ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Захищена корпоративна мережа на базі FortiGate NGFW»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олександр МЕЛЬНИК
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
МЕЛЬНИК Олександр
(прізвище, ім'я)

Керівник д.ф. СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 8

ВСТУП ……..…… 9

1 **ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ** ……..….. 11

1.1 Актуальність проблеми захисту корпоративної мережі ……. 11
1.2 Аналіз підходів до захисту корпоративної мережі ……...…….. 17
1.3 Аналіз існуючих рішень для захисту корпоративної мережі ……. 24

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ FORTIGATE NGFW** …….....…. 30

2.1 Призначення та основні функції рішення FortiGate NGFW …..… 30
2.2 Архітектура рішення FortiGate NGFW ……...… 34
2.3 Основні можливості рішення FortiGate NGFW ……. 40

3 **РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ FORTIGATE NGFW** ……..…….……. 43

3.1 Порядок створення системи захисту корпоративної мережі на базі FortiGate NGFW …….. 43
3.2 Рекомендації щодо захисту корпоративної мережі ……..…. 51

ВИСНОВКИ …….. 55

ПЕРЕЛІК ПОСИЛАНЬ 57

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 59

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

APT – Advanced Persistent Threat

CDN – Content Delivery Network

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

IDS – Intrusion Detection System

MPLS – Multiprotocol Label Switching

MSSP – Managed Security Service Provider

NAC – Network Access Control

NGFW – Next Generation Firewall

PCAP – Packet Capture

TDR – Threat Detection and Response

SASE – Secure Access Service Edge

SOC – Security Operations Center

SWG – Secure Web Gateway

VDOMs – Virtual Domains

VPN – Virtual Private Network

WAF – Web Application Firewall

ZTNA – Zero Trust Network Access

ВСТУП

Актуальність дослідження. Корпоративні мережі містять велику кількість цінної інформації, включаючи фінансові дані, персональні дані клієнтів, комерційну таємницю та інші конфіденційні відомості. Кібератаки можуть призвести до викрадення цих даних, що може завдати значної шкоди репутації організації та призвести до юридичних наслідків. Враховуючи постійне зростання кількості та складності кібератак, захист периметру корпоративної мережі є критично важливим для забезпечення безпеки та стабільності бізнесу.

Застосування міжмережевих екранів нового покоління (Next Generation Firewall, NGFW) є критично важливим для сучасних корпоративних мереж, оскільки вони забезпечують багаторівневий захист від складних кіберзагроз.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів захисту корпоративної мережі на базі FortiGate NGFW.

Об'єкт дослідження – захист корпоративної мережі.

Предмет дослідження – методи та засоби захисту корпоративної мережі на базі FortiGate NGFW.

Мета роботи – розробити рекомендації щодо застосування методів та засобів захисту корпоративної мережі.

Наукові завдання:

дослідити сутність проблеми захисту корпоративної мережі;

проаналізувати підходи до захисту корпоративної мережі;

проаналізувати існуючі рішення для захисту корпоративної мережі;

проаналізувати методи та засоби захисту корпоративної мережі на базі FortiGate NGFW;

розробити варіант системи захисту корпоративної мережі на базі FortiGate NGFW.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано варіант системи захисту корпоративної мережі на базі FortiGate NGFW, а також розроблено рекомендації фахівцям з кібербезпеки щодо застосування методів та засобів захисту корпоративної мережі.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1. Актуальність проблеми захисту корпоративної мережі

Microsoft [1] зазначає, що протягом останнього року ландшафт кібернетичних загроз продовжував ставати все більш небезпечним і складним. Зловмисники світу стають все більш забезпеченими ресурсами та краще підготовленими, маючи все більш витончені тактики, методи та інструменти, які кидають виклик навіть найкращим у світі захисникам кібербезпеки. Навіть корпорація Microsoft стає жертвою добре організованих атак рішучих і добре забезпечених зловмисників, і клієнти Microsoft щодня стикаються з понад 600 мільйонами атак кібернетичних зловмисників і атак на державному рівні, починаючи від програм-вимагачів і закінчуючи фішингом і атаками з викраденням персональних даних.

DDoS-атаки продовжували розвиватися, націлюючись на мережевий рівень. У другій половині 2024 року корпорація Microsoft попередила 1,25 мільйона DDoS-атак, що в 4 рази більше, ніж минулого року (рисунок 1.1) [1].

