він запускає сценарії, які завантажуються з Інтернету і не підписуються, лише якщо сценарії розблоковано.
- Вимикання політики виконання, вимкнувши 'AuthorizationManager' - таку функцію можна виконати через інтерактивну консоль або перемикач 'command': function Disable-ExecutionPolicy {($ctx = $executioncontext.gettype().getfield(“_context”,” nonpublic,instance”).getvalue(

$executioncontext)).gettype().getfield(“_authorizationManager”,”nonpublic,instance”).setvalue($ctx, (new-objectManagement.Automation.AuthorizationManager “Microsoft.PowerShell”)) } Disable-ExecutionPolicy .runme.ps1 Ця функція замінить «AuthorizationManager» на null. Це призведе до того, що політика виконання буде встановлена як необмежена для поточного сеансу. Цей обхід не призведе до змін конфігурації запису на диск.

- Встановлення для ExecutionPolicy значення Scope Process. Для процесу, яким ви керуєте, політика виконання може бути необмеженою протягом решти сеансу. Цей обхід не призведе до змін конфігурації запису на диск.
- Встановлення для ExecutionPolicy значення Scope CurrentUser за допомогою перемикача Command. Цей обхід подібний до попереднього, але буде застосовано параметр до середовища поточного користувача шляхом зміни ключа реєстру. Цей обхід не призведе до змін конфігурації запису на диск.
- Встановлення для ExecutionPolicy значення Scope CurrentUser за допомогою реєстру — цей обхід подібний до попереднього, тільки він безпосередньо змінює розділ реєстру.

2. *Виконання скриптів*. PowerShell зазвичай використовуються як завантажувач додаткових корисних даних після фази експлуатації. Політика виконання не дозволить користувачам запускати сценарії з розширенням .ps1, але зловмисники можуть використовувати інші розширення для виконання своїх сценаріїв. PowerShell використовує позначки командного рядка, які можна використовувати зловмисно, щоб уникнути виявлення та обійти локальні обмеження. Найбільш часто використовувані шкідливі команди PowerShell і функції в командному рядку:

- *(New-Object System.Net.Webclient).DownloadString()*
- *(New-Object System.Net.Webclient).DownloadFile()*
- *-IEX / -Invoke-Expression*
- *Start-Process*

Клас System.Net Webclient використовується для надсилання або отримання даних з віддалених ресурсів. Цей клас включає метод DownloadFile, який завантажує вміст із віддаленого розташування в локальний файл. Він також включає метод DownloadString, який завантажує вміст із віддаленого розташування до буфера в пам’яті. Після завантаження корисного навантаження для запуску додаткового коду використовується інший метод. Найпоширенішими методами запуску нового процесу з PowerShell є Invoke-Expression і Start-Process. Ось деякі з найпоширеніших способів зараження:

- Прапори. Зловмисники використовують цю змінну середовища, щоб приховати сценарій від реєстраторів командного рядка.
- Електронні листи – дуже часто використовуються як вектор доставки для завантажувачів PowerShell. Зловмисники використовують соціальну інженерію, щоб обманом змусити користувача відкрити вкладений файл і активувати його вміст. Якщо користувач відкриває вкладені файли, запускається сценарій PowerShell.
- Nemucod downloader - троян, який завантажує шкідливі файли на заражений комп'ютер
- Макроси Office – використання шкідливих макросів у документах Office. Зловмисники використовують електронні листи, щоб обманом змусити користувача ввімкнути та виконати макрос у вкладенні, а макрос видаляє сценарій PowerShell.

3. *Розширення доступу та горизонтальне переміщення*. Методи бічного переміщення дозволяють зловмисникам поширюватися в середовищі з одного скомпрометованого комп’ютера. Зловмисники використовують віддалені команди PowerShell для горизонтального поширення. Бічне переміщення залежить від конфігурації комп’ютера та дозволів користувача. Ось деякі з найбільш часто використовуваних методів бокового переміщення PowerShell.

- Invoke-command – Invoke-Command дозволяє запускати сценарії PowerShell на віддалених комп’ютерах. Зловмисник може як надати, так і виконати команду на кількох віддалених комп’ютерах паралельно.

- Enter-PSSession – команда PSSession дозволяє інтерактивний віддалений сеанс PowerShell, який користувач може використовувати для віддаленого виконання команд. Цей параметр залежить від служби віддаленого керування Windows (WinRM). WinRM має бути ввімкнено, щоб використовувати цей метод.
- WMI-WMI можна використовувати для запуску програми на віддалених комп'ютерах. Він не обмежується сценаріями PowerShell, але його легко використовувати для цієї мети.
- Ін'єкція профілю – якщо зловмисник має права «запису» у файли профілю PowerShell на віддаленому комп'ютері, він може додати до них шкідливий код. Використання системних або публічних інструментів, таких як Task Scheduler, PsExec і Mimikatz.

4. *Закріплення.* Створення постійних точок завантаження, які перезапускають бекдор, є поширеним методом для зловмисників, щоб зберегти свою присутність у мережі. Ці точки завантаження активуються щоразу, коли Windows перезавантажується. Ось кілька поширених методів, які використовують PowerShell для підтримки постійності в мережі:

- Реєстр: зловмисники зберігають сценарій у реєстрі, що робить зараження повністю безфайловим і їхню атаку важко виявити. Доступ до реєстру також дозволить зловмиснику встановити політику виконання. Це, мабуть, найпоширеніша точка навантаження.
- Заплановані завдання - зловмисник може створити завдання, яке буде запущено в певний момент і виконає команду PowerShell.
- Папка автозавантаження – папка автозавантаження дозволяє користувачеві автоматично запускати певний набір програм під час запуску Windows. Невеликий файл сценарію можна розмістити в папці автозавантаження, який буде виконано після перезавантаження Windows.
- WMI- WMI є потужним у поєднанні з PowerShell. Зловмисник може створити фільтр для певної події, яка підтримуватиметься споживацьким методом для

виконання шкідливого сценарію. Його можна використовувати як локально, так і віддалено.

- Групові політики (GPO) – змінюючи існуючі політики, зловмисники можуть використовувати GPO для додавання точки завантаження для сценарію бекдора PowerShell.
- Інфікування локальних профілів – зловмисник може розмістити шкідливий код в одному з шести профілів PowerShell або створити власний профіль. Код буде виконано під час запуску PowerShell[11].

1.3 Внутрішні кібератаки на кінцеві пристрої корпоративної мережі

Атака watering hole (атака водопою). Незалежно від того, чи йдеться ви про кібербезпеку чи джунглі, атака на водопою – це коли загрозливі суб'єкти вражають свої цілі там, де вони збираються. У дикій природі водопій — це природне поглиблення води, куди спраглі тварини приходять напитися. Без великої уваги під час водопою вони стають легшою здобиччю для таких мисливців, як леви. Це схожа концепція в кібербезпеці, за винятком того, що замість великих котів і газелей це хакери, які переслідують користувачів комп'ютерів у мережі. Атаки на водопій працюють наступним чином. Атака на водопою – це коли кіберзлочинці атакують окремих осіб, когорти чи організації на веб-сайті, який вони відвідують, використовуючи такі навички, як хакерство та соціальна інженерія[12]. Крім того, зловмисник може заманити жертву (жертв) на створений ними веб-сайт. Атаки вимагають ретельного виконання на всіх чотирьох наступних етапах:

- Збір розвідувальної інформації. Зловмисник збирає інформацію, відстежуючи звички веб-перегляду своєї цілі. Загальні інструменти для збору розвідувальних даних включають пошукові системи, сторінки соціальних мереж, демографічні дані веб-сайтів, соціальну інженерію, шпигунське програмне забезпечення та кейлоггери. Іноді загальні знання дуже допомагають. Наприкінці

цього етапу кіберзлочинці мають веб-сайт короткий список цілей, які можна використовувати для кібератаки.

- Аналіз. Кіберзлочинці аналізують список веб-сайтів на предмет недоліків домену та субдомену, якими вони можуть скористатися. Крім того, зловмисники можуть створити шкідливий клон веб-сайту. Іноді вони роблять і те, і інше — скомпрометують легітимний веб-сайт, щоб він перевів ціль на фальшивий.
- Підготовка. Хакери впроваджують на веб-сайт веб-експлойти, щоб заразити свої цілі. Такий код може використовувати такі веб-технології, як ActiveX, HTML, JavaScript, зображення тощо, для компрометації браузерів. Для більш цілеспрямованих атак зловмисники також можуть використовувати набори експлойтів, які дозволяють їм заражати відвідувачів певними IP-адресами. Ці набори експлойтів особливо корисні, якщо зосередитися на організації.
- Виконання. З готовим водопоєм зловмисники чекають, поки зловмисне програмне забезпечення виконає свою роботу. Якщо все йде добре, цільові браузери завантажують і запускають шкідливе програмне забезпечення з веб-сайту. Веб-браузери можуть бути вразливими до експлойтів через Інтернет, оскільки вони зазвичай без розбору завантажують код із веб-сайтів на локальні комп’ютери та пристрої. Методи використовують хакери для атак на водопою. Міжсайтовий сценарій (XSS): за допомогою цієї ін’єкційної атаки хакер може вставляти шкідливі сценарії у вміст сайту, щоб перенаправляти користувачів на шкідливі веб-сайти. Впровадження SQL: хакери можуть використовувати атаки впровадження SQL для викрадення даних. Отруєння кеш-пам’яті DNS: хакери використовують цю техніку маніпулювання, щоб надсилати цілі на шкідливі сторінки. Миттєві завантаження: цілі можуть завантажувати зловмисний вміст без їх відома, згоди чи дії під час мимовільного завантаження. Шкідлива реклама: відома як шкідлива реклама, хакери вводять шкідливий код у рекламу, щоб поширити шкідливе програмне забезпечення на свою жертву. Експлуатація нульового дня: суб’єкти загрози можуть

використовувати вразливості нульового дня на веб-сайті чи в браузері, якими можуть скористатися зловмисники.

Атаки на постачальників. Хоча атаки на водопій та атаки на ланцюги поставок можуть бути схожими, вони не завжди однакові. Атака на ланцюг постачання доставляє зловмисне програмне забезпечення через найслабший елемент у мережі організації, як-от постачальника, постачальника чи партнера. Атака на ланцюжок поставок також може використовувати скомпрометований веб-сайт як джерело, але це необов'язково. Зловмисники шукають незахищені мережеві протоколи, незахищені серверні інфраструктури та небезпечні методи кодування. Вони зламують, змінюють вихідні коди та ховають зловмисне програмне забезпечення в процесах створення й оновлення. Оскільки програмне забезпечення створено та випущено перевіреними постачальниками, ці програми та оновлення підписані та сертифіковані. Під час атак на ланцюг постачання програмного забезпечення постачальники, ймовірно, не знають, що їхні програми чи оновлення заражені шкідливим кодом, коли вони оприлюднюються. Потім шкідливий код запускається з тими ж правами довіри та дозволами, що й програма. Кількість потенційних жертв є значною, враховуючи популярність деяких програм. Типи атак на ланцюги поставок:

- Зламані інструменти створення програмного забезпечення або оновлена інфраструктура;
- Викрадені сертифікати кодового підпису або підписані зловмисні програми за допомогою ідентичності компанії-розробника;
- Зламаний спеціалізований код, доставлений у компоненти обладнання чи мікропрограми;
- Попередньо встановлене шкідливе програмне забезпечення на пристроях (камерах, USB, телефонах тощо)[13].

Приклад складної атаки на ланцюг поставок:

1. Зловмисник виявляє великі організації за допомогою компонента з відкритим кодом, створеного певною групою розробників;

2. Зловмисник ідентифікує розробника, який не активно працює над проектом, і компрометує його обліковий запис GitHub;

3. Використовуючи скомпрометований обліковий запис GitHub, зловмисник вносить у проект невинний код, який насправді містить бекдор Бекдор включено в наступний випуск;

4. Коли одна з цільових організацій оновлює компонент з відкритим кодом до нової зламаної версії, вони належать зловмиснику;

Ризики, пов’язані з атаками на ланцюги поставок, ніколи не були вищими завдяки новим типам атак, зростаючій обізнаності громадськості про загрози та посиленню нагляду з боку регуляторів. Тим часом зловмисники мають у своєму розпорядженні більше ресурсів та інструментів, ніж будь-коли раніше, створюючи ідеальний шторм.

1.4 Аналіз кібератак на кінцеві пристрої корпоративної мережі

Найпростіший спосіб моніторингу та слідкування за кінцевими пристроями це в корпоративній мережі. Наприклад якщо інфраструктура побудована на Windows OS, то навіть Active Directory дозволяє це зробити легко та зручно. Але цього зовсім недостатньо коли пристрій знаходится за межами контрольованої мережі. Саме з такими проблемами стикнулися підприємства під час обмеженнь через Covid-19.

Згідно звіту Ponemon Institute LLC[14] ефективність забезпечення безпеки підприємств знизилась з середніх 71% до 44%. Майже в половину підприємства втратили змогу захищатися від атак зловмисників та шахраїв. Саме фактор різкого обмеження став основним у таком знижені ефективності команд безпеки компанії. Також через обмеження доволі сильно зросла кількість запитів до критичних додатків компанії. Що додатково збільшило навантаження на IT-інфраструктури підприємств.

Через нестачу інструментів забезпечення захисту віддалених працівників час реакції на загрози збільшився у 35% компаній, що також є доволі високим показником.

Епідемія Covid-19 зробила дуже великий внесок в побудову захисту кінцевих пристроїв та організації роботи віддалених працівників. Саме через обмеження в переміщенні потрібно було мати інструменти моніторингу безпеки кінцевих пристроїв та швидкої реакці на загрози безпеці ресурсів компанії. Після початку Covid-19 більше половини компанії стикнулися з шкідливим програмним забезпеченням яке обійшло їх системи детектування вторгнень, рисунку 1.3.

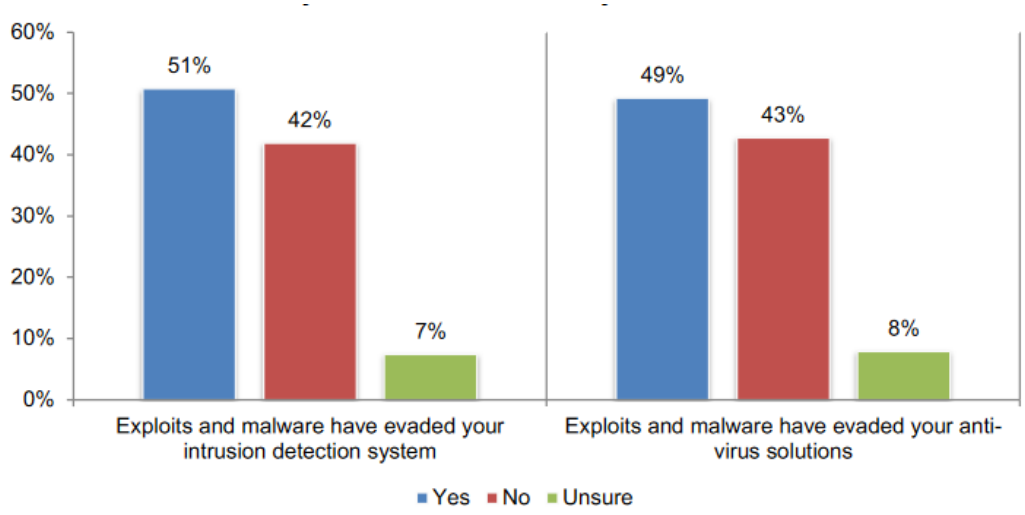

Рис. 1.1. Статистика обходу IPS/Antivirus[15]

У 2020 році 49% компаній стикнулися з тим, що шкідливе програмне забезпечення не було задетектовано їх засобами Anti-virus.

За 2021 рік 53% компаній були атаковані програмами вимогачами, про це свідчить звід від Black Kite[16].

Через несприятливі чинники епідемії та недостатньої готовності підприємств до різкого збільшення віддалених працівників, зловмисники досягли доволі великих успіхів у зламі кінцевих пристроїв. Збільшення навантаження на інфраструктуру компаній та неможливість швидко реагувати на загрози зумовила негативну статистику захисту кінцевих пристроїв компаній. Саме через великий ландшафт

загроз, велику кількість усіляких атак на кінцеві пристрої та неможливість бачити усю інфраструктуру зумовили прекрасні умови для нападу на підприємства у період Covid-19.

Висновки до першого розділу

Проаналізовано атаки на кінцеві пристрої. Визначено підкатегорії згідно з типами атак.

Окреслено що внутрішні, що зовнішні атаки становлять велику загрозу якщо будуть успішними. Так як корпоративні пристрої мають доступ до чутливої інформації, то отримання доступу до них зловмисниками може принести великі збитки. Встановлено, що розуміння атак допомагає зменшити поверхню атак, а згідно зменшити ризик захоплення кінцевого пристрою зловмисником.

Досліджено звіти щодо зламу кінцевих пристроїв. Визначено як саме вплинула епідемія Covid-19 та чому у компаній знизилась захистна спроможність.

Встановлено чиники які спричинили зниження захисту. Підкреслено, що ці чиники можуть бути змінені або виправлені, щоб у кінці отримати захищені кінцеви пристрої та захищену корпоративну мережу.

2 АНАЛІЗ ФУНКЦІЙ ТА МОЖЛИВОСТЕЙ ЗАСОБІВ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК НА БАЗІ FORTICLIENT EMS, А ТАКОЖ FORTINET SECURITY FABRIC

2.1 Агент Forticlient

FortiClient – це додаток який встановлюється на кінцевий пристрій. FortiClient забезпечує комплексний захист кінцевих точок для Windows, Mac і Linux. Настільні ПК, ноутбуки, файлові сервери та мобільні пристрої, такі як iOS та Android.

Це допомагає захистити системи з передовими технологіями безпеки, усіма якими можливо керувати з єдиної консолі керування. FortiClient дозволяє будь-якому пристрою — локальному чи віддаленому, стаціонарному чи мобільному — інтегруватися з FortiClient EMS (Enterprise Management Server далі EMS) і FortiGate.

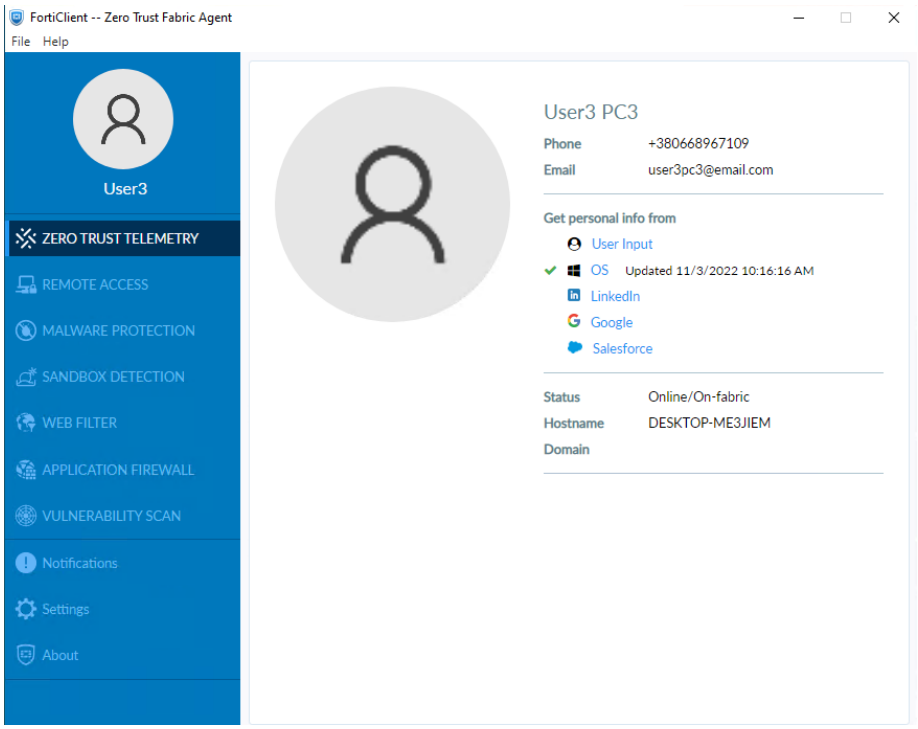

Рис. 2.1. Сторінка за замовчуванням агента Forticlient

FortiClient підтримує Windows, Mac OS, Linux, iOS, мобільні пристрої Android і hromebook, а також інтегрує домашні офіси, мобільних працівників і партнерів до єдиної платформи керування. Панель керування Forticlient зображена на рис.2.1

FortiClient необхідно використовувати з FortiClient EMS. FortiClient має підключитися до FortiClient EMS, щоб активувати ліцензії та отримати профіль кінцевої точки, який адміністратор може налаштувати у FortiClient EMS. Неможливо використовувати жодні функції FortiClient, доки FortiClient не буде підключено до FortiClient EMS і не буде ліцензовано. Коли FortiClient підключено лише до FortiClient EMS, FortiClient EMS надає FortiClient і керує ним. FortiClient EMS також надсилає правила нульової довіри до FortiClient і використовує результати FortiClient для динамічно групувати кінцеві точки в EMS. Тільки FortiClient EMS може контролювати з'єднання між FortiClient і FortiClient EMS. Однак FortiClient не може брати участь у Fortinet Security Fabric. FortiClient у структурі безпеки підключається до FortiClient EMS, щоб отримати профіль інформації про конфігурацію частина політики кінцевої точки. FortiClient EMS підключено до FortiGate для участі в единії системі захисту - Security Fabric. FortiClient EMS надсилає інформацію про кінцеву точку FortiClient до FortiGate. FortiGate також може отримувати динамічні списки груп кінцевих точок із FortiClient EMS і використовувати їх для створення динамічних політик брандмауера. FortiClient автоматизує запобігання відомим і невідомим загрозам за допомогою вбудованого стека безпеки на базі хосту та інтеграція з FortiSandbox. FortiClient також забезпечує безпечний віддалений доступ до корпоративних активів через VPN.