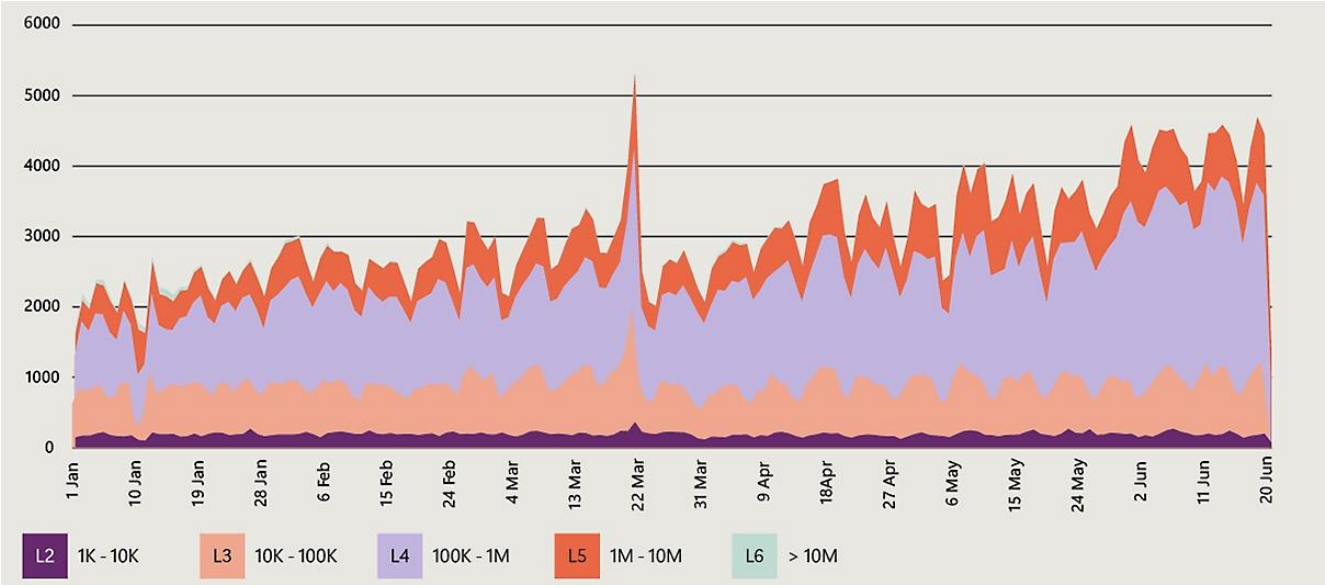

Рис. 1.1. Кількість мережевих DDoS-атак (січень-червень 2024) [1]

На рисунку 1.1 зображено рівні атак на основі кількості пакетів за секунду (pps), позначених наступним кольором: L2 (1K – 10K, фіолетовий), L3 (10K – 100K, світло-помаранчевий), L4 (100K – 1M, лавандовий), L5 (1M – 10M, темно-помаранчевий) і L6 (>10M, зелений).

На графіку видно помітне збільшення атак рівня 4 (L4), особливо приблизно в середині березня, з піком приблизно 20 березня та 15 травня. Атаки на прикладному рівні більш приховані, складні, і їх важко подолати, ніж атаки на мережевому рівні [1].

Microsoft [1] зазначає, що організації повинні визначити найбільш імовірні шляхи кібератак, що ведуть до критичних активів, і постійно зменшувати ступінь їх впливу. Аналіз шляху кібератаки включає інвентаризацію активів, дані про вразливості та зовнішні фактори кібератак, щоб створити можливий ланцюжок кібератак, що веде до критичного активу.

Рис. 1.2. Аналітика шляху атаки для захисту на основі даних про загрозу [1]

На рисунку 1.2 показано, що [1]:

10% шляхів атак містять три або менше кроків;

90% організацій вразливі принаймні перед одним шляхом атаки;

61% шляхів атак ведуть до вразливих облікових записів користувачів;

3% організацій незахищені від понад 1000 шляхів атак;

40% шляхів атак включають бокове зміщення на основі неінтерактивного віддаленого виконання коду;

80% організацій мають шляхи атак, які загрожують критичним ресурсам;

<1% ресурсів організації дуже цікавлять зловмисників.

Найпоширенішими методами початкового доступу залишаються соціальна інженерія, зокрема фішинг електронної пошти, фішинг SMS і голосовий фішинг, компрометація ідентифікаційної інформації та використання вразливостей у загальнодоступних програмах або операційних системах без виправлень. Зловмисники продовжують використовувати нещодавно виявлені загальні вразливості та ризики (CVE) із загальною системою підрахунку вразливостей (CVSS) має оцінки вище 8. Коли зловмисник потрапляє в мережу, він втручається в продукти безпеки або встановлює інструменти віддаленого моніторингу та керування (RMM), щоб вимкнути або уникнути виявлення та залишатися в мережі [1].

Microsoft спостерігали віддалене шифрування в 70% успішних атак, причому 92% походили з некерованих пристроїв у мережі, що підкреслювало необхідність для організацій реєструвати пристрої для керування або виключати некеровані пристрої з мережі [1].

SentinelOne [2] зазначають, що кіберзагрози розвиваються з шаленою швидкістю, оскільки зловмисники стають все більш витонченими, а кількість підключених пристроїв у всьому світі продовжує зростати. Їх дослідження показує, що минулого року було виявлено понад 30 000 вразливостей, що на 17 відсотків більше, ніж попередні дані, і відображає стабільне зростання кіберризиків. Зі зростанням віддаленої роботи та впровадження хмарних технологій кінцеві точки та потоки даних стають привабливими цілями для атак.

Оскільки безпека на основі периметра втрачає актуальність, нульова довіра стає новою модною тенденцією. Нульова довіра надає повний доступ лише після

початкової автентифікації, а потім повторно перевіряє кожен запит. На тлі горизонтального переміщення, що є ознакою складних порушень, цей підхід надає важливий варіант для захисників. Нульова довіра є однією з головних тенденцій кібербезпеки у 2025 році, оскільки все більше організацій впроваджують мікросегментацію, перевірку контексту користувачів та постійний моніторинг сеансів [2].

В [4] зазначається, що уряди інвестуватимуть у модернізовані та безпечні системи, особливо з огляду на посилення атак національних держав на критичну інфраструктуру. Ці зусилля виходять за рамки заміни застарілих технологій і зосереджуються на впровадженні інтелектуальних технологій, одночасно захищаючи як застарілу, так і нову інфраструктуру для задоволення потреб цифрового світу.

Багато критично важливих середовищ, включаючи промислові об’єкти та віддалені об’єкти, стикаються з унікальними проблемами захисту інфраструктури. Посилені NGFW є важливим рішенням для цих умов, забезпечуючи надійний захист у місцях, де традиційне обладнання може вийти з ладу. Зі зростанням загроз та складністю захисту пристроїв Інтернету речей та OT, надійний підхід до видимості та захисту є надзвичайно важливим [4].

У 2025 році однією з найбільш тривожних тенденцій у кібербезпеці стане зростаюче використання багатовекторних атак та багатоетапних підходів. Як це працює? Кіберзлочинці використовують комбінацію тактик, методів та процедур (TTP), атакуючи одночасно на кілька областей для порушення захисту. Ми побачимо зростання витонченості та ухилення від веб-атак, атак на основі файлів, атак на основі DNS та атак програм-вимагачів, що ускладнить ефективний захист від сучасних загроз традиційними, ізольованими інструментами безпеки [4].

Розглянемо основні типи загроз безпеці, які можуть вплинути на мережу організації.

Шкідливе програмне забезпечення та програми-вимагачі. Шкідливе програмне забезпечення (скорочення від malware software) стосується широкої категорії шкідливих програм, включаючи віруси, черв’яків, трояни, шпигунські

програми та програми-вимагачі. Ці програми проникають у мережі, щоб викрадати дані, порушувати роботу або надавати зловмисникам віддалений доступ. Шкідливе програмне забезпечення може поширюватися через заражені вкладення електронної пошти, шкідливі завантаження, скомпрометовані веб-сайти та вразливості програмного забезпечення.

Програми-вимагачі – один із найшкідливіших типів шкідливих програм. Вони шифрують файли або цілі системи та вимагають оплату в обмін на ключ розшифрування. Деякі штами програм-вимагачів також викрадають дані перед шифруванням, погрожуючи витоком конфіденційної інформації, якщо викуп не буде сплачено. Гучні атаки програм-вимагачів спрямовані на організації, заклади охорони здоров'я та державні установи.

Фішинг та соціальна інженерія. Фішинг – це метод кібератаки, за якого зловмисники видають себе за довірені особи, щоб обманом змусити людей розкрити конфіденційну інформацію, таку як облікові дані для входу, банківські реквізити або особисті дані. Фішингові електронні листи часто містять шкідливі посилання або вкладення, які встановлюють шкідливе програмне забезпечення або перенаправляють жертв на шахрайські веб-сайти, призначені для крадіжки інформації.

Соціальна інженерія виходить на новий рівень фішингу, використовуючи людську психологію. Зловмисники маніпулюють людьми, змушуючи їх обходити протоколи безпеки, часто створюючи відчуття терміновості або довіри. Поширені тактики соціальної інженерії включають претекстування (вигадування сценарію для отримання інформації), цькування (пропонування фальшивих стимулів) та стеження за уповноваженим персоналом (фізичне переслідування уповноваженого персоналу в обмежені зони).

Атаки типу «відмова в обслуговуванні» (DoS/DDoS). Атака типу «відмова в обслуговуванні» (DoS) спрямована на порушення доступності мережі, сервера або веб-сайту шляхом перевантаження його надмірним трафіком або запитами на ресурси. Більш серйозний варіант, розподілена атака типу «відмова в обслуговуванні» (DDoS), передбачає кілька скомпрометованих пристроїв, часто

входять до складу ботнету, які координовано працюють, щоб затопити цільову систему шкідливим трафіком, роблячи її недоступною для законних користувачів.

DDoS-атаки можуть паралізувати роботу онлайн-сервісів, спричиняючи фінансові втрати, шкоду репутації та операційні збої. Зловмисники використовують різні методи, такі як волюметричні атаки (перевантаження пропускної здатності), атаки на протоколи (використання слабких місць у мережевих протоколах) та атаки на рівні додатків (націлені на веб-додатки).

Розширені постійні загрози (APT). Розширені постійні загрози (APT) – це тривалі, високотехнологічні кібератаки, під час яких зловмисники отримують несанкціонований доступ до мережі та залишаються непоміченими протягом тривалого часу. Ці атаки часто здійснюються державними групами або добре фінансованими кіберзлочинними організаціями, спрямованими на урядові установи, корпорації та інфраструктуру.

APT зазвичай включають кілька етапів атаки, включаючи розвідку, початкову компрометацію (наприклад, через фішинг або експлойти нульового дня), ескалацію привілеїв, витік даних та методи збереження даних для підтримки довгострокового доступу. Ці атаки спрямовані на крадіжку інтелектуальної власності, порушення операцій або збір розвідувальних даних з часом.

Завантаження через Drive-By та атаки типу «людина посередині». Завантаження шкідливого програмного забезпечення відбувається, коли користувачі ненавмисно завантажують та встановлюють шкідливе програмне забезпечення, просто відвідуючи скомпрометований веб-сайт. Зловмисники використовують вразливості у веббраузерах, плагінах або застарілому програмному забезпеченні для запуску шкідливого програмного забезпечення без взаємодії з користувачем. Завантаження шкідливого програмного забезпечення може призвести до зараження програмами-вимагачами, розгортання шпигунських програм або захоплення системи.

Атаки типу «людина посередині» (MitM) передбачають перехоплення та зміну комунікацій між двома сторонами без їхнього відома. Зловмисники розміщуються між користувачами та легітимними сервісами, щоб викрасти

облікові дані, змінити транзакції або впровадити шкідливий контент. Поширені методи MitM включають прослуховування Wi-Fi, захоплення сеансів та видалення SSL-сертифіката.