FortiClient EMS - FortiClient EMS працює на сервері Windows. EMS керує кінцевими точками FortiClient за допомогою розгортання FortiClient (Windows) і політик кінцевих точок на кінцевих точках, і кінцеві точки можуть підключити FortiClient Телеметрія до EMS. Кінцеві точки FortiClient можуть підключатися до EMS для участі в Security Fabric. FortiClient кінцеві точки підключаються до EMS для керування в режимі реального часу. Панель керування зображена на рис.2.2. Також Forticlient EMS має хмарну версію. Хмарна версія коштує трохи більше, але надалі ці

витрати виправдовуються, тому що платформу буде тримати сам Fortinet. Це доволі просте та дієве рішення для невеликих компанії.

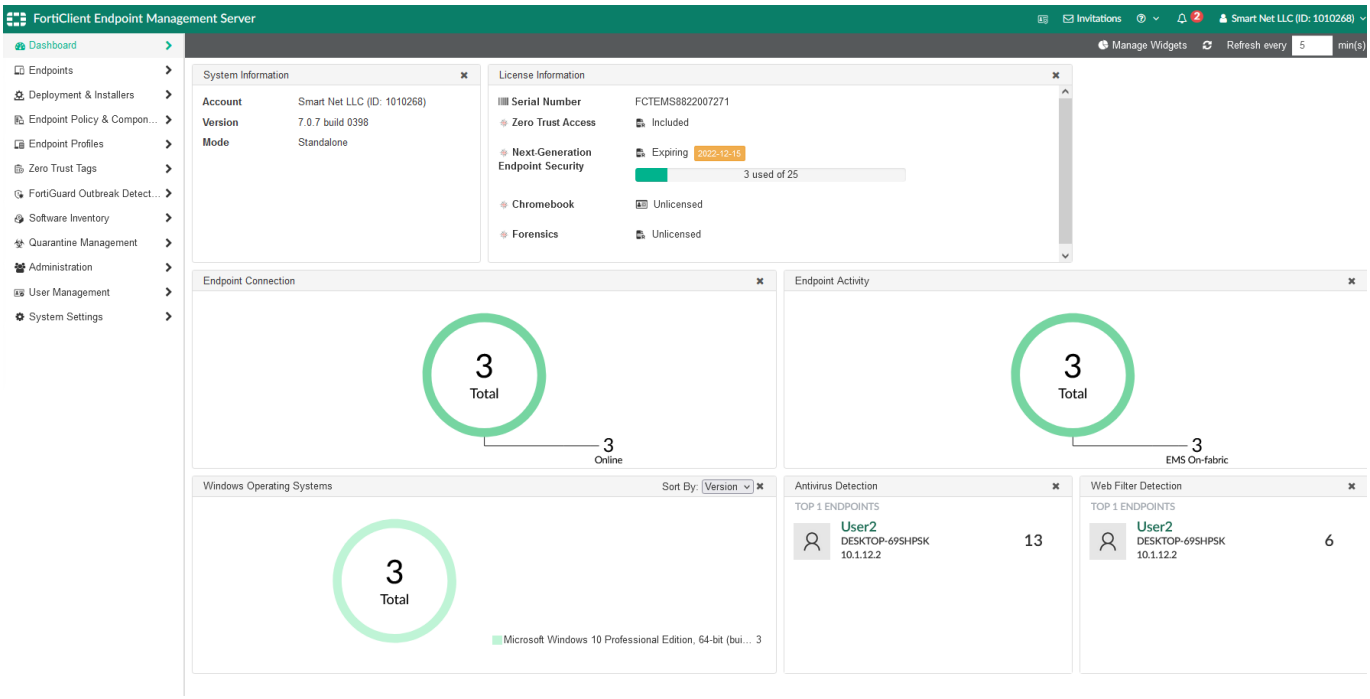

Рис. 2.2. Панель керування EMS

FortiGate - FortiGate забезпечує безпеку мережі. EMS визначає правила перевірки відповідності для підключених кінцевих точок і передає правила кінцевим точкам і FortiGate. FortiGate використовує правила та інформація щодо кінцевих точок від EMS для динамічного налаштування політик безпеки. Панель керування Fortigate версії 7.2.2 зображений на рис.2.3.

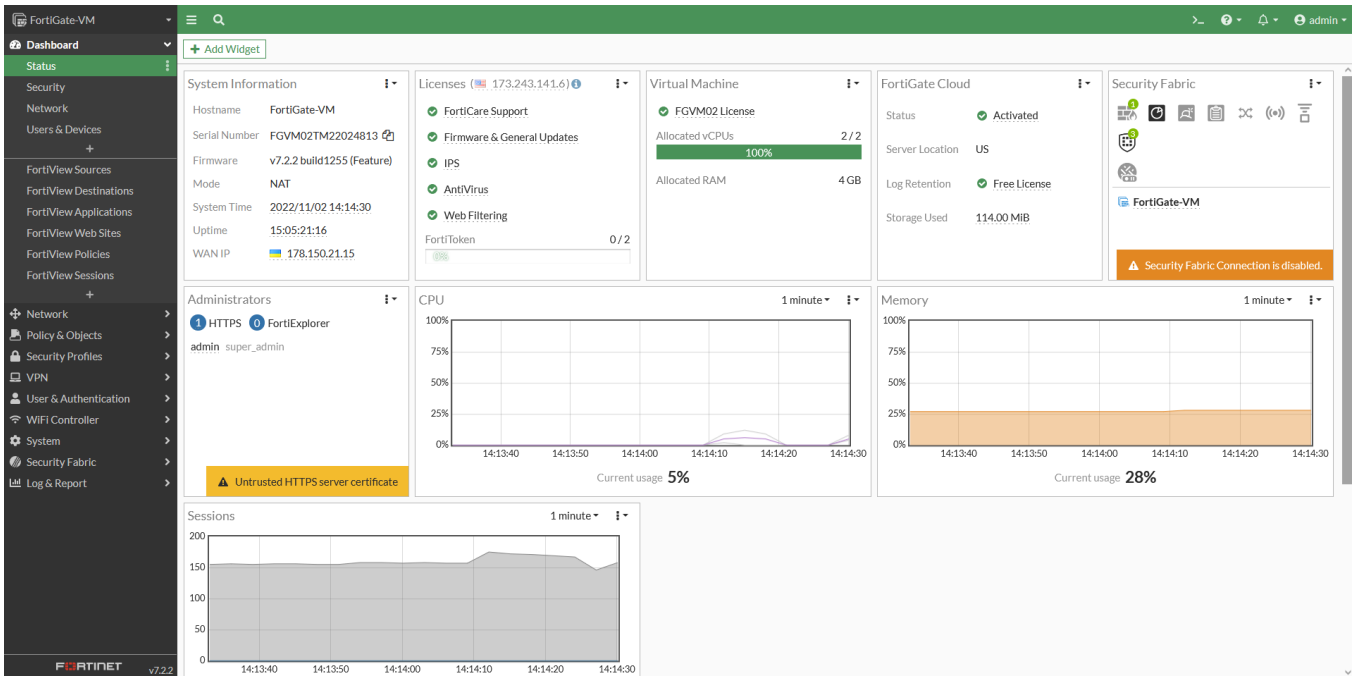

Рис.2.3. Панель керування Fortigate

Інтеграція FortiClient Security Fabric забезпечує видимість кінцевої точки за допомогою телеметрії та гарантує, що вся мережа компоненти, FortiGate, FortiAnalyzer, EMS, керовані точки доступу, керовані комутатори та FortiSandbox мають уніфікований перегляд кінцевих точок, щоб забезпечити відстеження та обізнаність, забезпечення відповідності та звітування. Безпечне віддалене підключення забезпечується традиційними тунелями VPN або новими автоматичними тунелями ZTNA. FortiClient доступний у чотирьох різних версіях:

- ZTNA (Zero Trust Network Access - доступ до мережі без довіри)
- EPP/APT (Endpoint Protection Platform/Advanced Persistent Threat)
- Керована служба
- Chromebook

У таблиці 2.1 наведено порівняння функцій чотирьох версій Forticlient.

Таблиця 2.1

Порівняння версій Forticlient за функціоналом.

	VPN/ZTNA	EPP/APT	Керована Служба	Chrome
Zero Trust Network Access	так	так	так	ні
Централізоване керування за допомогою FortiCloud	так	так	так	так
Централізоване керування та звітність	так	так	так	так
SSL VPN та багатофакторна авторизація	так	так	так	ні
IPsec VPN та багатофакторна авторизація	так	так	так	ні
SSO Мобільний агент	так	так	так	ні
Агент слідкування за вразливостями	так	так	так	ні
Веб-фільтрація	так	так	так	так
Керування USB пристроями	так	так	так	ні
FortiSandBox	так	так	так	ні
FortiClient хмарний SandBox	ні	так	так	ні
AI Антивірус	ні	так	так	ні
Automated Endpoint Quarantine	ні	так	так	ні
Ransomware Protection	ні	так	так	ні
Endpoint On-boarding	ні	ні	так	ні
Initial Provisioning	ні	ні	так	ні
Security Fabric Setup/Integration	ні	ні	так	ні
Vulnerability Monitor	ні	ні	так	ні
Endpoing Security Monitoring	ні	ні	так	ні

FortiClient ZTNA працює з FortiOS, щоб забезпечити безпечний детальний доступ до програм, незалежно від того, чи є користувач зареєстрований у EMS або ні. Кожен сеанс ініціюється за допомогою автоматичного зашифрованого тунелю від FortiClient до FortiOS проксі-точки для перевірки користувача та пристрою. Якщо

перевірено, доступ надається для цього сеансу. Двофакторний автентифікацію також можна використовувати для забезпечення додаткового рівня безпеки. З ZTNA організації виграють як від кращого рішення для віддаленого доступу, так і від узгодженої політики для контрольованого доступу до програм і поза мережею.

FortiClient EPP/APT: містить усі функції, описані для ліцензії Zero Trust Network Access (ZTNA), а також антивірус (AV), antiransomware програмне забезпечення, антиексплойт, хмарне виявлення шкідливих програм, брандмауер програм, інвентаризація програмного забезпечення та розширений захист від загроз через FortiClient Cloud Sandbox.

Керована служба включає всі функції, детально описані для версій ZTNA та EPP, а також початкове хмарне налаштування FortiClient та налаштування його хмарного середовище FortiClient, налаштування та інтеграція системи безпеки та моніторинг уразливості кінцевої точки

Chromebook: ліцензія дозволяє керувати одним користувачем Google Chromebook. Якщо кількість Chromebook якими керує EMS, перевищує кількість доступних ліцензій Chromebook, будь які доступні ліцензій Fabric Agent можуть бути використані для розширення.

2.2 FortiClient Enterprise Management Server

FortiClient EMS — це рішення для керування безпекою, яке забезпечує масштабоване та централізоване керування кілька кінцевих точок (комп’ютерів). EMS також забезпечує ефективне та ефективне адміністрування запущених кінцевих точок FortiClient і видимість у мережі для безпечного обміну інформацією та призначення профілів безпеки кінцеві точки. EMS створений для максимального підвищення ефективності роботи та включає автоматизовані можливості для пристрою управління та усунення несправностей. FortiClient EMS також працює з розширенням FortiClient Web Filter для забезпечення веб-фільтрації для користувачів Google Chromebook.

Перевагами розгортання FortiClient EMS є :

• Віддалене розгортання програмного забезпечення FortiClient на комп’ютерах Windows;

• Оновлення профілів для кінцевих користувачів незалежно від місця доступу Адміністрування з’єднань кінцевих точок FortiClient, наприклад прийняття, роз’єднання та блокування з'єднання;

• Управління та моніторинг кінцевих точок, таких як інформація про стан, систему та підпис;

• Виявлення застарілих версій програмного забезпечення FortiClient;

• Визначення правил веб-фільтрації в профілі та віддалене розгортання профілю у FortiClient Web Filter, розширення на кінцевих точках Google Chromebook. Можливо керувати безпекою кінцевої точки для платформ Windows і macOS за допомогою уніфікованої організаційної безпеки політики. Політика безпеки організації забезпечує повне, зрозуміле уявлення про політики безпеки, визначену в організації. Можливо переглянути всі правила політики, призначення та винятки в єдиному уніфікованому поданні. FortiClient EMS є частиною пакету Fortinet Endpoint Security Management, який забезпечує комплексну політику адміністрування та забезпечення виконання корпоративної мережі.

FortiClient EMS складається з наступних компонентів:

• FortiClient EMS: керує FortiClient на кінцевих точках, які підключаються до корпоративоної мережі підприємства. Він також керує Розширення FortiClient Web Filter, встановлене на кінцевих точках Google Chromebook, підключених до домену Google. Він включає два типи програмного забезпечення: Консольне програмне забезпечення, яке керує профілями безпеки, FortiClient на кінцевих точках і кінцевих точках Chromebook та серверне програмне забезпечення, яке забезпечує безпечний зв’язок між кінцевими точками та консоллю, а також між кінцевими точками Chromebook і консоль адміністратора Google;

• База даних: зберігає профілі безпеки та події. Також зберігає інформацію про користувача, отриману від Google Консоль адміністратора для Chromebook. База даних SQL інсталюється як частина інсталяції FortiClient EMS;

• FortiClient: допомагає посилити безпеку та захист кінцевих точок. FortiClient працює на серверах, настільних і портативних комп'ютерах комп'ютери, які будуть захищатися;

• Розширення FortiClient Web Filter: взаємодіє з FortiClient EMS і забезпечує веб-фільтрування Кінцеві точки Google Chromebook.

Для того щоб EMS розумів стан кінцевої точки, Forticlient агент збирає певні дані – телеметрію та передає на сервер. Коли FortiClient Telemetry підключено до EMS, FortiClient збирає інформацію про апаратне забезпечення (MAC адреси), інформацію про програмне забезпечення (версія ОС на кінцевій точці), ідентифікаційну інформацію (ім'я користувача, аватар, і ім'я хоста), а також інформацію про вразливості, яку модуль сканування вразливостей повідомляє про кінцеву точку і його навантаження, і надсилає його до EMS. Коли EMS бере участь у Security Fabric, Security Fabric використовує інформацію для розуміння кінцевої точки та її робочого навантаження для кращого захисту. Після встановлення FortiClient автоматично запускається та підключає телеметрію до створеного сервера EMS встановлений пакет розгортання. Також можливо вручну ввести IP-адресу EMS або код запрошення. Коли підтверджується телеметричне підключення до EMS, можна наказати FortiClient запам'ятати IP-адреса EMS. Якщо потрібен ключ підключення, FortiClient також запам'ятовує ключ підключення. FortiClient може запам'ятати до 20 IP-адрес для EMS. Коли на FortiClient вказана опція забути IP-адресу для EMS, FortiClient Telemetry не використовує IP-адресу адреса для автоматичного підключення до EMS під час повторного підключення до мережі. Для підключення FortiClient до іншого EMS потрібно відключити FortiClient Телеметрія від EMS для підключення до іншого EMS або для вимкнення та видалення FortiClient.

У FortiClient 7.0.0 відповідність залежить від FortiClient EMS і FortiOS. Функція збору телеметрії доступна, лише якщо використовується FortiClient 7.0.0 із FortiClient EMS 7.0.0 і FortiOS 7.0.0. Через внесення змін до ліцензії, не можна мати середовище з змішанними версіями. Адміністратор може визначити правила перевірки відповідності на FortiClient EMS на основі критеріїв, таких як сертифікати, домен для входу в систему, наявні файли, версії ОС, запущені процеси та ключі реєстру. Коли кінцева точка FortiClient реєструється на FortiClient EMS, FortiClient EMS динамічно групує кінцеву точку на основі про правила перевірки відповідності. FortiOS може отримувати динамічні групи кінцевих точок від FortiClient EMS і використовувати їх для створення динамічних політик брандмауера. Кінцева точка може не мати доступу до мережі якщо правила перевірки відповідності не налаштовані. Правила підключення ZTNA на FortiClient створюють безпечне зашифроване підключення до захищених програм без за допомогою VPN. FortiClient використовує функцію проксі-сервера пристрою FortiGate для створення безпечного з'єднання через HTTPS за допомогою сертифіката, отриманого від EMS, який містить UID FortiClient. FortiGate діє локальний проксі-шлюз. FortiGate отримує UID, щоб ідентифікувати пристрій і перевірити іншу інформацію про кінцеву точку, яку надає EMS FortiGate, який може містити іншу інформацію про особу та позицію. FortiGate дозволяє або забороняє доступ за налаштуванням. Для налаштування доступу не веб-додатків потрібно сконфігурувати наступне:

- Назва правила: дозволяє ввести бажану назву правила;
- Хост призначення: дозволяє ввести IP-адресу або FQDN і номер порту призначення хост/сервер;
- Проксі-шлюз: дозволяє ввести IP-адресу та номер порту доступу пристрою FortiGate;
- Режим: дозволяє вибрати прозорий режим для підключення.

FortiClient має розширені можливості для виявлення шкідливих програм. Захист включає антивірусний захист, захист від програм-вимагачів, захист від шкідливих

програм у хмарі, захист від експлойтів і доступ до знімних USB пристроїв. В антивірусі FortiClient, коли функцію ботнету включена, FortiClient відстежує та порівнює мережевий трафік на скомпрометованій системі зі списком відомих командних і контрольних серверів і блокує доступ. Функція захисту в реальному часі у FortiClient використовує тісну інтеграцію з Microsoft Windows для моніторингу файлів локально або через мережеву файлову систему, коли вони завантажуються, зберігаються, запускаються, копіюються, перейменовуються, відкрито або написано. FortiClient може сканувати системні файли, виконувані файли, знімні носії, файли динамічної бібліотеки (DLL), пам'ять, і драйвери. FortiClient також сканує та видаляє руткіти. Файлове шкідливе програмне забезпечення, шкідливі веб-сайти, Захист URL-адрес від фішингу та спаму є частиною антивірусного компонента.

Після реєстрації FortiClient в EMS налаштування конфігурації Web Filter надсилаються на керований пристрій і доступні лише для читання на консолі FortiClient. Функції веб-фільтра дозволяють блокувати, дозволяти, попереджати та відстежувати веб-трафік на основі категорії URL-адреси чи налавштовуванного URL-фільтра. Категоризація URL-адрес виконується FDN. Можно створити спеціальний список виключень фільтра URL-адрес, яка перекриває категорію FDN. Адміністратор EMS може ввімкнути плагін веб-браузера для веб-фільтрації HTTPS на кінцевій точці. Це покращує виявлення та застосування правил Web Filter на сайтах HTTPS. Після ввімкнення цієї опції необхідно відкрити браузер, щоб підтвердити встановлення нового плагіна. Плагін підтримується лише для Google Браузер Chrome на платформах Windows.