Внутрішні загрози. Внутрішні загрози походять від окремих осіб в організації, таких як співробітники, підрядники або ділові партнери, які зловживають своїм доступом, щоб завдати шкоди організації. Ці загрози можуть бути навмисними (зловмисники, які прагнуть фінансової вигоди, помсти або шпигунства) або ненавмисними (недбайливі інсайдери, які випадково розкривають дані через погані методи безпеки).

Зловмисники можуть красти конфіденційні дані, впроваджувати шкідливе програмне забезпечення або саботувати системи. Натомість, недбалі інсайдери можуть стати жертвами фішингових шахрайств, повторно використовувати слабкі паролі або неправильно поводитися з конфіденційною інформацією, що збільшує ризик кіберінцидентів.

У 2025 році мережева безпека буде більш динамічною, інноваційною та проактивною, ніж будь-коли раніше, трансформуючи способи захисту організацій своїх найцінніших активів та забезпечуючи безпечне, стійке майбутнє в умовах постійно мінливого цифрового світу [4].

1.2. Аналіз підходів до захисту корпоративної мережі

У сучасному цифровому світі організації всіх розмірів стикаються з дедалі більшою кількістю та складністю кіберзагроз. Зловмисники постійно розробляють нові методи проникнення в корпоративні мережі, що ставить під загрозу безперервність бізнесу, фінансову стабільність і репутацію компаній. У той час як традиційне поняття чітко визначеного мережевого периметру зазнало змін через поширення хмарних технологій, віддаленої роботи та пристроїв Інтернету речей (IoT), необхідність захисту меж цифрових активів організації залишається надзвичайно важливою.

Мережевий периметр є, по суті, захищеною межею, яка відокремлює

приватну, внутрішньо керовану мережу організації від публічного Інтернету або будь-яких інших зовнішніх, неконтрольованих мереж. Його можна розглядати як цифровий еквівалент фізичного кордону, що визначає межі контролю організації над своїми цифровими активами.

Мережева безпека передбачає захист мереж від несанкціонованого доступу, неправильного використання, несправностей, модифікації, знищення або неналежного розголошення. Вона забезпечує конфіденційність, цілісність та доступність (CIA) мережевих даних і ресурсів. Ця дисципліна включає технології, процеси та політики для захисту мереж від внутрішніх та зовнішніх загроз [3].

Мережева безпека включає низку тактик, від апаратних рішень, таких як мережеві екрани, до програмного забезпечення для виявлення загроз. Вона має вирішальне значення для підтримки бізнес-операцій та захисту конфіденційних даних від кіберзлочинців та інших зловмисників. Впроваджуючи заходи мережевої безпеки, організації можуть зменшити ризики та запобігти витокам даних і збоям у роботі системи [3].

Розглянемо архітектуру та моделі мережевої безпеки.

Глибокоешелонований захист – це багаторівневий підхід до захисту мереж шляхом впровадження кількох захисних механізмів. Замість того, щоб покладатися на один захід безпеки, ця модель гарантує, що у разі збою одного рівня додаткові рівні забезпечать постійний захист.

Ключові компоненти глибоко ешелонованого захисту включають [3]:

безпека периметра: мережеві екрани, системи запобігання вторгненням (IPS) та засоби контролю доступу запобігають несанкціонованому доступу;

захист кінцевих точок: антивірусне програмне забезпечення, засоби виявлення та реагування на кінцеві точки (EDR) і керування виправленнями захищають окремі пристрої;

безпека даних: Шифрування, контроль доступу та запобігання втраті даних (DLP) захищають конфіденційну інформацію;

обізнаність користувачів: навчання з безпеки та симуляції фішингу допомагають запобігти атакам соціальної інженерії;

моніторинг та реагування: системи управління інформацією та подіями безпеки (SIEM) та розвідка про загрози дозволяють швидко виявляти загрози та пом’якшувати їх.

NIST [16] визначає мережеві екрани як пристрої або програми, які контролюють потік мережевого трафіку між мережами або хостами, що використовують різні засоби безпеки. Хоча мережеві екрани часто обговорюються в контексті підключення до Інтернету, вони також можуть мати застосування в інших мережевих середовищах. Наприклад, багато корпоративних мереж використовують мережеві екрани для обмеження підключення до внутрішніх мереж та з них, що використовуються для обслуговування більш чутливих функцій, таких як бухгалтерський облік або персонал. Використовуючи брандмауери для контролю підключення до цих областей, організація може запобігти несанкціонованому доступу до своїх систем та ресурсів.

Розглянемо архітектуру нульової довіри.

Архітектура нульової довіри (ZTA) – це система безпеки, що базується на принципі «ніколи не довіряй, завжди перевіряй». На відміну від традиційних моделей безпеки, які передбачають довіру в межах периметра мережі, нульова довіра вимагає постійної автентифікації, авторизації та моніторингу для кожного користувача та пристрою, які отримують доступ до ресурсів.

Основні принципи нульової довіри включають [3]:

керування ідентифікацією та доступом (IAM): багатофакторна автентифікація (MFA) та доступ з мінімальними привілеями гарантують, що доступ до ресурсів матимуть лише авторизовані користувачі;

мікросегментація: сегментація мережі обмежує горизонтальне переміщення, обмежуючи доступ на основі ролей користувачів та положення пристрою;

безперервний моніторинг: аналітика на основі штучного інтелекту та виявлення загроз на основі поведінки допомагають виявляти аномалії та потенційні загрози;

шифрування та безпечний доступ: безпечне тунелювання, таке як віртуальні приватні мережі (VPN) та мережевий доступ з нульовою довірою (ZTNA), захищає

дані під час передачі.

Сегментація мережі поділяє мережу на менші, ізольовані сегменти для контролю потоку трафіку та обмеження поширення кіберзагроз. Ця стратегія покращує безпеку, продуктивність та відповідність вимогам, обмежуючи несанкціонований доступ до критично важливих систем. Вона допомагає запобігти горизонтальному переміщенню зловмисників та зменшити вплив порушень [3].

Типи сегментації мережі [3]:

фізична сегментація: використовує окреме обладнання, таке як маршрутизатори та комутатори, для ізоляції сегментів мережі;

логічна сегментація: Реалізація віртуальних локальних мереж (VLAN) та програмно-визначених мереж (SDN) для розділення трафіку в межах спільної інфраструктури;

мікросегментація: використовує детальні політики для контролю доступу на рівні робочого навантаження або програми, зменшуючи вектори атак.

Видимість та моніторинг мають вирішальне значення для виявлення та реагування на кіберзагрози в режимі реального часу. Організації повинні постійно контролювати мережеву активність, щоб виявляти підозрілу поведінку та зм'якшувати ризики.

Ключові компоненти, які забезпечують видимість та моніторинг, включають:

управління інформацією та подіями безпеки (SIEM): централізоване ведення журналу та кореляція подій безпеки допомагають виявляти аномалії;

аналіз мережевого трафіку (NTA): моніторить потоки даних для виявлення несанкціонованого доступу або активності шкідливого програмного забезпечення;

виявлення та реагування на кінцеві точки (EDR): надає детальну інформацію про загрози безпеці кінцевих точок та автоматизує реагування на інциденти;

розвідка загроз: використовує зовнішні джерела даних для виявлення нових загроз та вразливостей.

Розглянемо основні методи та інструменти мережевої безпеки.

Стратегії мережевої безпеки включають різні рішення для захисту від різних мережевих загроз. Ось деякі з основних з них.

Мережеві екрани діють як бар’єр між довіреними та недовіреними мережами. Вони відстежують та контролюють вхідний і вихідний трафік на основі попередньо визначених правил безпеки. Мережеві екрани мають вирішальне значення для забезпечення дотримання політик безпеки мережі, запобігання несанкціонованому доступу та зменшення таких загроз, як шкідливе програмне забезпечення та DDoS-атаки.

Існує кілька типів мережевих екранів [3]:

мережеві екрани фільтрації пакетів: перевіряють окремі пакети та дозволяють або блокують їх на основі IP-адреси джерела/приймача, порту та протоколу;

мережеві екрани з перевіркою стану: відстежують активні з’єднання та приймають рішення щодо фільтрації на основі стану з’єднання;

проксі-брандмауери: діють як посередники між користувачами та сервісами, фільтруючи трафік та маскуючи внутрішні IP-адреси;

мережеві екрани наступного покоління (NGFW): поєднують традиційні функції брандмауера з глибокою перевіркою пакетів, запобіганням вторгненням та обізнаністю про програми.

Антивірусні рішення виявляють, запобігають появі та видаляють шкідливе програмне забезпечення, включаючи віруси, трояни, черв’яки, шпигунські програми та програми-вимагачі. Ці інструменти використовують виявлення на основі сигнатур, евристичний аналіз та методи на основі поведінки для виявлення загроз.

Сучасні рішення інтегрують штучний інтелект та машинне навчання для розпізнавання нових загроз, пропонуючи захист у режимі реального часу від шкідливого програмного забезпечення, що постійно розвивається. Рішення для виявлення та реагування на кінцеві точки (EDR) забезпечують покращені можливості, такі як безперервний моніторинг та автоматизоване усунення загроз [3].

Системи виявлення та запобігання вторгненням (IDPS) виявляють та усувають шкідливу діяльність у мережі [3]:

системи виявлення вторгнень (IDS): моніторять мережевий трафік на наявність підозрілих шаблонів і генерують сповіщення про виявлення загроз;

системи запобігання вторгненням (IPS): розширюють функціональність IDS, активно блокуючи або пом’якшуючи виявлені загрози.

Рішення IDPS аналізують трафік за допомогою методів виявлення на основі сигнатур, аномалій або гібридних методів. Вони допомагають запобігати кібератакам, таким як SQL-ін’єкції, атаки методом повного перебору та експлойти нульового дня.

Віртуальні приватні мережі (VPN) створюють зашифровані тунелі між віддаленими користувачами та корпоративними мережами, забезпечуючи безпечну передачу даних через загальнодоступні або ненадійні мережі. Хоча VPN покращують безпеку та конфіденційність, вони все частіше доповнюються мережевим доступом з нульовою довірою для більш детального контролю доступу.

Типи VPN включають [3]:

VPN-мережі віддаленого доступу: дозволяють співробітникам безпечно підключатися до корпоративних мереж з будь-якого місця;

VPN-мережі типу «сайт-сайт»: безпечне з’єднання кількох офісів через Інтернет.

Контроль доступу до мережі (NAC) застосовує політики безпеки для регулювання доступу пристроїв у мережі. Він гарантує, що підключатися можуть лише автентифіковані та відповідні пристрої. NAC підвищує безпеку, запобігаючи доступу неавторизованих або скомпрометованих пристроїв до конфіденційних ресурсів.

Функції NAC включають [3]:

автентифікація та авторизація: перевіряє ідентифікаційні дані користувачів та призначає рівні доступу;

перевірки відповідності кінцевих точок: забезпечує відповідність пристроїв вимогам безпеки (наприклад, оновлена ОС, антивірус).