FortiClient підтримує як IPsec, так і SSL VPN-підключення до корпоративної мережі для віддаленого доступу. FortiClient Адміністратор EMS може надати підключення VPN клієнта в профілі FortiClient (профіль кінцевої точки EMS) або користувач кінцевої точки може налаштувати нові підключення на консолі FortiClient. Також можна налаштувати двофакторну автентифікацію за допомогою FortiToken для підвищення безпеки для обох типів VPN на пристрої FortiGate для підключень

FortiClient VPN. Функції FortiClient VPN не обмежуються базовою конфігурацією та підготовкою, але їх можна використовувати для розширених конфігурації. Наприклад, можна автоматично підключитися до VPN під час запуску FortiClient або можливо зіставити або скасувати під'єднання мережевого диска, коли тунель підключено або відключено відповідно. Також можливо налаштувати FortiClient для підключення до VPN до входу в систему (або під час входу в Windows або через середовище AD).

Розширені функції, як-от надлишковий IPsec VPN і на основі пріоритетів SSL VPN також підтримується FortiClient для Windows і Mac OS. Приклад панелі підключення до віддаленого ресурсу компанії зображений на рис.2.4.

Рис.2.4. Приклад підключення SSL-vpn з'єднання

Можливо використовувати функцію брандмауера програм для виявлення та вжиття заходів проти мережевого трафіку, залежно від програми, яка генерує трафік. Брандмауер програм використовує для аналізу декодери протоколу IPS і виявляти трафік додатків, навіть на нестандартних портах. FortiClient може розпізнавати трафік, створений великою кількістю програм. Можливо створити правила для блокування

або дозволити трафік програми на FortiGate або EMS залежно від категорії або програми. Тоді правила будуть надіслані до керованого FortiClient. Параметри брандмауера програми доступні лише для читання на консолі FortiClient. Можна переглянути заблоковані програми за останні сім днів.

Коли користувачі кінцевої точки передають дані через Інтернет, хакери можуть використовувати вразливі місця в кінцевій точці пристроїв і використовувати ці вразливості для отримання несанкціонованого доступу до системи. FortiClient може виконувати сканування вразливостей для пошуку вразливостей на кінцевих пристроїв, щоб виявити слабкі місця та надати деталі про вплив цих недоліків і рекомендувати дії для захисту програм, що працюють на кінцевих пристроях. FortiClient зв’язується з FortiGuard Center, щоб отримати оновленні сигнатури. Після завершення сканування FortiClient відображає список уразливостей і деталі.

Висновки до другого розділу

Визначено основні компоненти продукту Forticlient EMS. Проаналізовано Forticlient агент та його основний функціонал. Визначено ліцензії на цей продукт та наведена порівнювальна табличка. Окреслено усі функції, що дає можливість зрозуміти потенціал продукту та його сильні сторони.

Проаналізовано Enterprise Management Server, він дає можливість контролювати кінцеві пристрої, їх налаштування, та забороняти ті чи інші веб-ресурси, додатки і інше. Показано можливість додавати кінцеві пристрої в карантин, що дає змогу швидко реагувати на загрози.

Зазначено сфери використання та які можуть бути контрольовані Forticlient та Enterprise Management Server.

3 ВАРІАНТ ТЕХНОЛОГІЇ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ FORTICLIENT EMS, FORTIGATE А ТАКОЖ FORTINET SECURITY FABRIC

3.1 Моделювання захищенної корпоративної мережі за допомогою Fortigate та Fortinet Security Fabric

Fortinet Security Fabric вирішує згадані вище проблеми безпеки, забезпечуючи широку видимість і контроль усієї цифрової поверхні організації для мінімізації ризиків, інтегроване рішення, яке зменшує складність підтримки кількох продуктів і автоматизований робочий процес для збільшення швидкості роботи. На рисунку 3.1 зображено які саме технології поєднує у собі Fortinet Security Fabric.

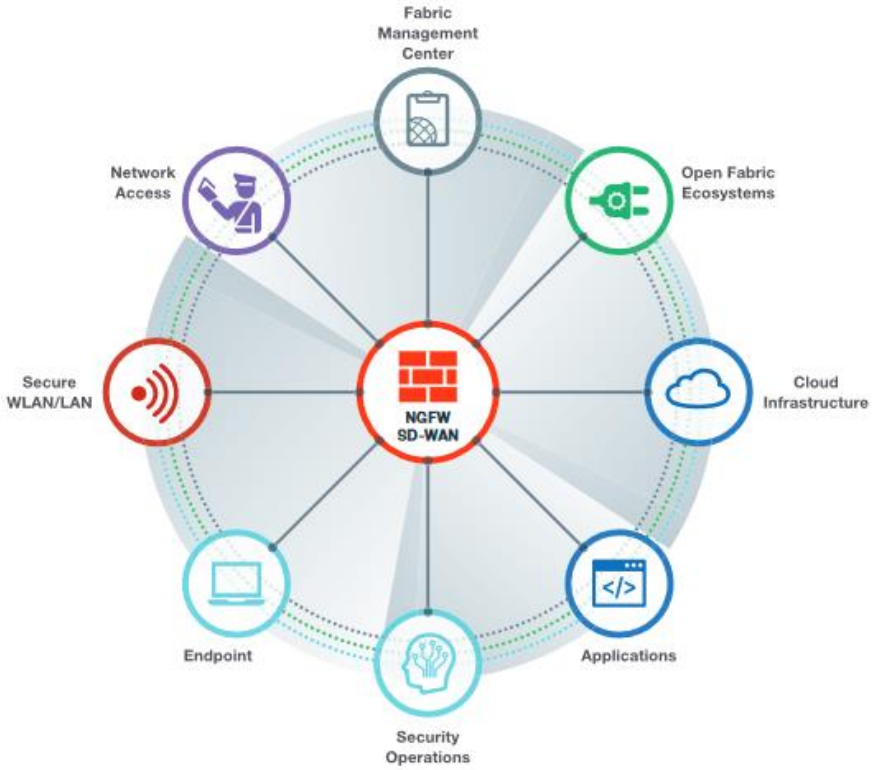

Рис.3.1. Fortinet Security Fabric дає змогу багатьом технологіям безпеки бездоганно працювати разом у всіх середовищах[17]

Оскільки мережа організації розширюються в результаті трансформацій цифрового простору, поверхня атаки також розширюється. Fortinet Security Fabric вирішує завдання розширення поверхні атаки шляхом забезпечення наскрізної безпеки організації і видимість у їхній мережевій інфраструктурі. З найширшим діапазоном високо-продуктивні, безпечні мережеві рішення для центрів обробки даних, філій і малого бізнес, і всіх основних хмарні постачальників, Fortinet Security Fabric гнучка щоб захистити кожен сегмент мережі. Усі компоненти налаштовуються, керуються та контролюються з єдиного центру системи управління. На додаток пов'язаних з точкою інфраструктури безпеки продуктів, єдиний інтерфейс для всіх компонентів безпеки зменшує навантаження та витрати на навчання персоналу. Система управління також полегшує розгортання віддалених компонентів без взаємодії, зниження експлуатаційних витрат.

З усіма компонентами, керованими тією ж мережевою операційною системою FortiOS, Fortinet Security Fabric забезпечує узгоджену конфігурацію та керування політикою і легке спілкування компонентів мережі в режимі реального часу через інфраструктуру безпеки між собою. Це мінімізує час виявлення загроз, зменшує ризики безпеки, що виникають внаслідок помилок конфігурації та ручної компіляції даних, а також сприяє своєчасному та точній відповіді аудиту відповідності. На додаток до інтеграції продуктів і рішень Fortinet, Security Fabric містить готові з’єднання інтерфейсу прикладного програмування для більш ніж 70 існуючих партнерів, які забезпечують глибоку інтеграцію всіх систем безпеки. Для продуктів безпеки, які не є частиною екосистеми Fabric-Ready Partner, API передачі репрезентативного стану і операції розробки (DevOps) сценарії дозволяють легко та швидко додавати інше обладнання до Security Fabric. На додаток до бездоганної інтеграції Fortinet Security Fabric є лідером галузі у застосуванні технологій машинного навчання, щоб не відставати від ландшафт кіберзагроз, що швидко розвивається. Fortinet Security Fabric включає розширені можливості оркестровки безпеки, автоматизації та реагування, а також проактивне виявлення загроз, кореляція

загроз, обмін розвідданими оповіщення, а також дослідження та аналіз загроз. FortiGate NGFW забезпечують найвище співвідношення ціна-якість по скануванню зашифрованого трафіку. Прискорення діяльності з реагування на інциденти також вимагає забезпечення того, щоб персонал служби безпеки не відволікався на інші проблеми, наприклад як збір даних і створення звітів для дотримання нормативних вимог. Ось Fortinet Security Fabric пропонує автоматичне агрегування журналів, кореляцію даних і створення звітів за допомогою вбудованих шаблонів. Рішення для захисту Fortinet Security Fabric надає рішення в п’яти ключових сферах: доступ із нульовою довірою, безпека мереж, динамічна хмарна безпека, операції безпеки на основі штучного інтелекту.

FortiGate NGFW (Next Generation FireWall надалі NGNF) спрощує складність безпеки та забезпечує видимість програм, користувачів і мереж. Вони використовують мету- вбудовані блоки обробки безпеки (SPU - security processing units) і служби аналізу загроз від FortiGuard Labs для забезпечення найвищої оцінки безпеки та високопродуктивний захист від загроз (наприклад, запобігання вторгненням, веб-фільтрація, захист від шкідливих програм, контроль програм) для відомих нападів. Невідомі атаки виявляються та запобігаються локальним і хмарним розширеним захистом від загроз Fortinet рішенням.

Як частина ширшої архітектури Fortinet Security Fabric, FortiGate NGFW використовують автоматизовані відповіді на основі політики щоб прискорити час вирішення. Коли FortiGate NGFW виявляє подію, він зв’язується з Security Fabric, яка визначає, якою інформацією буде ділитися підприємство. Наприклад, коли зловмисне програмне забезпечення виявлено в одній частині організації, Security Fabric ділиться інформацією про загрози з рештою IT-інфраструктури підприємства.

В іншому випадку, коли політика створюється для одного рішення безпеки, Security Fabric може контекстно застосовувати ту саму політику для інших рішення безпеки в архітектурі для послідовного та скоординованого контролю. FortiGate NGFW забезпечує гнучкість розгортання, яке можна адаптувати до конкретних потреб

безпеки підприємства, яке потребує запуск однієї чи кількох функцій безпеки, таких як перевірка SSL/TLS, IPS і антивірус окремо або одночасно з мінімальними зниження продуктивності.

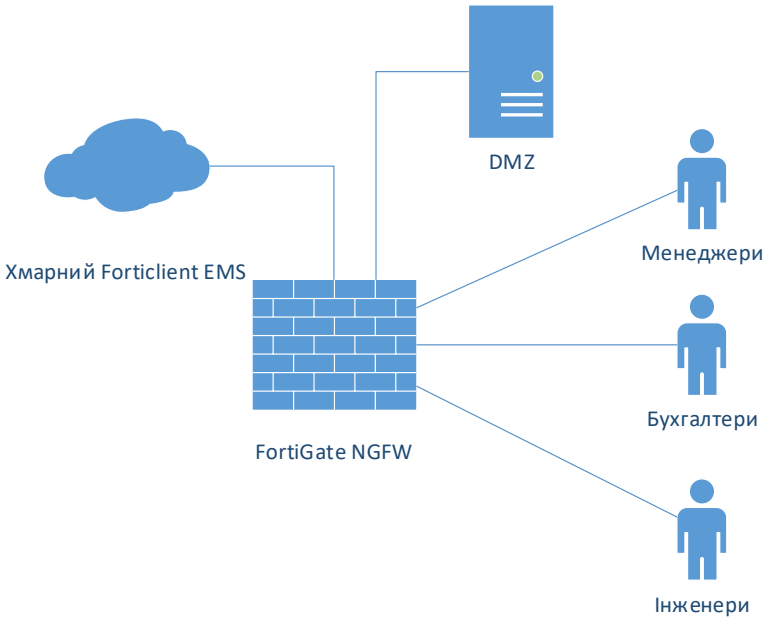

Рис.3.2. Логічна схема мережі підприємства

Усі розгорнуті пристрої FortiGate в мережевій інфраструктурі організації з'єднані між собою через єдину систему безпеки. Ця інтеграція забезпечує комплексний захист у режимі реального часу, спрощуючи розгортання та скорочення потреба в кількох точках дотику та політиках на підприємстві. Логічна топологія мережі підриємства зображена на рис.3.2.

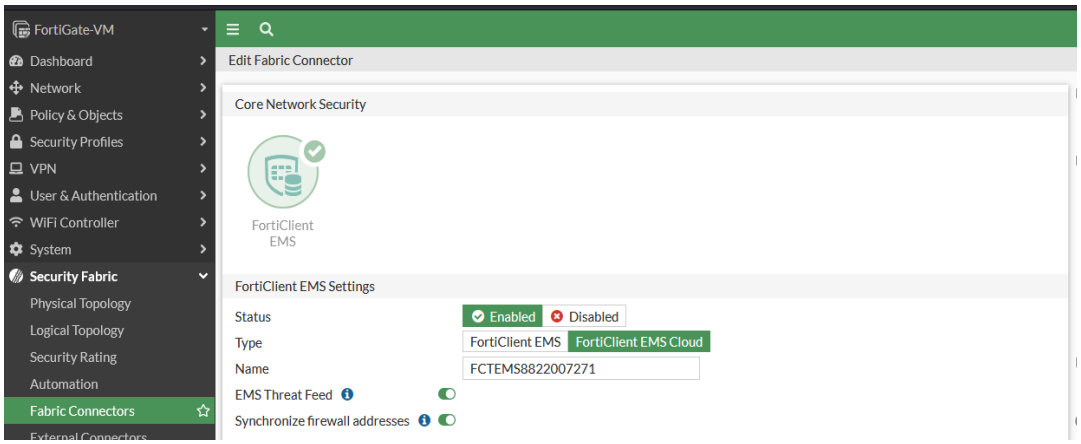

Рис.3.3 Налаштування SecurityFabric

Налаштування взаємодії між FortiClient EMS та Fortigate на Fortigate в Security Fabric зображено на рис.3.3.

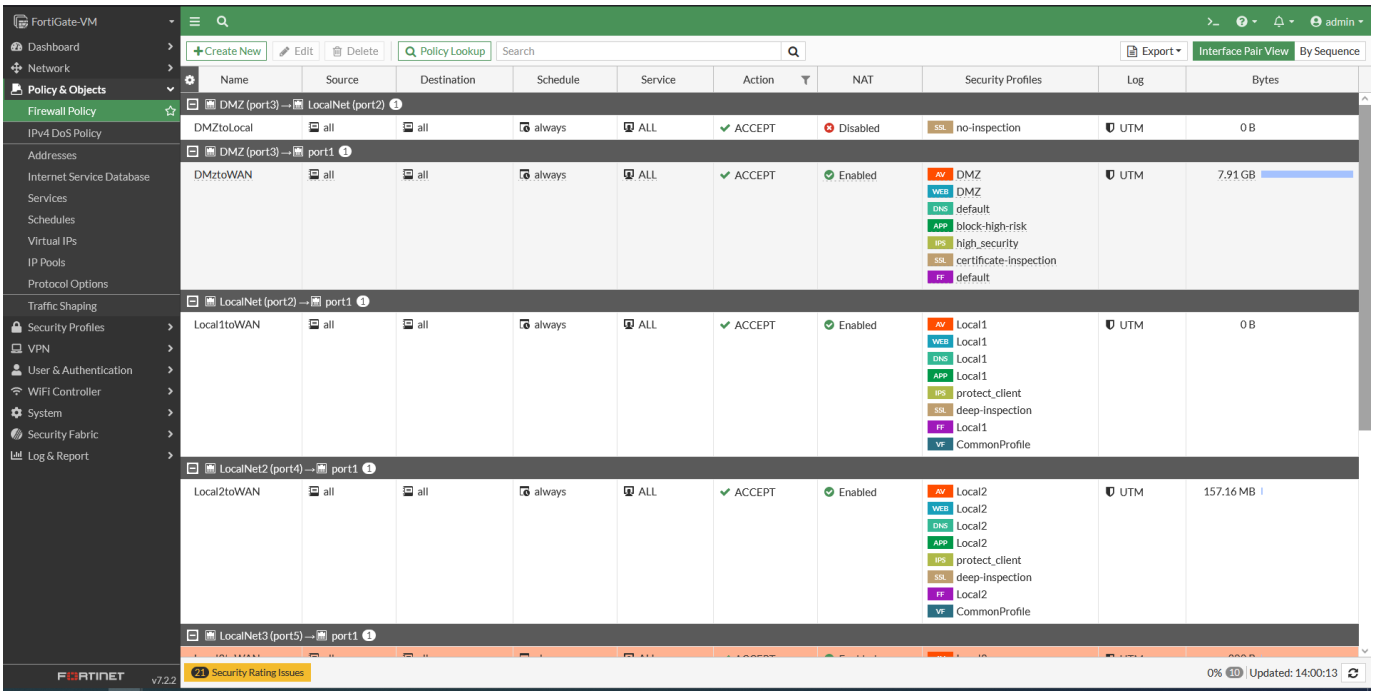

Рис.3.4. Налаштування політик безпеки та профілів безпеки

Одним з найголовніших аспектів безпеки є розмежування доступу та правильне налаштування профілів безпеки для мереж які знаходяться в периметрі захисту. Налаштування політик безпеки та профілів безпеки на Fortigate показано на рис.3.4.

3.2 Налаштування FortiClient та FortiClient EMS

Початок налаштування захисту кінцевих точок здійснюється з встановлення FortiClient на кінцевий пристрій та реєстрацію в Встановлення FortiClient на кінцевий пристрій та реестрація на FortiClient EMS. Типи інсталяторів які пропонує FortiClient EMS зображені на рис.3.5.

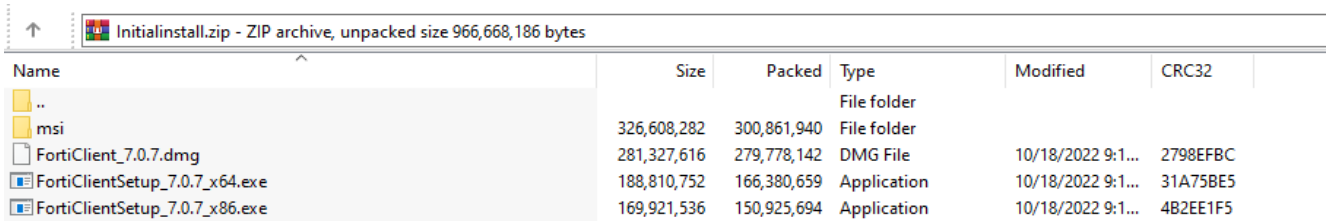

Рис. 3.5. Типи інсталяторів

У архіві маємо інсталятори для архітектури x86 та x64, msi формат для встановлення FortiClient за допомогою AD, а також dmg формат для встановлення на MacOS.

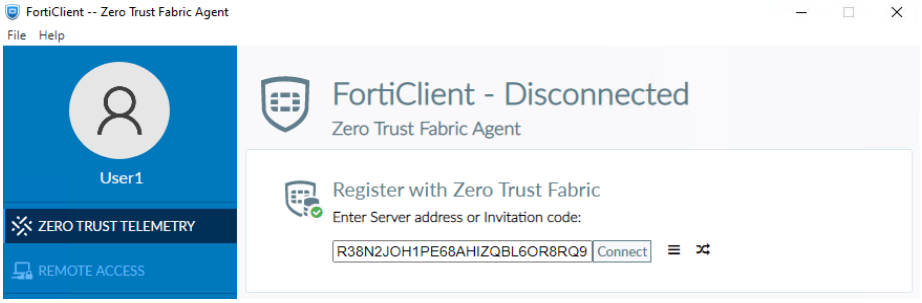

Рис.3.6. Реєстрація Forticlient

Після встановлення потрібно зареєструвати пристрій в EMS. Для цього потрібно перейти в панель керування а саме в Workgroups > Invitations > Add. Після створення треба скопіювати ідентифікатор та вставити в Forticlient. Приклад реєстрації наведений в рис.3.6-7.

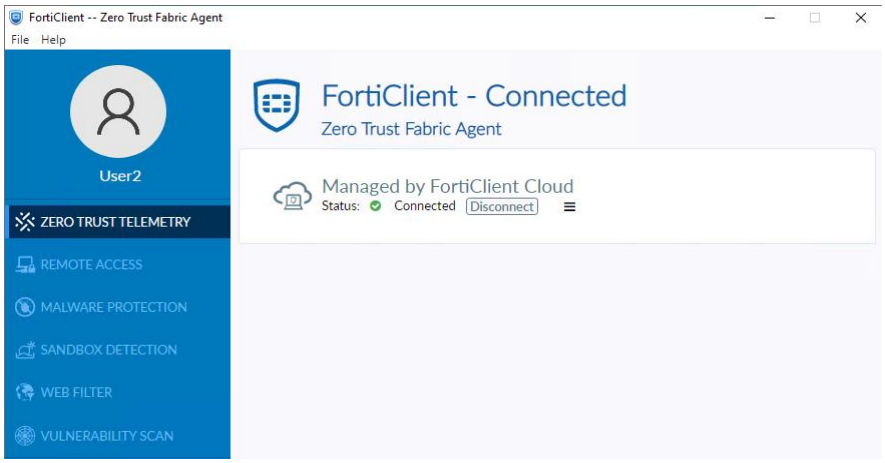

Рис. 3.7 Статус підключення

Для того, щоб правильним чином застосувати налаштування для трьох різних підмереж потрібно створити три групи користувачів. Створення груп користувачів зображено на рис.3.8.

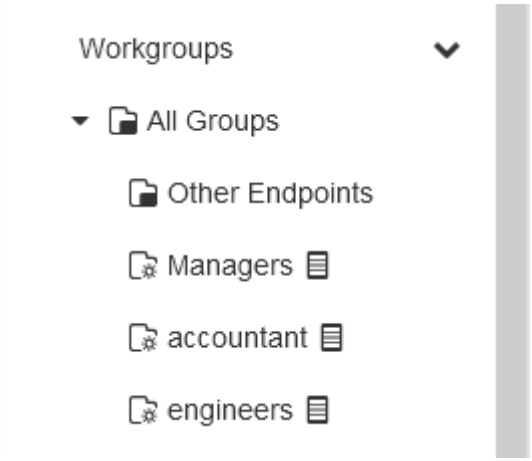

Рис.3.8 Створення груп користувачів

Налаштування профілів безпеки для кінцевих точок та користувачів. Першим в списку є Remote Access. Цей профіль дозволяє налаштовувати профілі підключення типу SSL VPN або IPsec VPN. Для усіх груп був налаштованний профіль віддаленого доступу до офісу, налаштування зображені на рис.3.9.

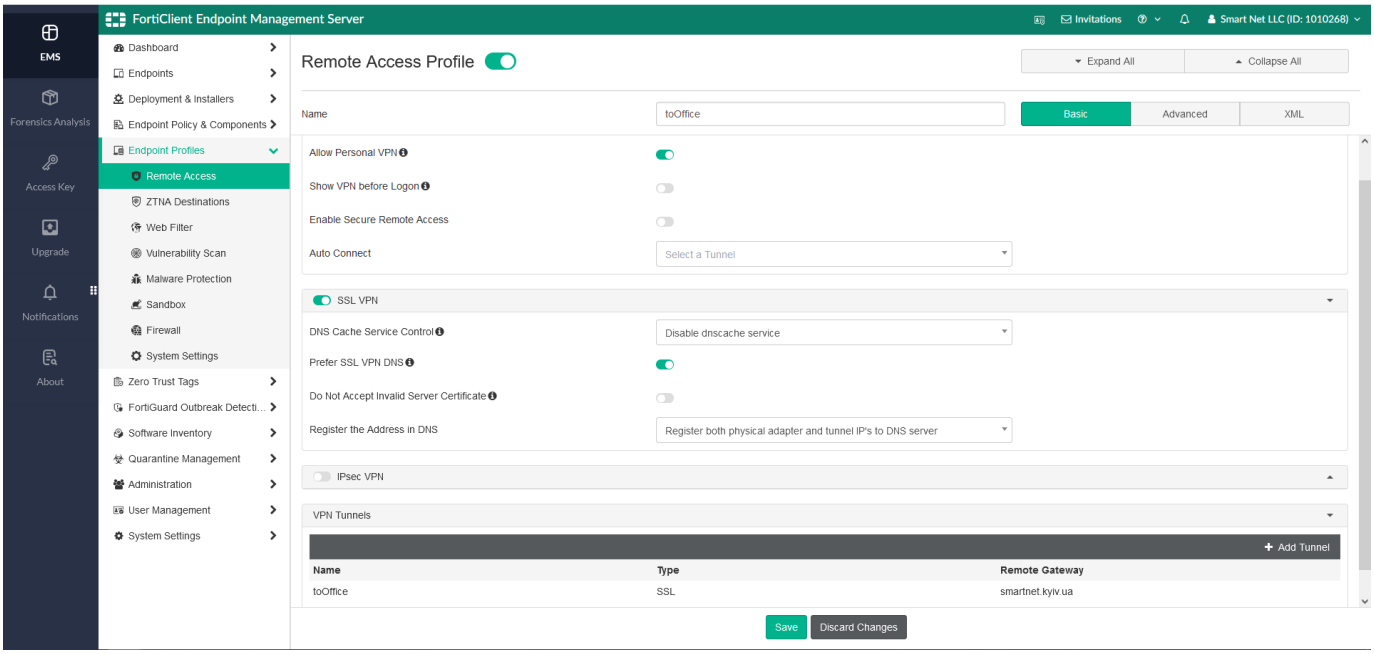

Рис.3.9. Налаштування профілю віддаленого доступу

Налаштування Web-profile ґрунтуються на фільтруванні категорій сайтів а також має певні параметри, а саме:

- Коли буде ввімкнена веб-фільтрація (весь час, чи коли Forticlient не буде подключений до EMS);
- Логувати трафік користувачів чи ні;
- Дія коли HTTPS сайт буде заблоковано (показати попередження в браузері чи в нотіфікацією від фортікліента);
- Ввімкнути плагін браузера для веб-фільтрації;

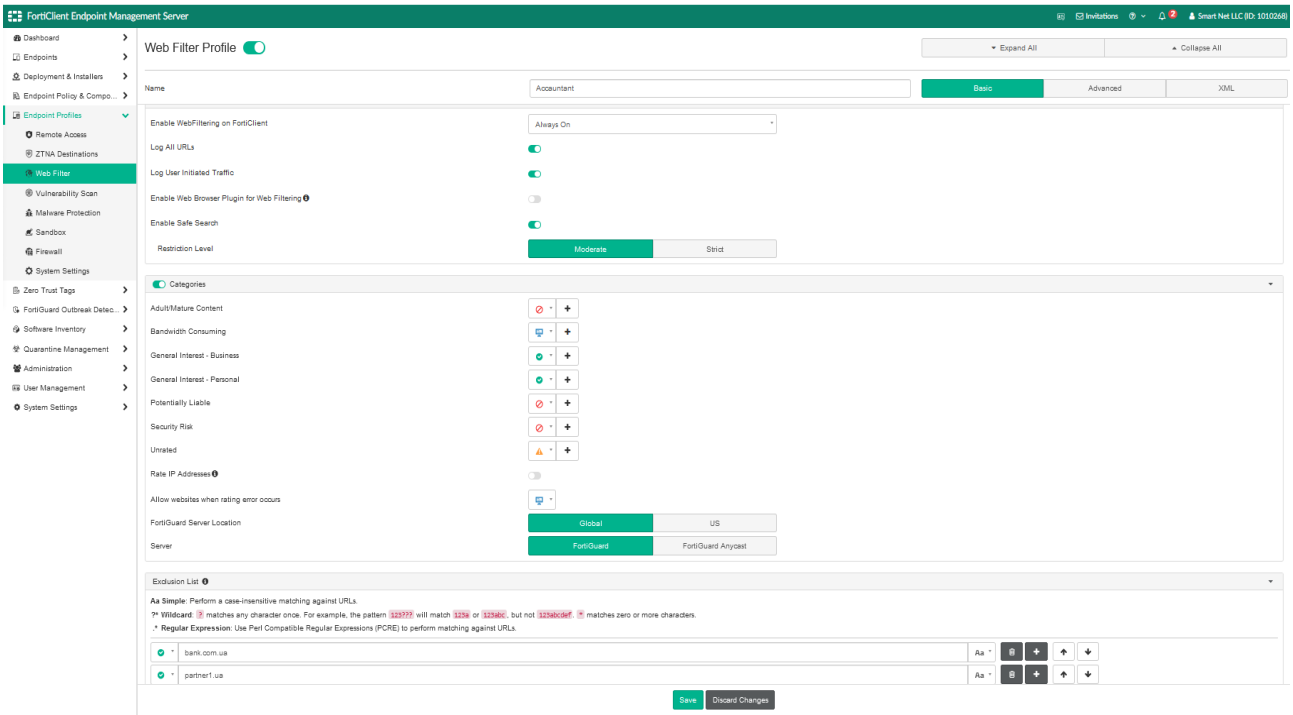

Рис.3.10. Налаштування для підмережі бухгалтерів

- Безпечний пошук - для кінцевих точок Windows і комп'ютерів Chromebook під час увімкнення Безпечного пошуку ви можете налаштувати рівень обмеження на Строгий або Помірний. Цей параметр впливає на вміст, до якого кінцеві користувачі можуть отримати доступ через YouTube і пошукову систему, зокрема Google і Bing;

- Категорії сайтів: Adult/Mature Content, Bandwidth Consuming, General Interest-Business, General Interest-Personal, Potentially Liable, Security Risk, Unrated. Також ці категорії мають підкатегорії на які вони розділяются;
- Використання HTTPS для доступу до Rating Server;
- Дія при недоступності Rating Server: Block, Warn, Allow, Monitor;
- Локація FortiGuard Server: Global, US;
- Список виключень з діями: Block, Allow, Monitor.

На рис.3.10-12 відображені налаштування для груп бухгалтери, менеджери та інженери.

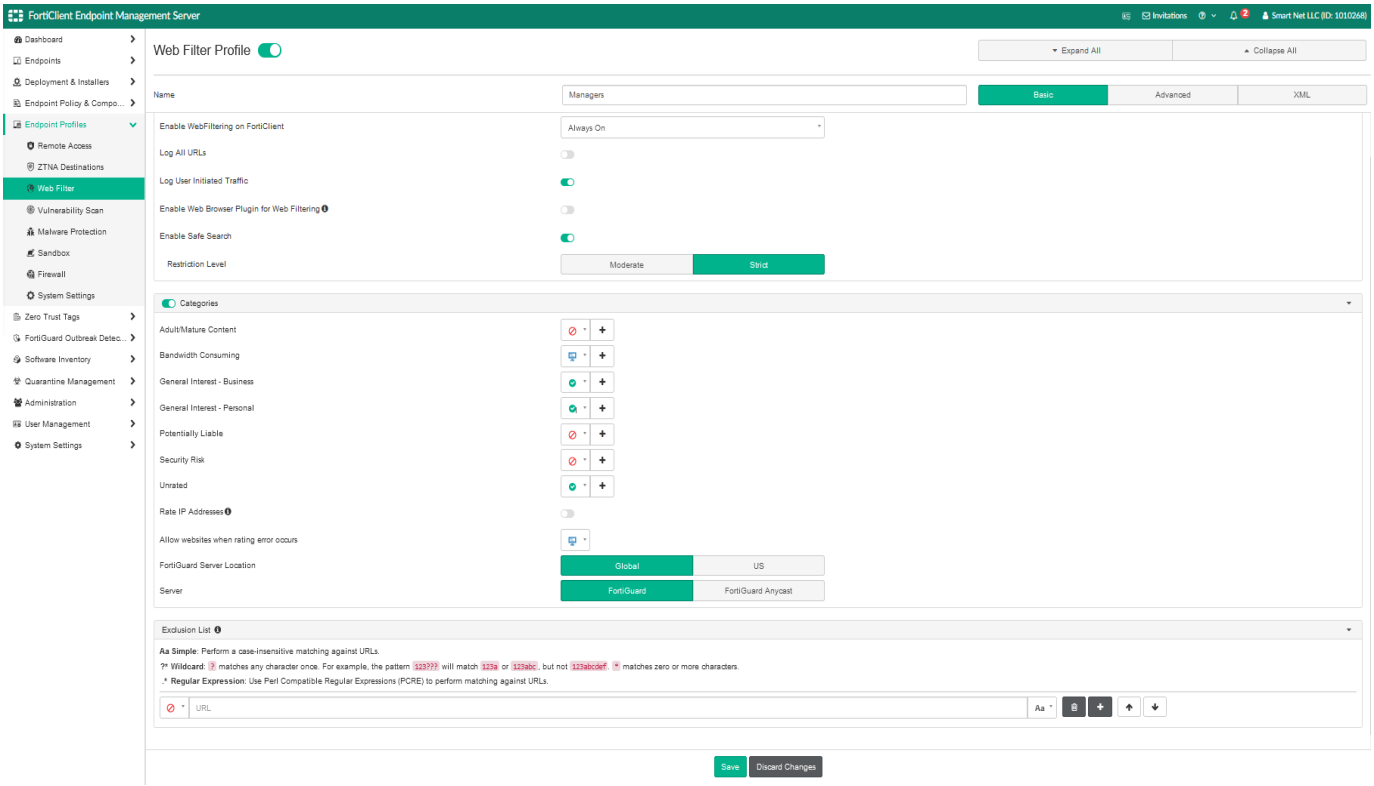

Рис.3.11. Налаштування для підмережі менеджерів

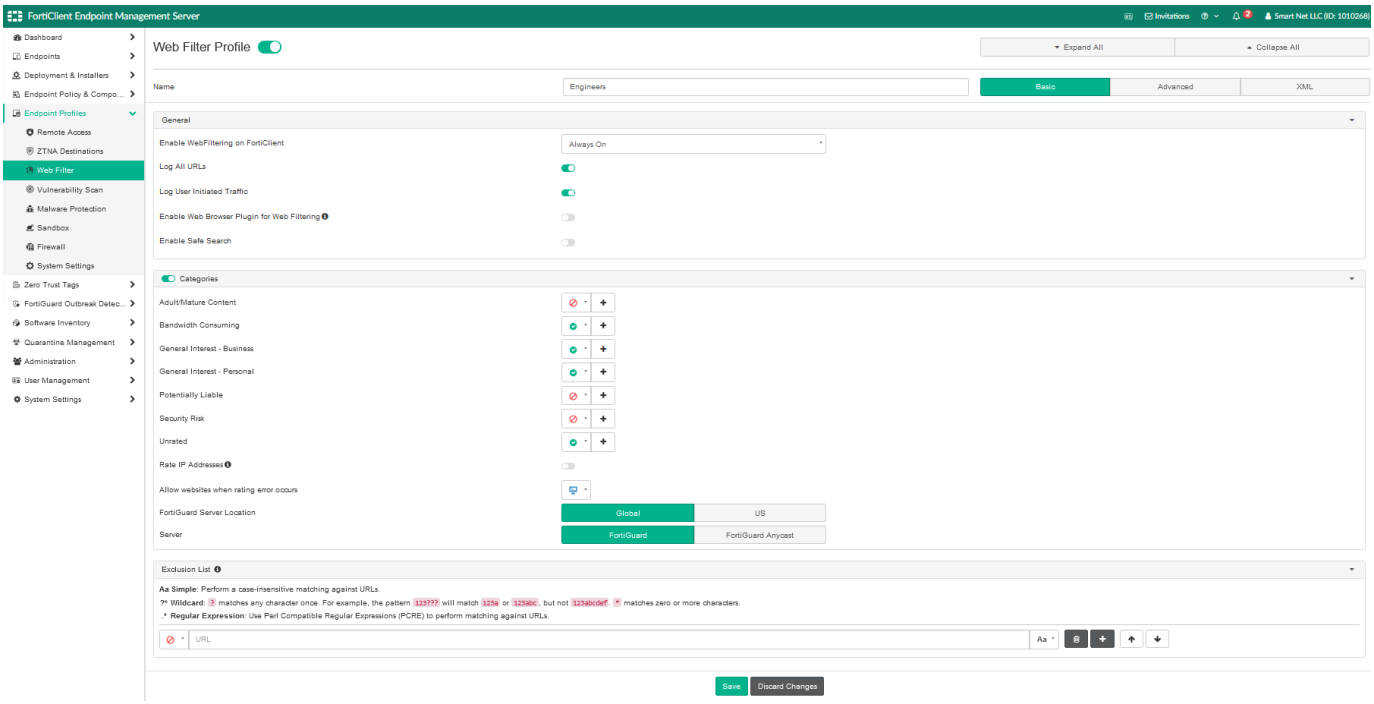

Рис.3.12. Налаштування для підмережі інженерів

Наступним профілем безпеки є Vulnerability Scan (сканування на вразливості), цей профіль має наступні налаштування:

- Сканування при реєстрації;
- Сканування при оновлені бази сигнатур;
- Сканування при оновлені ОС;
- Автоматичне сканування з певним проміжком часу;
- Сканування за розкладом;
- Автоматичний патчинг при певному рівні вразливості;
- Виключення для ручного оновлення певних вразливостей;
- Виключення для оновлення певних програм.

Профіль сканування з періодом сканування кожні 90 днів був створений для всіх трьох груп. Налаштування зображені на рис.3.13.

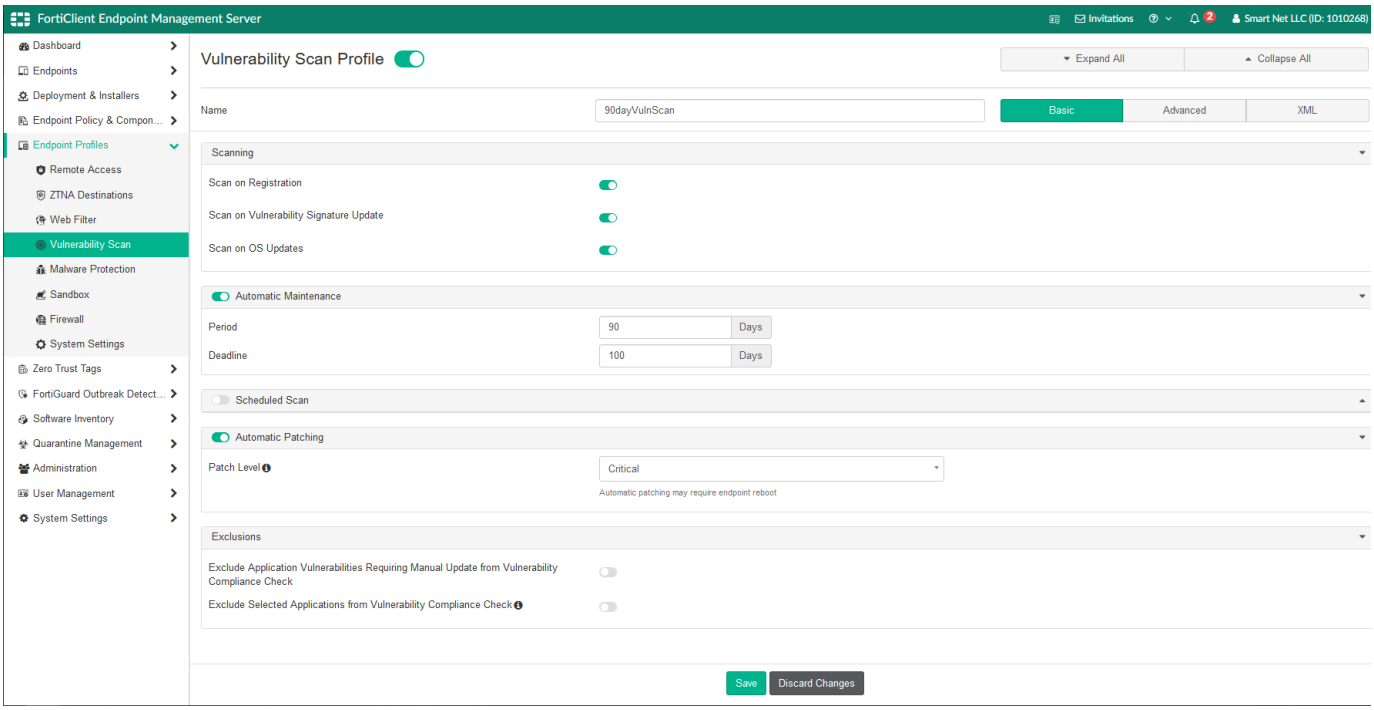

Рис.3.13. Налаштування профілю сканування вразливостей

Налаштування були зроблені таким чином, щоб сканувати пристрої користувачів після оновленя ОС або бази сигнатур, також період сканування був встановлений на один раз у квартал.