Контроль доступу на основі ролей (RBAC): обмежує доступ до мережі на основі ролей користувачів.

Рішення для запобігання втраті даних (DLP) запобігають несанкціонованому передаванню даних, моніторячи та контролюючи конфіденційну інформацію в мережах, кінцевих точках і хмарних середовищах. Технології шифрування захищають дані в стані спокою, під час передачі та використання, перетворюючи їх у нечитабельні формати, забезпечуючи конфіденційність навіть у разі перехоплення.

Функції DLP включають [3]:

перевірка вмісту: сканує файли та електронні листи на наявність конфіденційних даних;

застосування політик: блокує, шифрує або реєструє несанкціоновані передачі даних.

управління відповідністю: забезпечує дотримання правил захисту даних, таких як GDPR та HIPAA.

Безпечні веб-шлюзи (SWG) фільтрують інтернет-трафік, щоб блокувати шкідливий контент, забезпечувати дотримання політик і запобігати витоку даних. Вони забезпечують захист від фішингу, шкідливого програмного забезпечення та шкідливих веб-сайтів.

Рішення для захисту електронної пошти виявляють і блокують такі загрози, як фішинг, спуфінг і вкладення, завантажені шкідливим програмним забезпеченням. Такі технології, як автентифікація, звітування та відповідність повідомлень на основі домену (DMARC), допомагають автентифікувати відправників електронних листів і запобігати шахрайству з електронною поштою.

Рішення для виявлення та реагування на мережу (NDR) використовують штучний інтелект та поведінкову аналітику для виявлення аномалій та складних загроз у мережевому трафіку. Вони виявляють підозрілу активність, яку традиційні засоби безпеки можуть пропустити.

Рішення для керування інформацією та подіями безпеки (SIEM) агрегують та аналізують журнали з кількох джерел безпеки, що дозволяє виявляти загрози в режимі реального часу та звітувати про відповідність вимогам. SIEM інтегрується з інструментами оркестрації безпеки, автоматизації та реагування (SOAR) для

автоматизованого реагування на інциденти.

Безпечний доступ до сервісу на межі (SASE) – це хмарна система безпеки, яка поєднує мережеві та безпекові функції в єдину послугу. Вона інтегрує SD-WAN, мережевий доступ з нульовою довірою (ZTNA), брокерів безпеки хмарного доступу (CASB), брандмауер як послугу (FWaaS) та безпечні веб-шлюзи (SWG).

Переваги SASE включають [3]:

безпечне та масштабоване підключення: забезпечує узгоджені політики безпеки для віддалених та локальних користувачів;

покращена продуктивність: зменшує затримку, надаючи послуги безпеки ближче до користувача;

спрощене управління безпекою: централізоване застосування політик у хмарних та локальних середовищах.

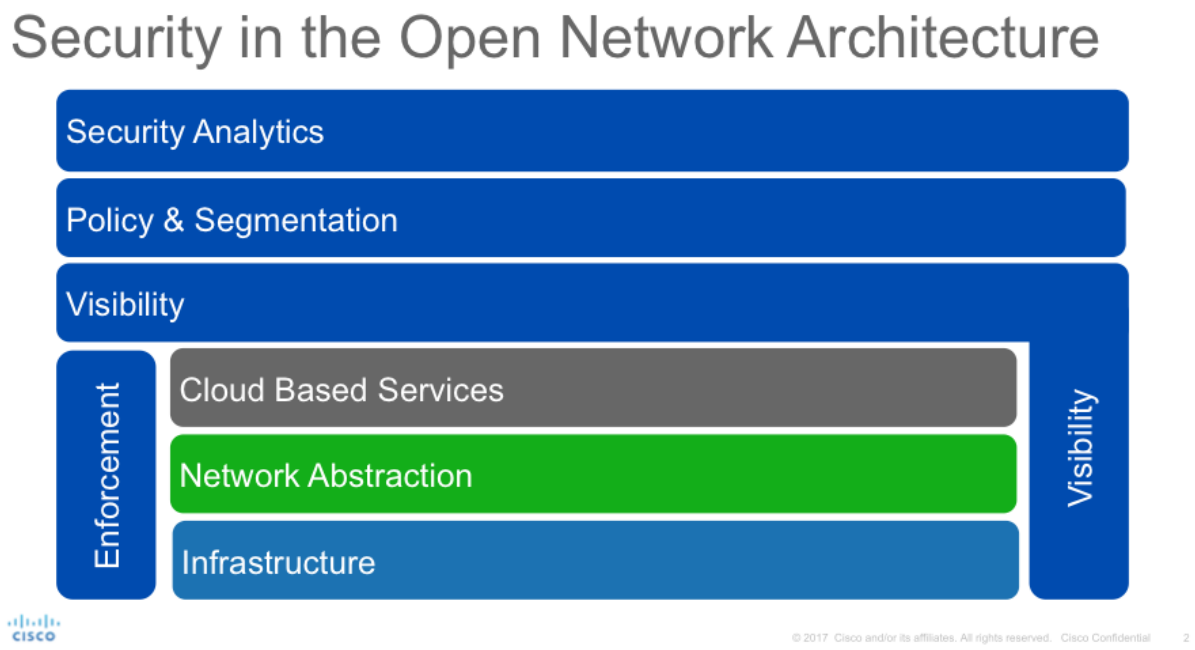

Рис. 1.3. Відкрита мережева архітектура [8]

У [8] звертається увага на необхідність всеохоплюючих підходів до безпеки та архітектури корпоративної мережі, щоб забезпечити безпечні та гнучкі сервіси проти дедалі складніших зловмисників. Всеохоплююча безпека є критично важливою для відкритої мережевої архітектури (ONA) (рисунок 1.3) [8].