Далі йде профіль Sandbox - використовується для перевірки різних файлів на небезпечні вкладення і тд. Цей профіль має наступні налаштування:

- FortiSandbox server – який сервіс використовувати: хмарний або наявний у компанії
- Метод інспекції
- Виключення для певних типів файлів
- Які файли будуть проінспектовані: усі додатки до електронних листів, усі веб-завантаження, усі файли, запущені зі знімних носіїв
- Дії по запобіганню: тут можна встановити відповідність рівня небезпеки з дією по відношенню до файлу.
- Виключення щодо надійних джерел
- Виключення для певних файлів або системних шляхів

- Включення для певних файлів або системних шляхів

Налаштування профілю для всіх груп користувачів зображено на рис.3.14.

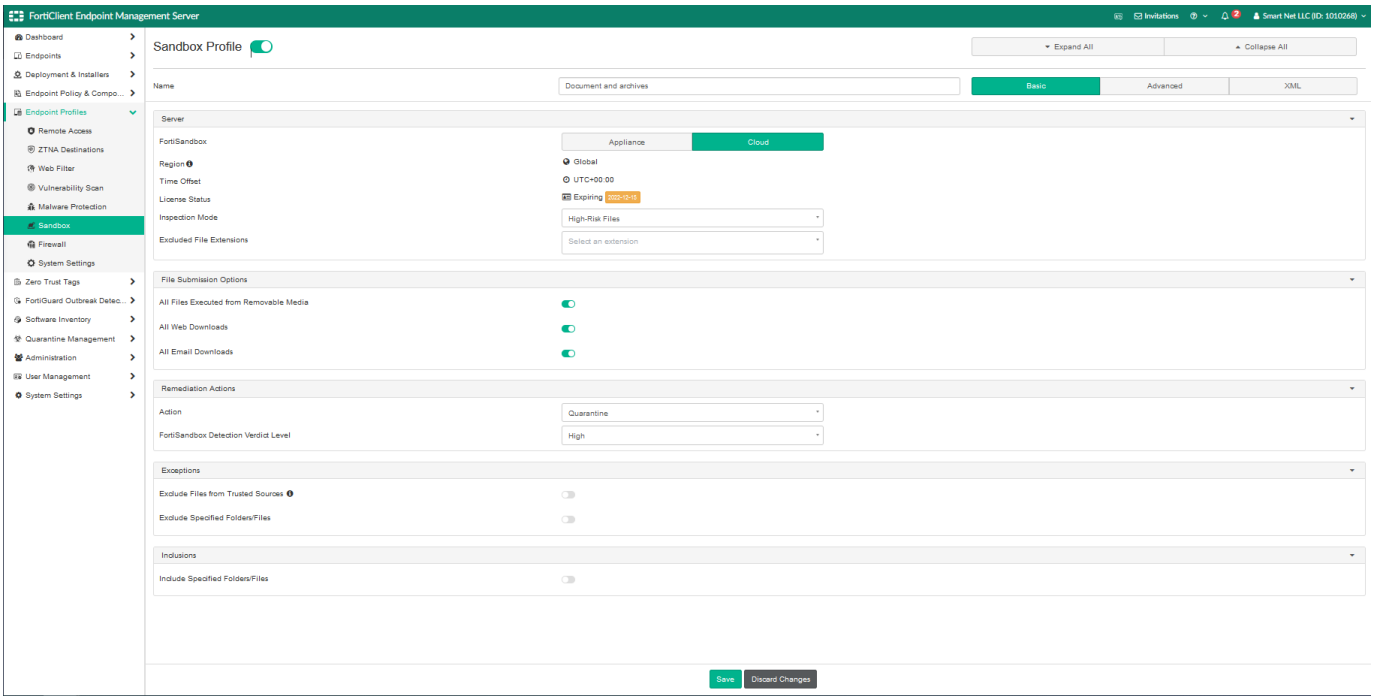

Рис.3.14. Налаштування Sandbox профілю

Профіль Firewall уявляє собою антивірус який дозволяє також фільтрувати до яких категорій додатків користувач буде мати доступ. Цей профіль має наступні налаштування:

- Нотіфікація користувача у разі блокування додатку;
- Детектування та блокування експлоїтів;
- Блокування відомих каналів зв’язку з C&C серверів;
- Блокування\Дозвіл\Логування наступних категорій додатків: Botnet, Business, Cloud.IT, Collaboration, Email, Game, General.Interest, Industrial, Mobile, Network.Service, P2P, Proxy, Remote.Access, Social.Media, Storage.Backup, Update, Video/Audio, VoIP, WebClient, All Other Unknown Applications.

Для усіх трьох груп були зроблені наступні налаштування які зображені на рис. 3.15.

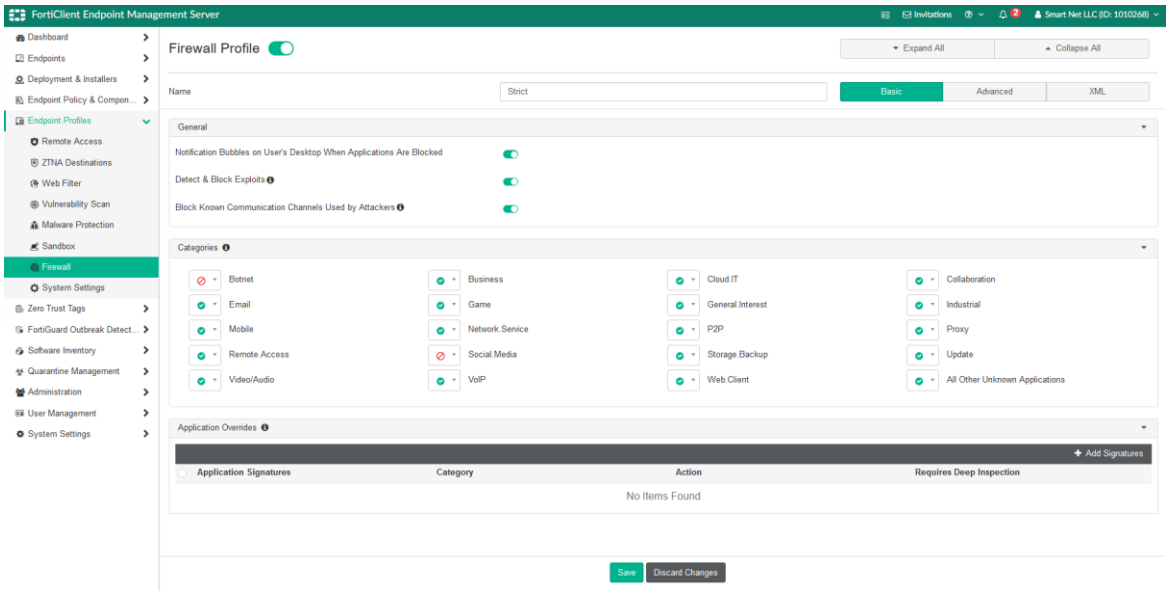

Рис.3.15. Налаштування профілю Firewall

Профіль системних налаштувань System settings дозволяє налаштовувати відображення налаштувань в самому Forticlient вже на комп'ютері користувача, та заборонити певні дії що можуть привести до зміни конфігурації. Профіль має такі налаштування, зображені на рис.3.16.

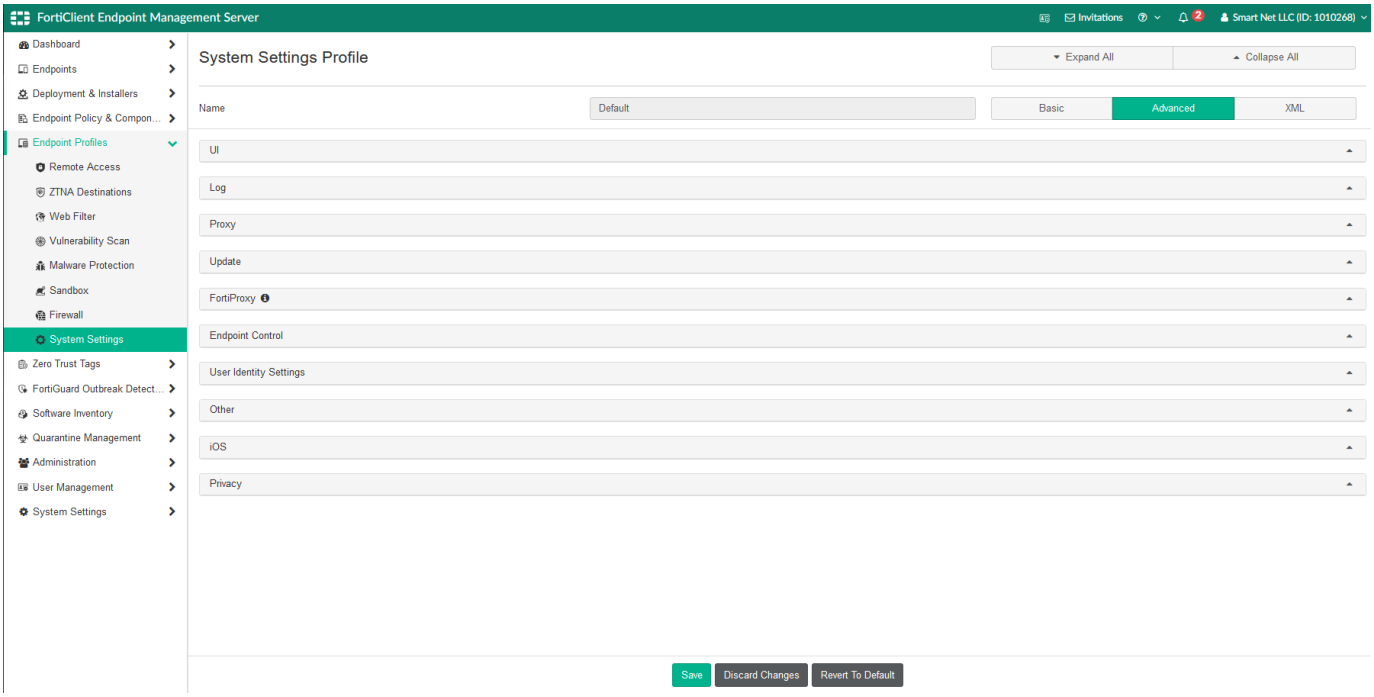

Рис.3.16. Налаштування профілю System Settings

Підкатегорії UI: Вимагати пароль для відключення від EMS, Не дозволяти користувачеві створювати резервну копію конфігурації, Дозволити користувачеві завершувати роботу після реєстрації в EMS, Приховати інформацію про користувача, Приховати іконку в трею, Показати Zero Trust Tag у графічному інтерфейсі FortiClient, Мова За замовчуванням. Вкладка за замовчуванням (яку вкладку будуть бачити користувачі).

Підкатегорії логування: Рівень логування (від Info до Alert та Debug), які саме категорії будуть логуватися (профілі захисту), Логування кліенту коли є підключення до FortiFabric, Завантаження логів до FortiAnalyzer/FortiManager. Обрані налаштування для перерахованих категорій зображені на рис.3.17.

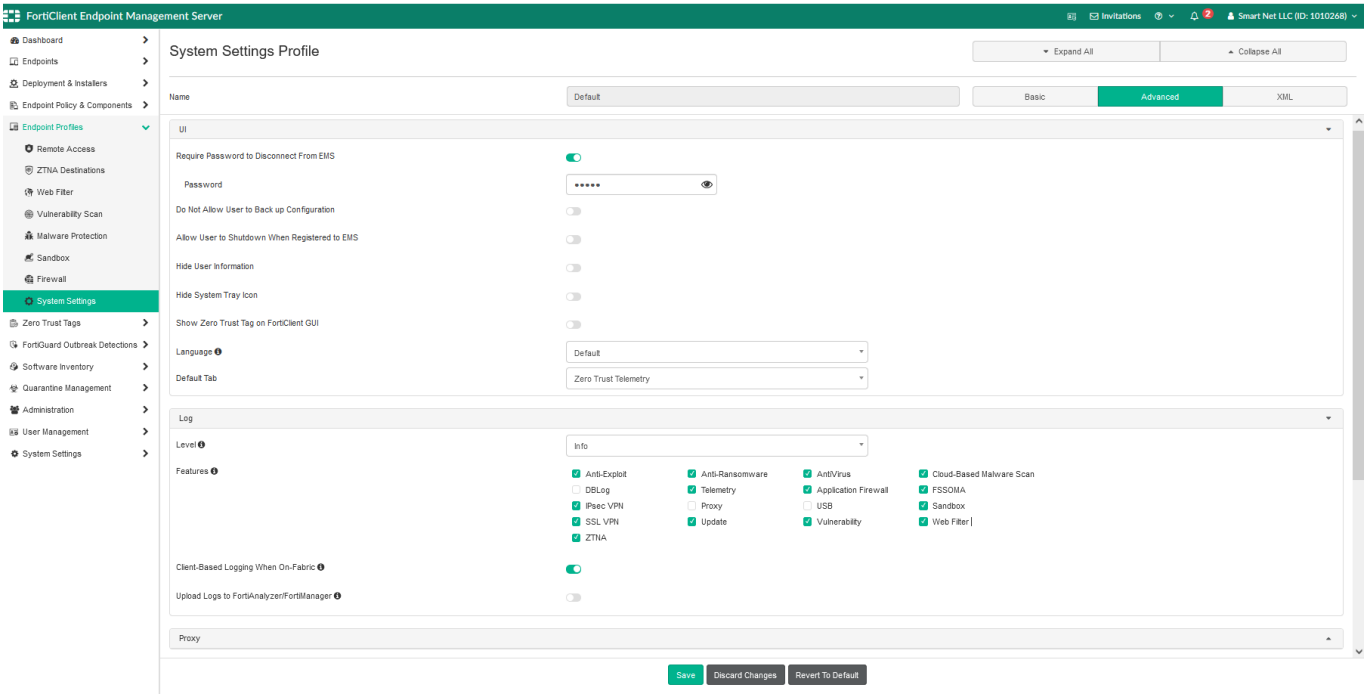

Рис. 3.17. Налаштування перших двух категорій профілю System Settings

Налаштування Proxy:

- Використання проксі для оновлення сервісів Fortiguard;
- Використання проксі для відправлення шкідливих файлів на аналіз.

Налаштування оновлень:

- Отримання налаштувань від FortiManager;

- Планування оновлень;
- Налаштування FortiGuard серверів.

Усі налаштування зображені на рис. 3.18.

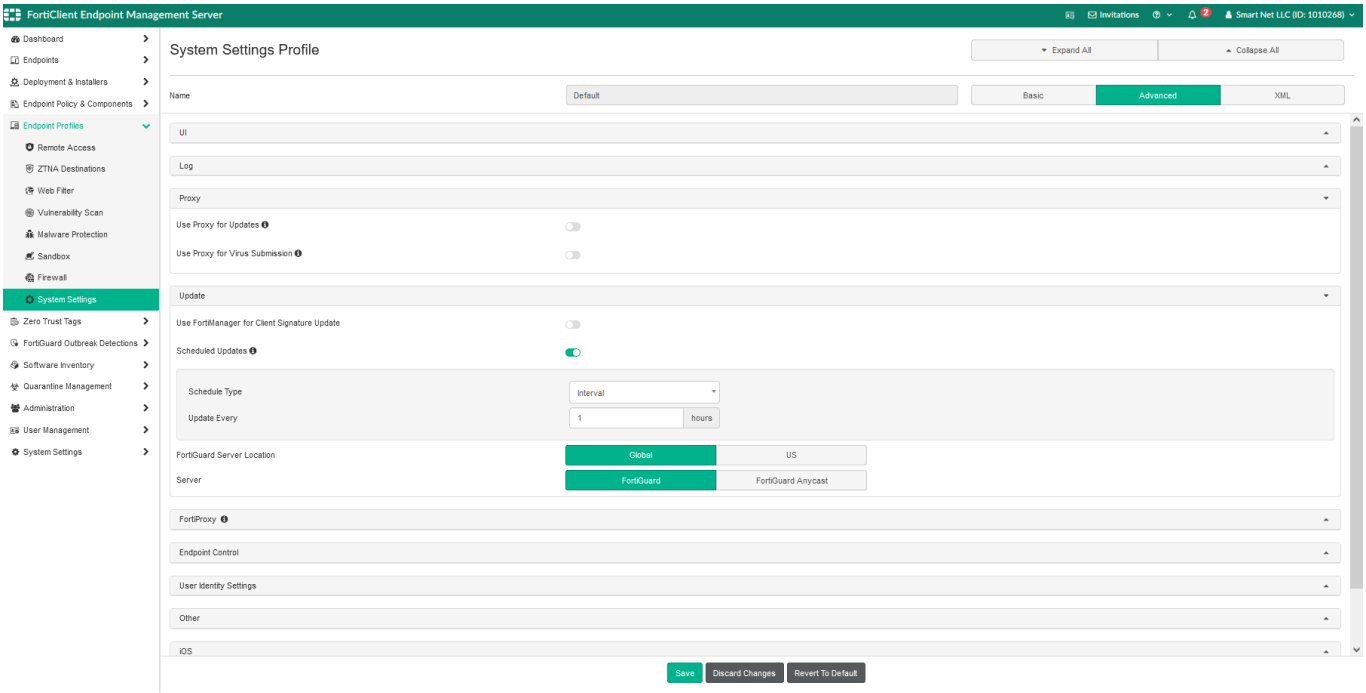

Рис.3.18. Налаштування Proxy та Update

Далі – Fortiproxy та Endpoint Control. Fortiproxy – Увімкнути\вимкнути FortiProxy, щоб використовувати Web Filter і деякі параметри AV. Ця частина профілю має такі налаштування які зображені на рис.3.19. Endpoint Control – налаштування нотіфікацій та іншого:

- Показати Bubble Notifications;
- Відключатися коли користувач виходить з windows;
- Вимкнути опцію відключення від серверу EMS;
- Відправляти перелік програм з кінцевої точки;
- Дія при неправильному сертифікаті.

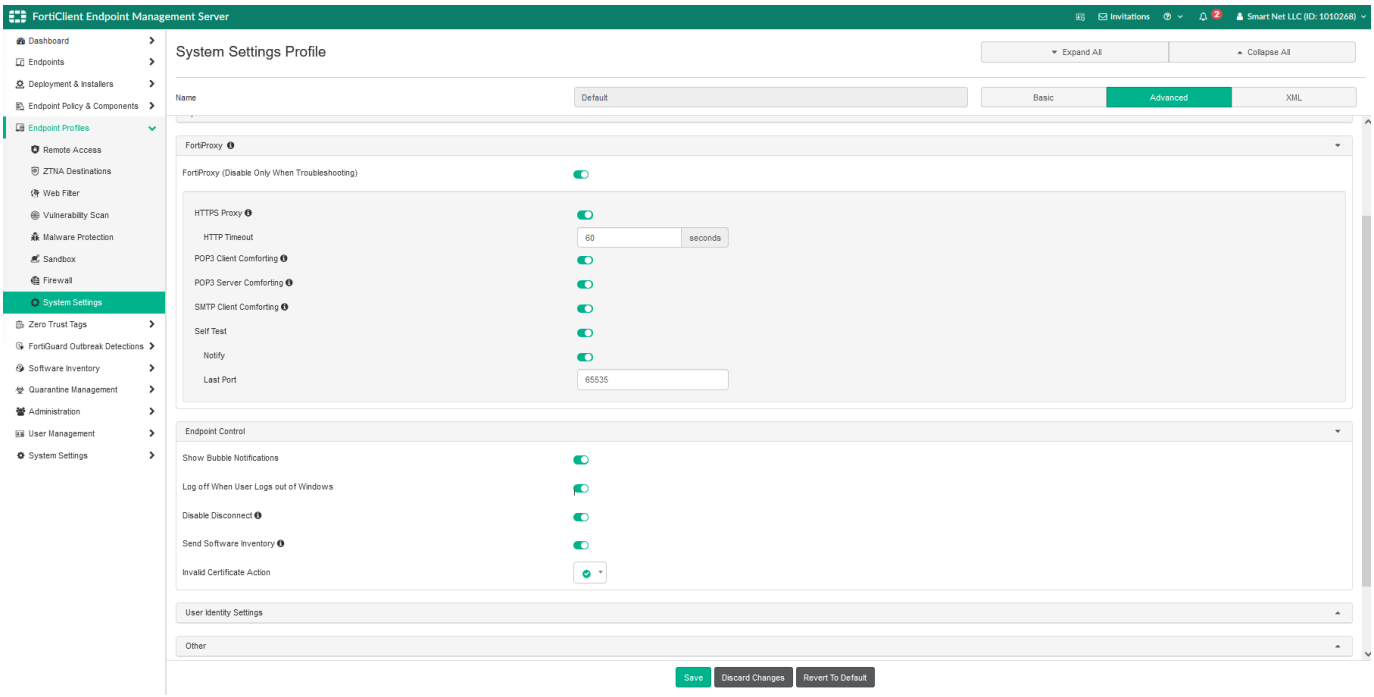

Рис.3.19. Налаштування FortiProxy та Endpoing Control

Налаштування ідентифікації користувача, інше, IOS, приватність. Налаштування додаткової ідентифікації - за замовчуванням EMS отримує інформацію про користувача від ОС кінцевої точки.

Якщо користувач надає свої дані за допомогою одного з наведених методів: LinkedIn, Google, Salesforce; EMS натомість отримує вказані користувачем дані. Якщо цей параметр вимкнено, EMS отримує та відображає відомості про користувача з ОС кінцевої точки. Інше – встановити CA certificate на кліент та FortiClient Single Sign-On Mobility Agent. Усі налаштування зображені на рис.3.20.

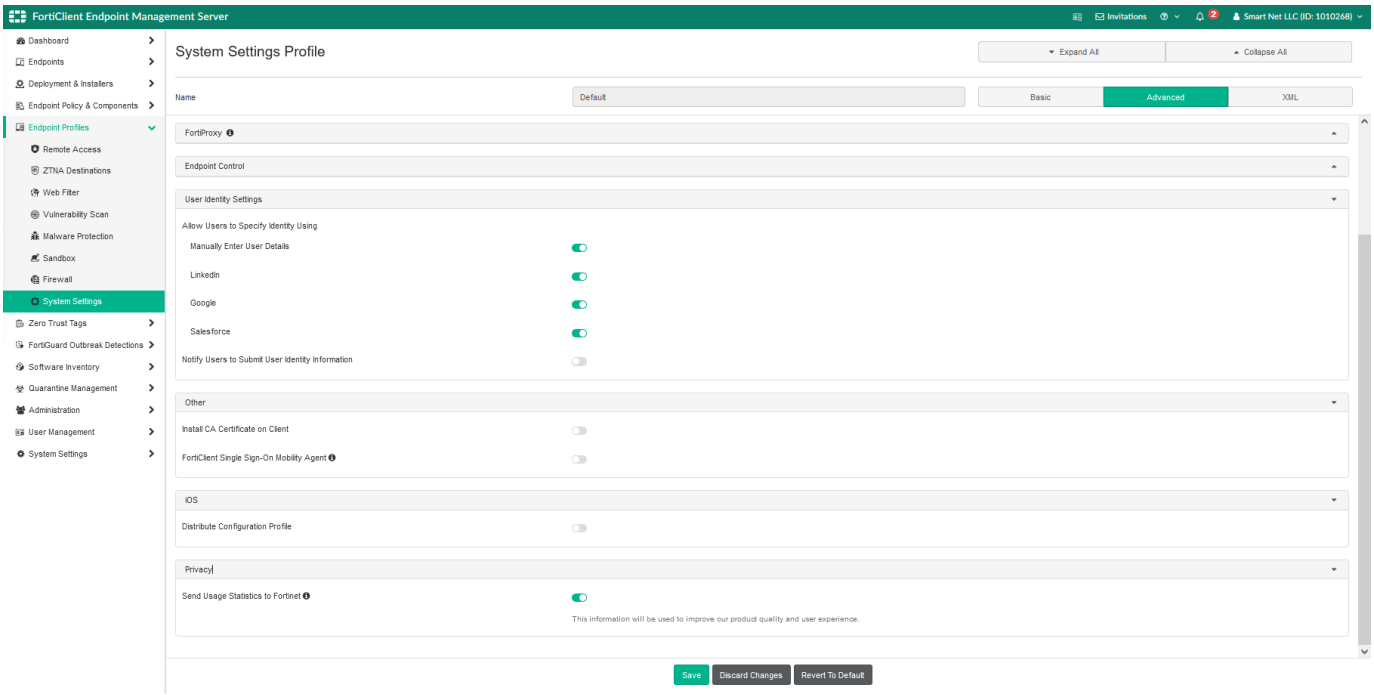

Рис. 3.20. Налаштування чотирьох останніх модулів профілю System settings

Наступним кроком потрібно налаштувати політики застосування профілів на групи. Таким чином було налаштоване застосування для групи бухгалтерів рис.3.21.

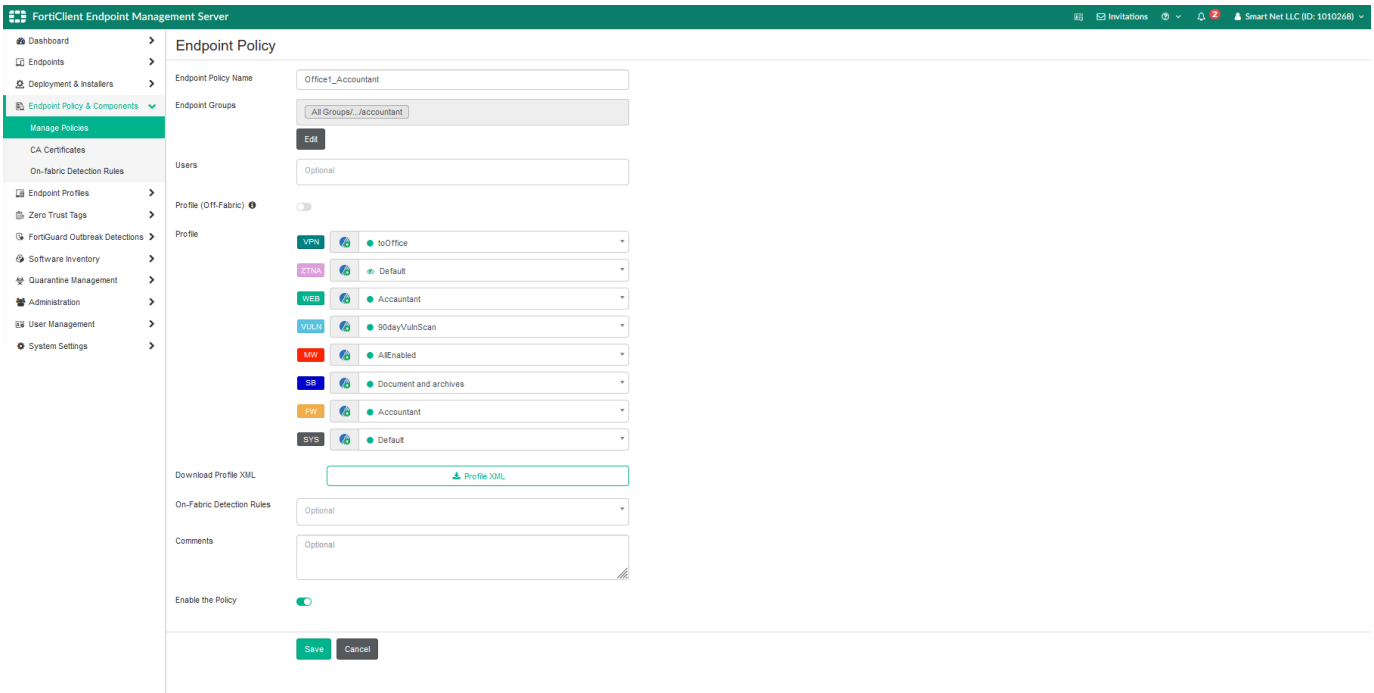

Рис. 3.21. Політика застосування профілів до груп

VPN – профіль toOffice, де налаштовано підключення до офісу за допомогою SSL vpn.

ZTNA – налаштування за замовчуванням. WEB – у цій категорії налаштований окремий профіль для групи бухгалтерів. Обмеження профілю бухгалтерів налаштовані на таких категоріях: Adult/Mature Content, Potentially Liable, Security Risk.

Для Unrated налаштована дія застереження, а для інших дозволено. VULN – профіль сканування та перевірки вразливостей періодом у 90 днів, який налаштований для усіх груп. MW – профіль захисту від шкідливого програмного забезпечення. Цей профіль також один на усі групи для забезпечення загального захисту усіх груп. SB – профіль пісочниці налаштований на сканування усіх завантажень, усіх додатків до електронної пошти та усіх файлів що запускаються, також один профіль на усі групи. FW – для бухгалтерів був налаштований на заборону категорій Botnet, P2P, SocialMedia. SYS – профіль за замовчуванням був підкоригований для усіх трьох груп.

Налаштування для менеджерів наступні, рис.3.22.

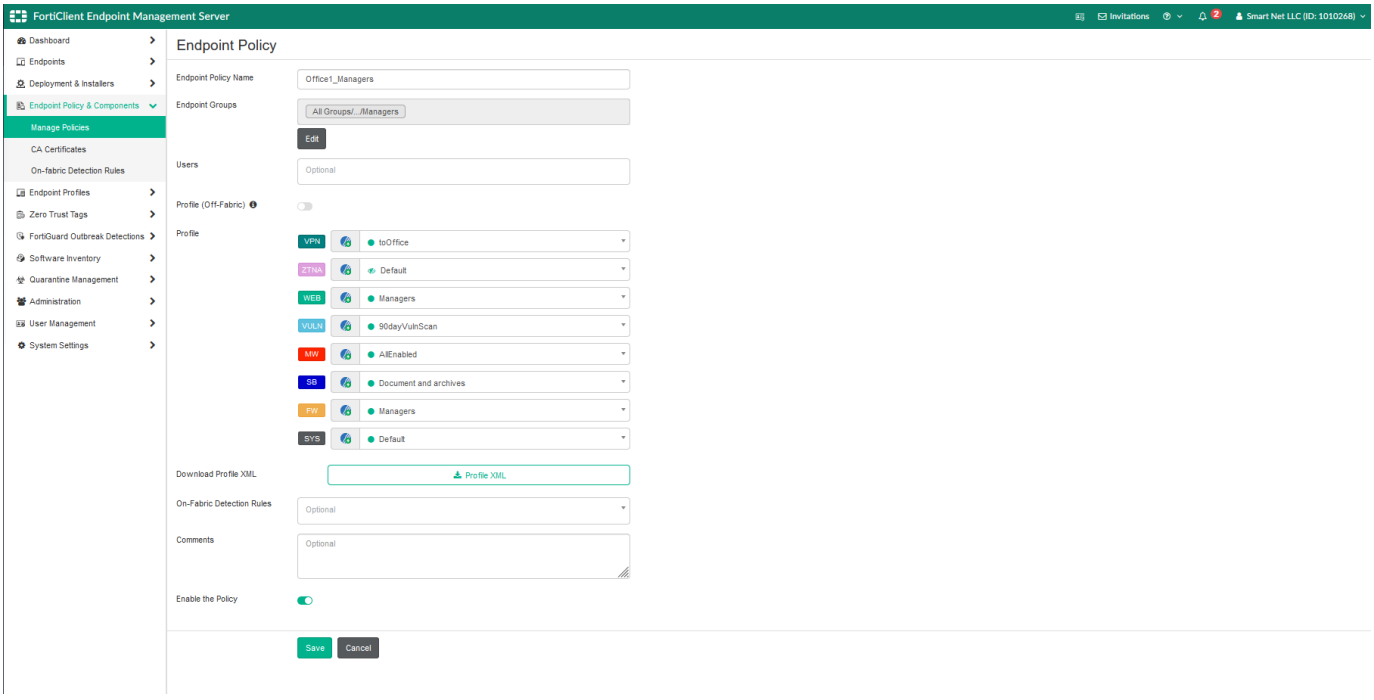

Рис.3.22. Налаштування профілів для менеджерів

WEB – заборона для таких категорій для менеджерів: Adult/Mature Content, Security Risk, Potentially Liable. Також профіль FW – заборона Botnet, P2P. Усе інше дозволено. Налаштування для інженерів було зроблено наступне рис.3.23.

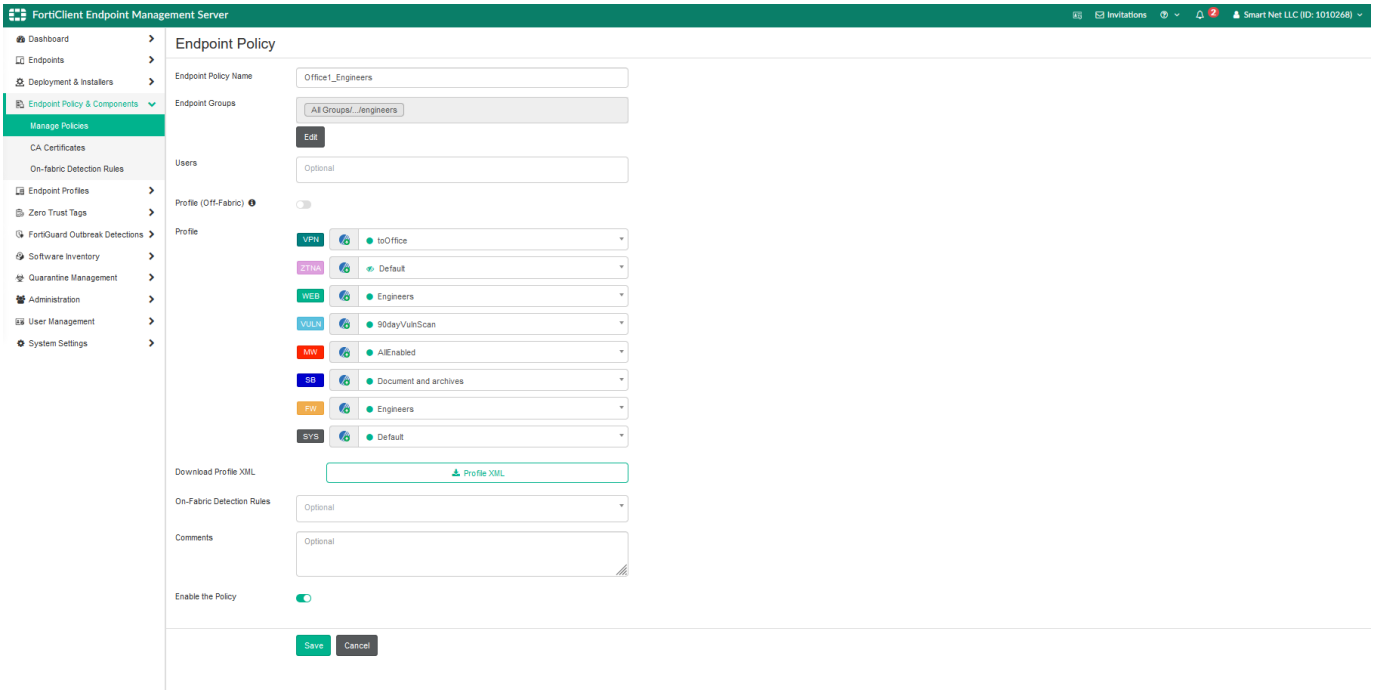

Рис.3.23. Налаштування профілів для групи інженерів

WEB – усе дозволено. FW – дозволено усе.

3.3 Перевірка FortiClient та FortiClient EMS за допомогою тестових вірусних файлів

Перевірка функціювання будь якої системи є невід'ємною частиною налаштування, а також побудови захисту. Перша перевірка це класичний файл для перевірки – eicar. Результати роботи Forticlient зображені на рис.3.24.

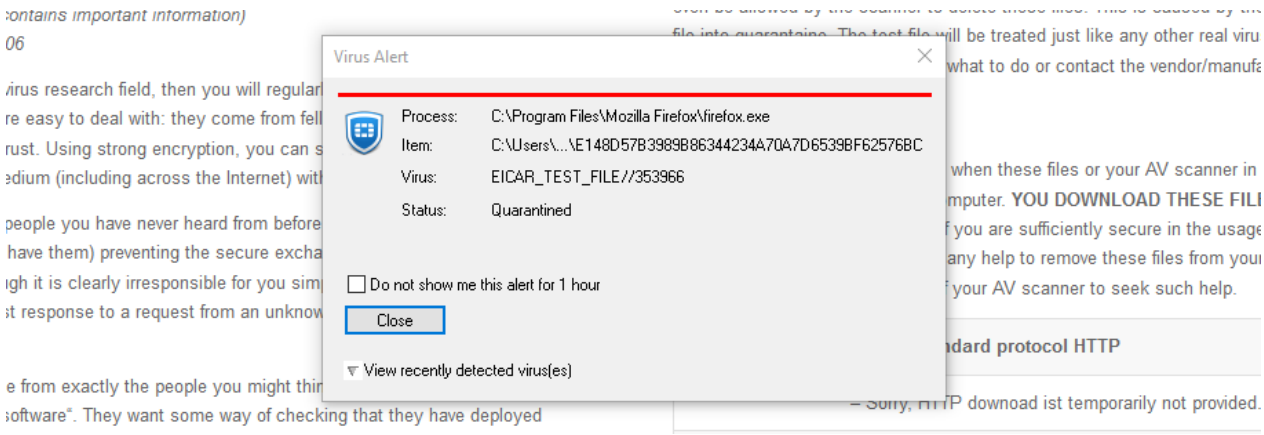

Рис.3.24. Результат блокування eicar файлу.

Наступний файл це тестовий файл від Palo Alto. Відповідь Forticlient на файл зображена на рис.3.25.