1.3. Аналіз існуючих рішень для захисту корпоративної мережі

Мережеві екрани наступного покоління (NGFW) виступають першою лінією захисту організації від кіберзагроз. Вони перевіряють та фільтрують весь трафік, що входить та виходить з корпоративної мережі, щоб блокувати спроби зараження шкідливим програмним забезпеченням та витоку даних [10].

NGFW розширюють можливості традиційних мережевих екранів, не лише виявляючи шкідливе програмне забезпечення, але й блокуючи його до того, як воно проникне в мережу. Завдяки розширеним функціям виявлення та реагування на загрози, мережеві екрани наступного покоління забезпечують комплексний захист у центрах обробки даних, корпоративних мережах та хмарних середовищах, зміцнюючи свою роль як основи сучасних стратегій кібербезпеки [9].

Для посилення безпеки організації вкрай важливо регулярно переглядати можливості NGFW. Зростаюча складність кібератак спонукає підприємства впроваджувати NGFW, заохочуючи постачальників постійно впроваджувати інновації та вдосконалювати свої пропозиції. Сучасні NGFW мають критично важливі можливості, такі як обізнаність про додатки, централізоване управління та глибока перевірка пакетів (DPI). Крім того, багато з них забезпечують розширені функції, включаючи захист від загроз зі швидкістю 100 Гбіт/с та гібридну хмарну безпеку, для боротьби зі загрозами, які обходять традиційні засоби захисту периметра [9].

Завдяки впровадженню передових технологій запобігання загрозам, NGFW оснащують команди IT-безпеки інструментами для захисту від шкідливого програмного забезпечення, спроб вторгнення та інших складних атак. Ці розширені можливості роблять NGFW незамінним компонентом екосистеми кібербезпеки будь-якої організації [9].

Найкращі NGFW оснащені розширеними функціями, такими як системи виявлення та запобігання вторгненням (IDS/IPS), веб-проксі та фільтрація URL-адрес, а також брандмауер веб-додатків (WAF). Вони також підтримують

віртуальні розгортання для хмарних середовищ і можуть легко захистити філії або мережі одного підприємства. Ці функції є вирішальними для захисту від сучасних загроз, одночасно покращуючи видимість додатків і мережі [9].

Компанія Palo Alto Networks продовжує лідирувати на ринку NGFW, визнана лідером у звіті Forrester's Q4 2024 Enterprise Firewalls Wave. Їхній портфель NGFW включає фізичні (серія PA), віртуалізовані (серія VM) та контейнеризовані (серія CN) мережеві екрани, всі з яких базуються на однопрохідній архітектурі, яка перевіряє весь трафік – додатки, загрози та контент – одночасно прив’язуючи його до користувача, незалежно від місцезнаходження чи пристрою. Завдяки інтеграції хмарного механізму ідентифікації та підтримці безпеки SaaS через CASB, Palo Alto Networks пропонує комплексний захист для гібридних та багатохмарних середовищ [9].

Palo Alto Networks розвиває свої сильні сторони завдяки передовому штучному інтелекту та машинному навчанню, забезпечуючи захист у режимі реального часу від загроз нульового дня та програм-вимагачів. Їхні рішення поширюються на безпеку Інтернету речей та операційних систем завдяки таким функціям, як мікросегментація, поведінкова аналітика та видимість пристроїв. Ці інновації зміцнюють роль Palo Alto Networks як наріжного каменю для організацій, що впроваджують стратегії нульової довіри та гібридної хмари [9].

NGFW Fortinet FortiGate відомі своєю високою продуктивністю та комплексними функціями безпеки. Побудовані на єдиній операційній системі, FortiGate NGFW забезпечують стабільний захист у фізичних, віртуальних та хмарних середовищах, ефективно захищаючи різні межі мережі будь-якого масштабу. Вони інтегрують розширені можливості, такі як запобігання вторгненням, контроль програм та захист від шкідливого програмного забезпечення, забезпечуючи комплексну безпеку через єдину платформу [9].

У 2024 році компанія Fortinet представила серію FortiGate 200G, розроблену для підвищення безпеки кампусної мережі. Ця серія, що працює на базі блоку обробки даних п’ятого покоління (SP5), пропонує підвищену пропускну здатність мережевого екрану, виявлення загроз на основі штучного інтелекту та порти 5GE

для підтримки найновішого стандарту Wi-Fi 7. Ці функції дозволяють організаціям ефективно керувати та захищати зростаючі обсяги трафіку, багатого на дані, та хмарних додатків.

Крім того, Fortinet було визнано лідером у звіті The Forrester Wave: Enterprise Firewall Solutions за 4 квартал 2024 року, що підкреслює його прагнення надавати передові мережеві та безпекові можливості за допомогою рішень FortiGate NGFW [9].

Cisco Secure Firewall – це рішення NGFW, яке поєднує в собі розширений захист від загроз, видимість додатків та єдине управління політиками. Воно забезпечує однакову безпеку у фізичних, віртуальних та хмарних середовищах, гарантуючи стабільний захист та спрощені операції [9].

Cisco Secure Firewall визнано лідером у звіті The Forrester Wave: Enterprise Firewall Solutions за 4 квартал 2024 року та пропонує передові можливості безпеки на основі штучного інтелекту, адаптовані до потреб сучасних підприємств. Завдяки штучному інтелекту та машинному навчанню, що забезпечують автоматизоване управління політиками та видимість зашифрованого трафіку, Cisco забезпечує проактивний захист від нових загроз. Його багаторівневий підхід до перевірки, включаючи механізм SnortML, забезпечує ефективне запобігання вторгненням, гарантуючи комплексну безпеку для різноманітних мережевих архітектур. Ці функції позиціонують Cisco як надійного партнера для організацій, які шукають масштабовані та адаптивні рішення для брандмауерів [9].