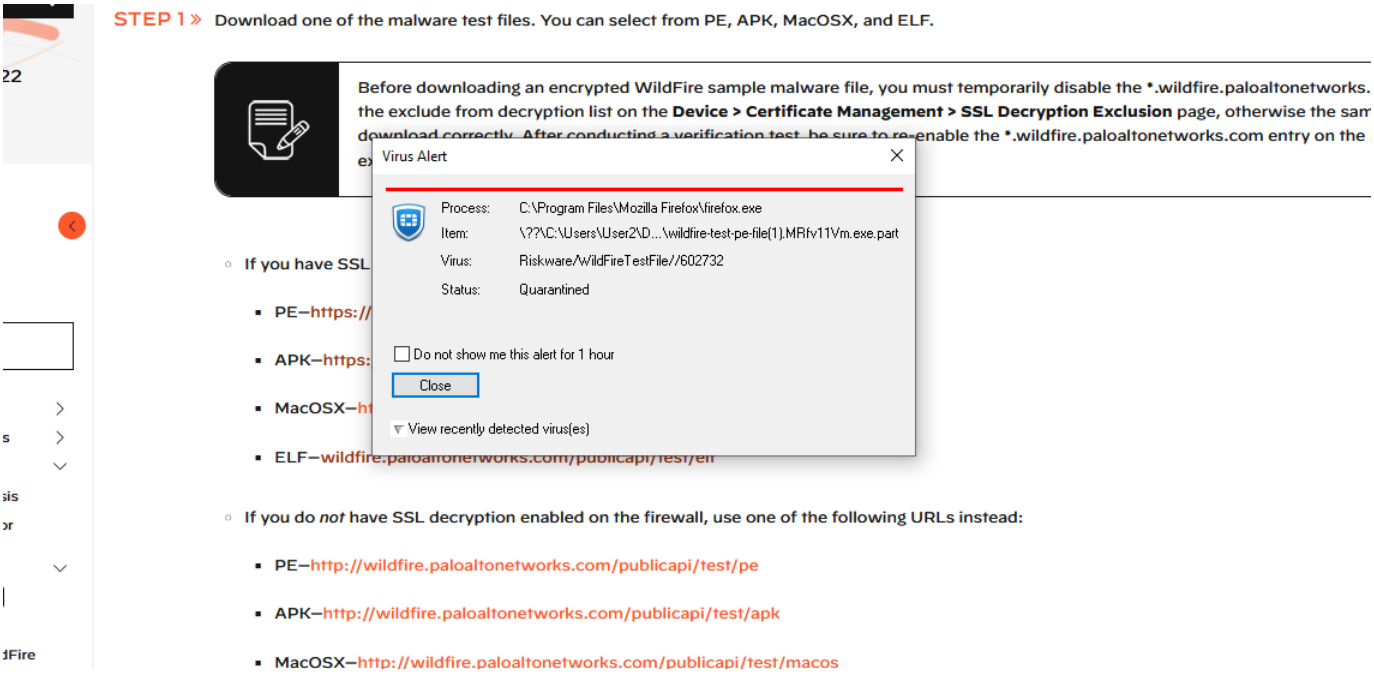

Рис.3.25. Forticlient та шкідливий файл від PaloAlto

Блокування забороненої веб-категорії Adult material, приклад можливо побачити на рис.3.26.

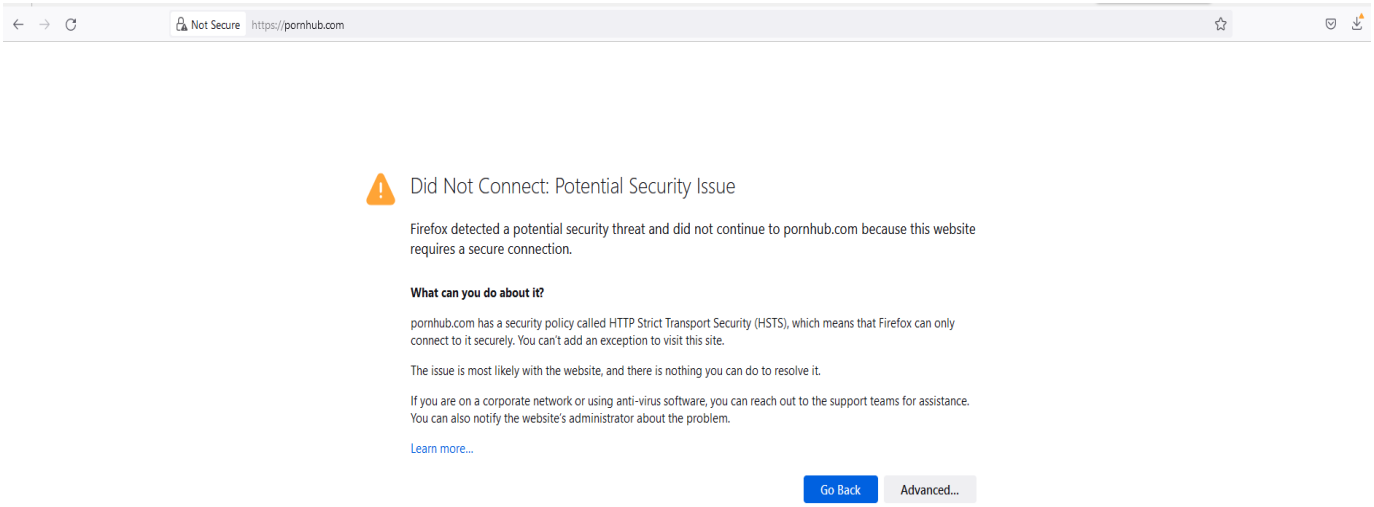

Рис.3.26. Блокування забороненої веб-категорії

Перегляд статистики блокувань можливо побачити на рис.3.27.

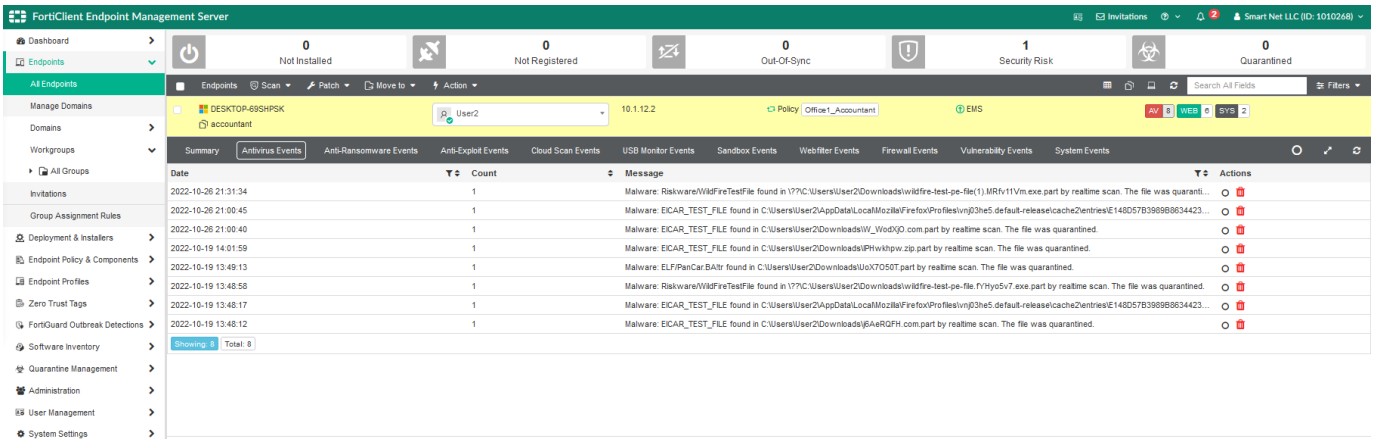

Рис.3.27. Статистика блокувать Antivirus.

Блокування Web категорій зображені на рис.3.28.

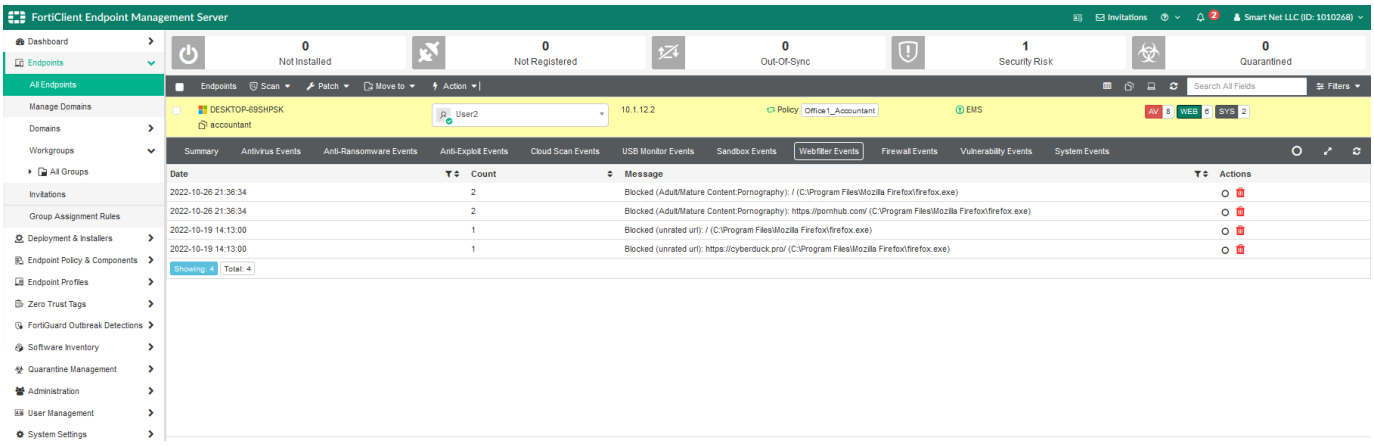

Рис. 3.28. Статистика блокувань Веб профілю

Блокування соціальних мереж за допомогою профілю рис.3.29.

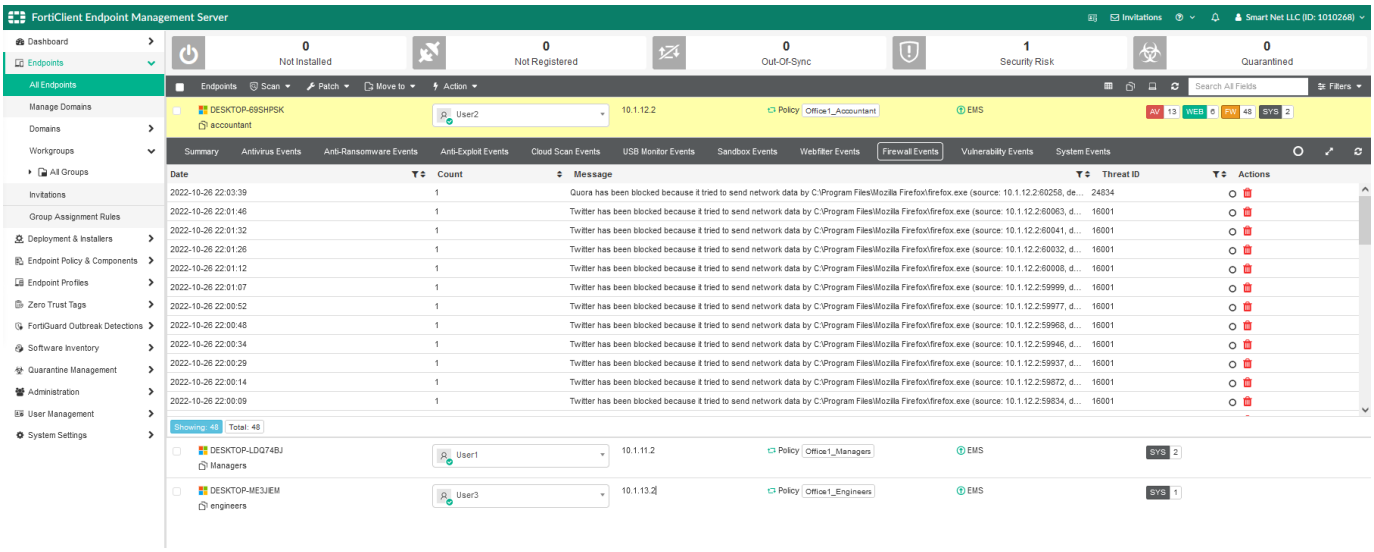

Рис.3.29. Блокування соціальних мереж

Також дуже корисною можливістю є додавання кінцевих пристроїв в карантин. Карантин обмежує усі зв’язки з навколишнім світом та не дозволяє розповсюдитися зараженню далі. Повідомлення карантинування зображено на рис.3.30.

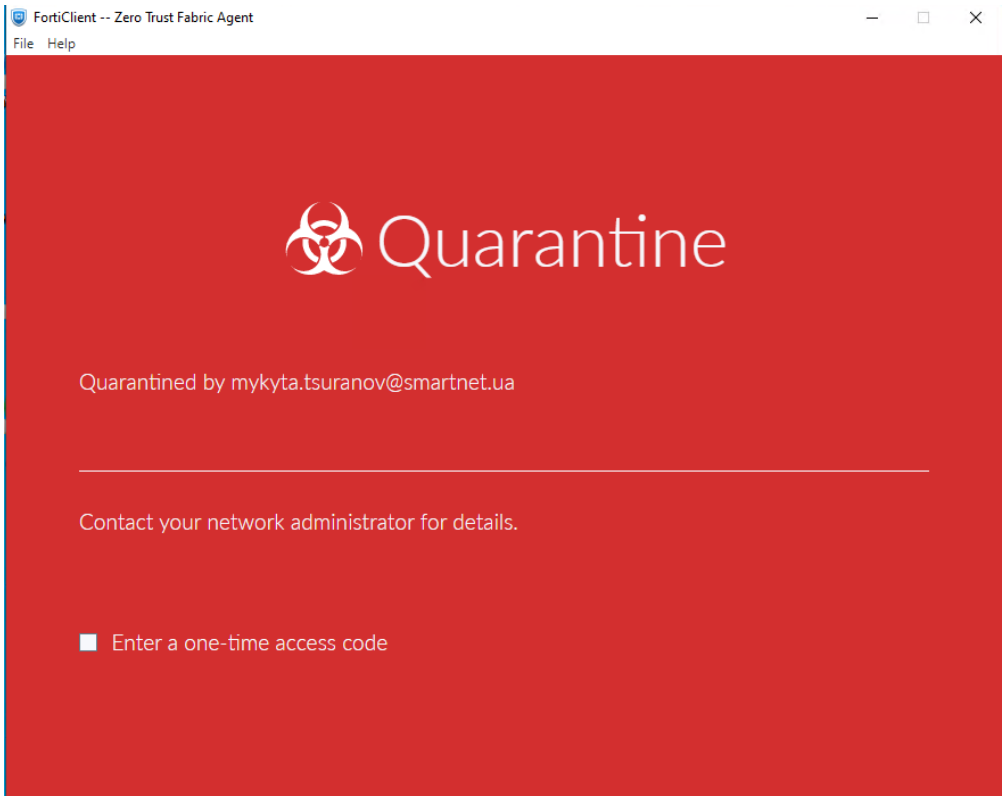

Рис. 3.30. Повідомлення карантинування

3.4 Розроблення рекомендацій щодо захисту кінцевих пристроїв

Кінцеві пристрої не тільки мають змогу підключатися до віддалених ресурсів компанії, такі як бази даних і тд. Але на кінцевих пристроях також можуть опрацьовуватися чутливі дані клієнтів компанії. Тому першу частину рекомендації буде присвячено фізичному доступу та налаштування шифрування дисків та інше.

Отже, фізичкий доступ має доволі велике значення в побудові захисту особливо при побудові захисту кінцевих пристроїв. Доступ до кінцевого пристрою доволі важко обмежити.

Якщо це офіс, то в працівників є свої робочі місця і якщо хтось буде сидіти не на своєму робочому місці буде доволі помітно. Фізичне обмеження в офісі починається в першу чергу з обмежень на вході в бізнес центр за допомогою персональних карт і тд. Наступне це відеоспостереження. Також можливість моніторингу мережі та підключення нових пристроїв до неї.

Коли працівники працюють віддалено, то в переважній більшості фізичний доступ до кінцевого пристрою може отримати будь-хто. Саме тому потрібно вжити заходів щодо фізичного захисту пристроїв. По-перше це елементарно – пароль на пристрій. Наступним рівнем є шифрування на пристрої. Організація може захотіти зашифрувати дані з багатьох причин. Наприклад, компанії у високотехнологічних галузях, таких як фармацевтика чи розробка програмного забезпечення, повинні захищати свої дослідження від конкурентів.

Організації в регульованих галузях, таких як охорона здоров'я та фінансові послуги, повинні шифрувати дані пацієнтів і споживачів, щоб відповідати державним нормам. Стандарт безпеки даних платіжних карток (PCI-DSS) вимагає від продавців шифрувати дані кредитних карток споживачів, щоб запобігти несанкціонованому використанню.

Нерегульовані організації також стурбовані безпекою даних. Порушення даних може призвести до негативного розголосу, втрати бізнесу та судових позовів від партнерів чи клієнтів. Кібератаки та витоки даних стають все більш поширеними явищами, і вони дорогі. Шифрування є важливим компонентом багаторівневої стратегії безпеки даних. Організації зазвичай включають кілька рівнів захисту, включаючи брандмауери, захист від вторгнень, захист від зловмисного програмного забезпечення та запобігання втраті даних. Шифрування діє як останній рівень захисту даних у випадку, якщо вони потраплять у чужі руки.

Оскільки дистанційна робота та використання мобільних пристроїв стають все більш поширеними, зростає загроза втрати та крадіжки пристроїв. Якщо пристрій загубили в метро або його вкрали зі столика в кафе, зловмисник, який має фізичний доступ до пристрою, може спробувати прочитати дані, що зберігаються на пристрої.

При заміні кінцевих пристрої на більш сучасні, пристрій може не форматуватись. Компанії та окремі особи постійно викидають пристрої, що містять потенційно конфіденційну інформацію. У деяких випадках учасники кіберзагроз

збирають ці вживані пристрої та намагаються прочитати дані, які вони містять, що може розкрити корпоративні дані або особисту інформацію клієнтів.

Основні компоненти всіх рішень шифрування кінцевих точок досить схожі. Алгоритми шифрування, які широко використовуються сьогодні, такі як Advanced Encryption Standard (AES) і Rivest-Shamir-Adleman (RSA), є загальнодоступними протоколами, якими може користуватися кожен. Вважається, що ці алгоритми шифрування захищені від атак сучасних комп'ютерів. Основною відмінністю між системами шифрування кінцевих точок є рівень, на якому застосовується шифрування. Двома основними типами систем шифрування кінцевих точок є повнодискове шифрування та шифрування файлів.

Повнодискове шифрування (Full Disk Encription) використовує універсальний підхід до шифрування. Весь диск шифрується за допомогою того самого алгоритму шифрування, налаштувань і секретного ключа. Цей секретний ключ зберігається на самому пристрої та доступний лише після автентифікації користувача в системі. Після входу користувача в систему можна розшифрувати всі файли та папки в системі. Це дає можливість завантажуватися системі та надає користувачеві повний доступ до своїх файлів і папок, забезпечуючи найкращу взаємодію з користувачем. З іншого боку, деякі системи шифрування кінцевих точок надають можливість виконувати шифрування окремо для кожного файлу. Це дозволяє користувачеві точно визначити, які файли він хоче зашифрувати, і деталі того, як це шифрування виконується.

Шифрування файлів, папок і знімних носіїв шифрує вибраний вміст на локальних дисках, мережевих ресурсах або знімних носіях. Програмне забезпечення для шифрування розгортає агенти, які шифрують файли на основі політики організації. Шифрування на основі файлів підтримує як структуровані, так і неструктуровані дані, тому його можна застосовувати як до бази даних, так і до документів і зображень. Шифрування на основі файлів зберігає дані в зашифрованому стані, доки їх не відкриє авторизований користувач. Це відрізняється від шифрування всього диска, яке розшифровує всі дані після автентифікації користувача та

завантаження системи. Таким чином, файлове шифрування кінцевої точки продовжує захищати дані навіть після того, як вони залишають організацію. Наприклад, коли зашифрований файл надсилається як вкладення електронної пошти, одержувач має пройти автентифікацію, щоб розшифрувати файл. Одержувачі, які не мають відповідного програмного забезпечення для шифрування/дешифрування, можуть натомість отримати посилання на портал, який може автентифікувати їх і розшифрувати файл, або отримати файл вкладення контейнера (наприклад, захищений паролем zip-файл), у якому одержувач має ввести пароль, наданий відправником. Шифрування на основі файлів покладається на політику шифрування організації для визначення типів вмісту для шифрування та обставин, які потребують шифрування. Після налаштування рішення для шифрування можуть автоматично застосовувати політики та шифрувати вміст.

Встановлення паролю на BIOS/UEFI є гарною практикою, що дозволить посили ти захист та убезпечитися від атаки «злої покоївки». Атаки «злих покоївок» описують загрозу отримання зловмисником фізичного доступу до пристрою, залишеного в готельному номері, офісі компанії тощо. За таких обставин зловмисник може мати змогу прочитати дані або встановити шкідливе програмне забезпечення на пристрій.

Наступним рівнем безпеки є перевірка налаштувань системи. Найпопулярнішою системою є системи Windows, тому саме для цього сімейства ОС буде наведений перелік налаштувань які можуть посилити безпеку кінцевого пристрою.

Захист системи – це практика мінімізації поверхні атаки комп’ютерної системи або сервера. Мета полягає в тому, щоб зменшити кількість недоліків безпеки та вразливостей, якими можуть скористатися зловмисники. Зміцнення ОС зазвичай передбачає встановлення виправлень і захист операційної системи сервера. Постачальники операційних систем, як-от Microsoft, зазвичай випускають оновлення, пакети оновлень і виправлення, які користувачі можуть установлювати вручну або

автоматично. Windows 10 має широкі вбудовані функції безпеки, які можна використовувати для посилення операційної системи.

Антивірус Windows Defender Антивірус (надалі WDA) вбудований у Windows і не потребує ручного налаштування чи підтримки (за винятком автоматичних оновлень). Це велика перевага в порівнянні з сторонніми антивірусними рішеннями. WDA має вбудований брандмауер і безпечне середовище перегляду для захисту користувачів від найпоширеніших загроз. Брандмауер підтримує три конфігурації мережі (доменну, приватну та публічну). Однак, як правило, ця функція ввімкнена за замовчуванням (щоб відповідати правилам безпеки за замовчуванням) і діє без будь-яких коригувань. WDA автоматично сканує кожен щойно завантажений файл, коли користувач відкриває його. Рекомендується проводити глибоке сканування руткітів принаймні раз на місяць.

Windows Defender Exploit Guard — це антишкідливе програмне забезпечення, яке захищає користувачів Windows 10 від вторгнення. Exploit Guard доступний як частина центру безпеки Windows Defender і може допомогти захистити комп’ютер від багатьох типів атак. Наприклад, він пропонує заходи захисту пам’яті для запобігання атакам, які маніпулюють внутрішньою пам’яттю. Інші використовувані методи запобігання вторгненням включають зменшення поверхні атаки програм, запобігання доступу шкідливих програм до папок і захист мереж від шкідливих програм. Щоб змінити налаштування Exploit Guard, можна скористатися програмою Windows Defender Security Center або Windows PowerShell. Також можна керувати цим інструментом за допомогою консолі керування Windows Defender Advanced Threat Protection (ATP).

Консоль керування ATP пропонує докладні звіти, включно зі сповіщеннями про підозрілий трафік. Windows Defender Device Guard Windows Defender Device Guard розроблено для захисту вашого пристрою шляхом додавання програм у білий список і впровадження політики цілісності коду. Це запобігає проникненню шкідливого коду на комп’ютер і скомпрометації операційної системи.

Політики цілісності коду визначають, чи дозволено програмному забезпеченню працювати в Windows 10, тому IT-спеціалісти можуть блокувати доступ до кінцевих пристроїв для невідомих або ненадійних плагінів, програм і доповнень. Windows Defender Application Guard вбудовано в Microsoft Edge, щоб захистити робочий стіл від шкідливих дій. Цей інструмент безпеки запускає сеанси браузера у віртуальній машині (VM), щоб ізолювати їх від робочого столу. Довірені сайти можна додати до білого списку, щоб їм не потрібно було запускати Windows Defender Application Guard, але будь-який інший сайт, до якого потрібно отримати доступ, має відкриватися за допомогою цього інструменту. Сайт працює в ізольованому контейнері Hyper-V.

Windows Defender Credential Guard допомагає запобігти крадіжці облікових даних шляхом ізоляції інформації для входу від загальної операційної системи. За допомогою Credential Guard облікові дані користувача можуть отримати лише привілейовані програми. Щоб запобігти атакам грубої сили, облікові дані зберігаються як рандомізовані повнорозмірні хеші. Облікові дані домену також захищені.

Microsoft SmartScreen SmartScreen — це вбудована функція, яка сканує та запобігає запуску відомих шкідливих програм. Він також порівнює надійність електронних листів і веб-сайтів із чорним списком Microsoft, тож може сповіщати користувачів Windows 10, коли вони намагаються відкрити підозрілий вміст. У поєднанні з традиційним навчанням співробітників з питань кібербезпеки цей хмарний інструмент може забезпечити додатковий рівень захисту від фішингу та атак зловмисного програмного забезпечення.

Microsoft Windows Hello — це функція контролю доступу, яка підтримує біометричну ідентифікацію за допомогою сканерів відбитків пальців, сканерів райдужної оболонки ока та технологій розпізнавання обличчя на сумісних пристроях під керуванням Windows 10. Механізм Hello дозволяє користувачам безпечно входити

на пристрій із необхідними апаратними компонентами, щоб вони не потрібно вводити пароль.

Пісочниця Windows. Якщо адміністратори вирішать дозволити користувачам встановлювати невідомі програми, Windows Sandbox стане ідеальним рішенням. Це дозволяє запускати нові програми в ізольованому віртуальному силосі та уникати повного впливу загроз.

Безпечне завантаження Windows. Функція Secure Boot захищає UEFI/BIOS користувача від програм-вимагачів. Користувачі Windows 10 можуть налаштувати функцію безпечного завантаження таким чином, щоб увесь код, який запускається відразу після запуску операційної системи, мав бути підписаний Microsoft або виробником апаратного забезпечення. UEFI Secure Boot також може створювати точки збереження Windows 10. Безпечне завантаження запобігає встановленню апаратного зловмисного програмного забезпечення, але безпечні точки пропонують систему безпеки, якщо у вас виникнуть проблеми зі встановленням нових програм.

Шифрування Windows BitLocker. Процеси шифрування кодують дані таким чином, що робить їх непридатними для використання неавторизованими користувачами, які не мають ключа дешифрування. Основна перевага шифрування полягає в тому, що воно перетворює дані в нечитабельну форму, яку неможливо використати в разі викрадення. Windows пропонує функцію під назвою BitLocker, яка дозволяє шифрувати цілі диски та запобігати несанкціонованим змінам системи. BitLocker розроблено корпорацією Майкрософт для забезпечення шифрування для дискових томів. Це безкоштовна вбудована функція в багатьох версіях Windows, включаючи Windows Vista та Windows 10. BitLocker запитує у користувачів пароль, генерує ключ відновлення та шифрує весь жорсткий диск.

Покращений набір інструментів для пом'якшення та захист від експлойтів. Enhanced Mitigation Experience Toolkit (EMET) — це інструмент безпеки, розроблений корпорацією Майкрософт для забезпечення захисту та пом'якшення сторонніх і застарілих програм. У версіях Windows 10, починаючи з 1709 і новіших, а також

Windows Server версії 2016 і новіших, EMET постачається як частина функції захисту від експлойтів операційної системи.

Захист інформації Windows. Оскільки все більше організацій дозволяють співробітникам використовувати свої особисті пристрої, зростає ризик випадкового витоку даних. Співробітники використовують багато корпоративних додатків і сервісів, які не можуть контролюватися організацією. Електронні листи, загальнодоступні хмарні служби та платформи соціальних мереж, наприклад, можуть призвести до витоку даних.

Windows Information Protection (WIP) розроблено для захисту від можливого витоку даних, не порушуючи роботу користувача. Раніше відома як захист корпоративних даних, ця послуга спеціально розроблена для зменшення ризиків витоку даних, що виникають через використання власного пристрою (BYOD), включаючи захист як особистих, так і корпоративних пристроїв. WIP не потребує зміни існуючих середовищ. Він пропонується як механізм керування мобільними програмами (MAM - mobile application management) у Windows 10. Можна використовувати WIP для керування застосуванням політики даних для документів і програм у настільних операційних системах Windows 10. Це також може допомогти видалити доступ до даних компанії з усіх пристроїв. WIP може допомогти розділити особисті та корпоративні дані, не змушуючи співробітників перемикатися між програмами чи середовищами. Сервіс також забезпечує захист даних для існуючих бізнес-додатків без необхідності оновлення додатків. Крім того, це дозволяє видаляти дані компанії із зареєстрованих пристроїв Intune mobile device management (MDM) без видалення особистих даних. Ще одна головна перевага WIP полягає в тому, що він надає звіти про аудит, які дозволяють відстежувати проблеми, а також дії для їх усунення. Можна інтегрувати WIP з існуючими системами керування, включаючи Microsoft Endpoint Configuration Manager і Microsoft Intune. Його також можна інтегрувати з існуючими системами MDM, що допоможе вам налаштувати, розгорнути та керувати WIP.

На додаток до використання вбудованих інструментів безпеки Windows, описаних вище, описано додатковий контрольний список для забезпечення належного захисту робочих станцій Windows 10 від загроз безпеці.

Управління програмами. Настійно бажано налаштувати Windows, щоб дозволяти інсталяцію лише схвалених програм із контрольованих сховищ програмного забезпечення або ринків програм. Це може запобігти таким ризикам безпеки: Зловмисники можуть надсилати шкідливі програми електронною поштою користувачеві або використовувати соціальну інженерію, щоб переконати їх завантажити та встановити їх. Навіть якщо потрібен адміністративний доступ на локальній машині для встановлення програмного забезпечення, користувачів можна переконати увійти як адміністратор, щоб установити шкідливу програму. Зловмисники можуть використати інсталяцію програм за допомогою підвищених привілеїв для створення скомпрометованого облікового запису адміністратора на комп'ютері користувача.

Контроль додатків. Багато векторів атак покладаються на виконання шкідливого коду, навіть якщо він не встановлений на пристрої користувача. Білий і чорний список виконуваних файлів у Windows 10 може бути надзвичайно ефективним у запобіганні цим атакам. Рекомендується створити білий список файлів, які дозволено виконувати на машинах кінцевих користувачів, і зробити це з нуля, не покладаючись на файли, які зараз запущені на машині, або список від постачальника програм. Білий список має чітко вказувати виконувані файли, бібліотеки, сценарії та інсталятори, які дозволено виконувати.

Вимкнення віддаленого доступу. Функція віддаленого робочого стола Windows у Windows 10 дозволяє користувачам віддалено підключати свій комп'ютер через мережеве з'єднання. Користувач із віддаленим доступом може керувати комп'ютером так само, як і користувач із прямим доступом. Недоліком віддаленого робочого столу є те, що зловмисники можуть використати віддалений доступ, щоб вирвати контроль над системою та викрасти конфіденційну інформацію або встановити шкідливе

програмне забезпечення. Функцію віддаленого доступу вимкнено за замовчуванням, і користувач може легко вимкнути її після ввімкнення. Обов’язково вимикайте цю функцію, коли користувачі нею активно не користуються.

PowerShell. Корпорація Майкрософт розробила PowerShell для автоматизованого адміністрування системи через інтегрований інтерфейс. Ця потужна мова сценаріїв є центральною функцією набору інструментів системного адміністратора, оскільки вона присутня скрізь і дозволяє легко контролювати середовище Microsoft Windows. На жаль, зловмисники також можуть скористатися цим, щоб повністю контролювати вашу систему. Зокрема, попередні версії PowerShell є небезпечними через їх вразливість у безпеці, тому вам слід видалити PowerShell 2.0 і старіші версії з операційної системи. Для мовного режиму слід встановити обмежений мовний режим, який допоможе вам збалансувати функціональність і потреби безпеки. Служби реагування на інциденти можуть використовувати функції журналювання PowerShell (наприклад, транскрипцію, журналювання модулів і журналювання блоків сценаріїв), щоб отримати важливу інформацію після інциденту безпеки, пов’язаного зі зловмисним використанням PowerShell. Автоматичні оновлення для операційної системи. Переконайтеся, що будь-яке термінове оновлення безпеки встановлено негайно. Чим швидше будуть застосовані нові патчі безпеки, тим швидше можна виправити вразливості та захистити себе від останніх відомих загроз. Ймовірно, організація має політику безпеки для оновлення операційних систем. Користувачів слід поінформувати про цю політику, щоб вони знали, чи слід їм інсталювати оновлення відразу чи дочекатися повідомлень від IT-спеціалістів, коли інсталювати оновлення.

Деякі компанії покладають відповідальність за оновлення операційних систем на IT-команду. Компанії, які використовують старіші версії Windows, піддаються більшому ризику. Наприклад, у січні 2020 року корпорація Майкрософт припинила підтримку Windows 7, тому всі, хто досі нею користується, ризикують піддатися

новим атакам. Тому важливо переконатися, що ваші операційні системи оновлені, перш ніж викриють.

Увімкнути резервне копіювання файлів. Налаштування резервного копіювання файлів на регулярній основі може допомогти запобігти критичній втраті даних під час катастроф, таких як збої обладнання або атаки зловмисного програмного забезпечення. Щоб допомогти захистити дані, Windows 10 пропонує кілька інструментів і функцій, зокрема: використання історії файлів – цей безкоштовний інструмент допоможе легко створювати резервні копії файлів. Створення дисків відновлення – слугує резервними образами, з яких можна відновити систему. Резервне копіювання в хмару – використання хмарних служб зберігання, такі як Dropbox, Google Drive і OneDrive, або корпоративні хмарні рішення для резервного копіювання, щоб постійно створювати резервні копії своїх даних.

Налаштування Forticlient. Рекомендації повинні будуть зазначені для кожного профілю окремо.

Перший профіль – Antivirus:

- Блокування шкідливих сайтів
- Блокувати відомі канали зв’язку, якими користуються зловмисники: ця функція використовує Application Firewall. Якщо програмний брандмауер не ввімкнено, він все одно буде активним, навіть якщо заблокувати Відомі канали зв’язку, які використовують зловмисники:
- Автоматично надсилати підозрілі файли до FortiGuard для аналізу: якщо не обмежено організаційною політикою безпеки, рекомендується ввімкнути цей параметр. Це дозволяє пришвидшити виявлення шкідливих файлів.
- Винятки: дотримуйтеся рекомендацій ОС та інших постачальників програмного забезпечення для налаштування Виключення AV сканування. Важливо налаштувати рекомендовані виключення на серверах.

WebFilter

- Блокування категорії сайтів із загрозою безпеці

- Client Web Filtering When On-Net
- Логування сгенерованого трафіку користувачем

VPN

- Auto Connect
- Enable Local LAN
- Dead Peer Detection: Рекомендується вимкнути цю опцію, коли погане підключення, оскільки ця опція може спричинити розрив з'єднань.
- Включити Implied SPDO
- Auto Keep Alive
- On Connect/On Disconnect Scripts

Vulnerability Scan

- Налаштування сканування за розкладом
- Увімкнути автоматичне виправлення для вразливостей, які мають рейтинг Високий і вище
- Деякі програми, такі як програмне забезпечення Adobe і Java, не можуть бути виправлені автоматично. Для цих програм потрібен ручний патч.

System Settings

- UI > Require Password to Disconnect from EMS: Можна використовувати блокування паролем що дозволить кінцевим користувачам відключати FortiClient від EMS за допомогою налаштованого пароля. Замість того, щоб вимикати опцію відключення користувачів, рекомендується її залишити увімкнути та налаштувати блокування паролем. Це дозволяє адміністраторам відключитися FortiClient використовує налаштований пароль, коли це необхідно та корисно для сценарії усунення несправностей.
- Log > Level: Не рекомендується встановлювати рівень журналу на Debug, за винятком з метою усунення несправностей.
- Update > Use FortiManager for Client Signature Update: Завантаження FortiClient оновлення безпосередньо з серверів FortiGuard. Потрібно переконатися, що

всі кінцеві точки мають доступ до оновлення серверів. Якщо є сервер FortiManager або Micro-FortiGuard для FortiClient, він може використовувати для отримання оновлень сигнатур.

- Endpoint Control > Disable Unregister: Якщо ввімкнено, FortiClient не може відключитися від EMS. Для відключення від EMS рекомендується використовувати запит пароля замість цього[18].

Кращими практиками щодо захисту кінцевих пристроїв є:

- Недовіра усім кінцевим пристроям мережі. Тобто вважати, що кожен пристрії є загрозою корпоративній мережі;
- Використання захищенних протоколів підключення для усіх пристроїв;
- Чітке розділення прав доступу;[19]

Висновки до третього розділу

Побудовано корпоративну мережу в тестовому оточені з чіткою логічною схемою. Встановлено та налаштовано Fortigate з усіма профілями та політиками безпеки.

Продемонстровано налаштування для основних профілів Forticlient: Remote Access, WebFilter, Vulnerability Scan, Malware Protection, Sandox, Firewall, System Settings згідно підмереж\груп мережі компанії. Проаналізовано функціонал на практиці.

Розроблено рекомендації щодо захисту для кінцевих пристроїв згідно з проаналізованими функціями продукту та штатними засобами Windows.

ВИСНОВКИ

В роботі отримано наступні наукові та науково-практичні результати:

1) Розглянуто та проаналізовано основні атаки на кінцеві пристрої корпоративної мережі. Визначено необхідний функціонал для побудови захисту кінцевих пристроїв.

2) Розроблено схему захищеної корпоративної мережі та рекомендації щодо захисту кінцевих точок на основі даних аналізу.

3) Розглянуто функції Forticlient та EMS для захисту кінцевих точок корпоративної мережі. Зазначено сфери використання засобів захисту та можливості використання в цих сферах, зазначено ліцензії та фінкціонал згідно цим ліцензіям. Enterprise Management Server є доволі складним обладнанням, що дає змогу дуже точно бути налаштованим під інфраструктуру компанії та гранулярно розмежувати доступ до тих чи інших ресурсів.

4) Досліджено захист кінцевих пристроїв підприємства, побудову захисту кінцевих пристроїв. Спроєктовано захист кінцевих пристроїв мережі в тестовому оточені. Сформовано рекомендації щодо захисту кінцевих пристроїв та фізичного доступу.

5) Підкреслено, що безпека кінцевих пристроїв є комплексним заходом та повинна постійно вдосконалюватись, щоб мати змогу завжди бути напоготові запобіганню вторгненню. Зазначено, що перевагою цього обладнання є постійне оновлення та підтримка виробником, що є дуже важливим для забезпечення надійного захисту.

ПЕРЕЛІК ПОСИЛАНЬ

1. What is cyberattack? [Електронний ресурс] – Режим доступу: https://www.ibm.com/topics/cyber-attack

2. Endpoint security risks are rising [Електронний ресурс] – Режим доступу: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-endpoint-security-risks-rising.pdf

3. What Are the Different Types of Phishing? [Електронний ресурс] – Режим доступу: https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html

4. What is a whaling phishing attack? [Електронний ресурс] – Режим доступу: https://www.rapid7.com/fundamentals/whaling-phishing-attacks/

5. Barrel Phishing | Beware Of The Conversational Phish [Електронний ресурс] – Режим доступу: https://www.cyberpilot.io/cyberpilot-blog/barrel-phishing-beware-of-the-conversational-phish

6. What Is Ransomware? / Definition and prevention [Електронний ресурс] – Режим доступу: https://www.proofpoint.com/us/threat-reference/ransomware

7. What is adware? Adware definition [Електронний ресурс] – Режим доступу: https://www.malwarebytes.com/adware

8. What Is Fileless Malware? [Електронний ресурс] – Режим доступу: https://www.trellix.com/en-us/security-awareness/ransomware/what-is-fileless-malware.html

9. Advanced persistent threat (APT) [Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

10. Microsoft Office Macros: Still Your Leader in Malware Delivery [Електронний ресурс] – Режим доступу: https://cofense.com/microsoft-office-macros-still-leader-malware-delivery/

11. The different stages of a PowerShell attack [Електронний ресурс] – Режим доступу: https://www.calcomsoftware.com/the-different-stages-of-a-powershell-attack/

12. What is a watering hole attack? Definition and examples [Електронний ресурс] – Режим доступу: https://marketbusinessnews.com/financial-glossary/watering-hole-attack/

13. Supply chain attacks [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware?view=o365-worldwide

14. Cybersecurity in the Remote Work Era: A Global Risk Report [Електронний ресурс] – Режим доступу: https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%

20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf

15. Third Party brached report [Електронний ресурс] – Режим доступу: https://f.hubspotusercontent10.net/hubfs/5234018/Third%20Party%20Breach%20Report%202022%20(2).pdf

16. Fortinet Security Fabric Enables Digital Innovation [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-security-fabric.pdf

17. FortiClient EMS - Best Practices [Електронний ресурс] – Режим доступу: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/b7f6e710-654b-11e9-81a4-00505692583a/FortiClient_EMS-6.2-Best_Practices.pdf

18. Цуранов Микита Олександрович. Захист кінцевих пристроїв корпоративної мережі компанії. ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ». Державний Університет Телекомунікацій. 27 жовтня 2021. Тези доповідей. С. 130 https://dut.edu.ua/uploads/p_2121_20358827.pdf