Таблиця 1.1

Порівняльний аналіз рішень NGFW [10]

	Check Point	PAN	Fortinet	Cisco
BUILT-TO-PREVENT	✓ Real-Time Prevention	✗ Prevention after the fact	✗ Prevention after the fact	✗ Prevention after the fact
IDENTIFICATION (apps/users/devices)	✓ Over 10,080, **up to 60% better visibility**	✗ Limited apps library ~4,300	✗ Limited apps library ~5,000	✗ Limited apps library ~6,000
INSPECTION WITHIN SSL/TLS	✓	✓	✓	✓
GOING BEYOND SIGNATURE-BASED DEFENSES	✓	✗ Partial coverage	✗ Partial coverage	✗ Partial coverage
ZERO-TRUST APPROACH	✓	✓	✓	✓
SHARED THREAT INTELLIGENCE MEANS BETTER SECURITY. AUTOMATED	✓	✓	✓	✓
UNIFIED MANAGEMENT CONFIGURATION	✓ 7 menu management	✗ **5x more effort-** 35 menus and significantly more time for same task	✗ **3x more effort-** 22 menus and significantly more time for same task	✗ **5x more effort-** 38 menus and significantly more time for same task
SECURITY FROM THE START Vulnerabilities on vendors' own security products 2020-2023 (lower is better)	✓ Only 38 vulnerabilities at start	✗ **4x more-** 162 vulnerabilities at start	✗ **9x more-** 339 vulnerabilities at start	✗ **10x more-** 357 vulnerabilities at start

Check Point є лідером галузі з виробництва NGFW, і Gartner визнає його лідером у цій галузі вже 22 роки. Деякі з особливостей, що відрізняють Check Point NGFW від інших постачальників, включають [10]:

найкраща операційна ефективність: Check Point Security Management – це найінтегрованіша та найнадійніша в галузі платформа для управління безпекою

будь-якого розміру;

перевірений та найстабільніший досвід: Check Point є лідером у сфері мережевої безпеки з 1997 року;

безпека понад усе: Check Point створює та розробляє свої рішення безпеки безпечно – з самого початку;

найкраща профілактика: запобігання загрозам у режимі реального часу є основною філософією рішень Check Point;

найкраща у своєму класі гіпермасштабна платформа: гіпермасштабні рішення Check Point забезпечують зростання з найкращою рентабельністю інвестицій у галузі.

Постачальники NGFW надають безліч можливостей безпеки для корпоративної мережі на периферії, центрів обробки даних та хмарних додатків за допомогою фізичних, віртуальних та контейнерних брандмауерів. Однак важливо зазначити, що, за даними Gartner [9], 99% порушень мережевих екранів є наслідком неправильних конфігурацій, а не недоліків самих пристроїв.

Необхідно відмітити, що кожна організація унікальна, і потрібно обирати рішення, адаптоване до конкретних потреб, одночасно дотримуючись галузевих стандартів і передових практик.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ FORTIGATE NGFW

2.1. Призначення та основні функції рішення FortiGate NGFW

У сучасному цифровому середовищі компанії стикаються з постійно зростаючим масивом кіберзагроз, які можуть поставити під загрозу їхню діяльність, дані та репутацію. Мережеві екрани – це перший захист для корпоративних мереж від витоків даних. Надійний NGFW має вирішальне значення для сучасних організацій, оскільки він пропонує розширені можливості безпеки та детальну видимість, що перевершує традиційний мережевий екран. NGFW інтегрують комплексну аналітику загроз, глибоку перевірку пакетів та обізнаність про програми для захисту від складних атак та вразливостей. Поєднуючи ці функції, NGFW підвищують безпеку та забезпечують операційну ефективність і безперервність бізнесу, що робить їх важливими інструментами для захисту сучасних складних та динамічних IT-середовищ [12].

У корпоративній мережі багато ресурсів може бути розташовано в корпоративній мережі в головному офісі або філіях. Вони можуть бути додатково розділені на спільні та індивідуальні ресурси та додатки, а також на різні типи пристроїв. Загалом, ці ресурси не слід неявно розміщувати в одній зоні довіри лише тому, що вони розташовані в одному офісі або в одному відділі.

Використання сегментації та мікросегментації може допомогти організувати ресурси в групи, що зробить адміністраторами мережі інтуїтивніше адміністрування доступу. Наприклад, під час використання функцій керування доступом до мережі (NAC) на мережевому екрані наступного покоління (NGFW) або інтелектуальному комутаторі, пристрої можна ідентифікувати на основі їх MAC-адреси, типу постачальника, версії програмного забезпечення тощо. Наприклад, VoIP-телефони в мережі певного відділу можна групувати в окремий мікросегмент, де віддалений доступ заборонено. ПК в мережі відділу можна

групувати в різні мікросегменти, які дозволяють віддалений доступ через RDP.

Zero Trust Network Access (ZTNA) – це продукт або послуга, яка захищає програми, дозволяючи доступ до програми лише довіреним особам. Довіра визначається брокером довіри, який постійно перевіряє ідентифікацію та контекст підключаючої особи, одночасно здійснюючи контроль доступу на основі цих факторів. Горизонтальні переміщення в межах захищеної програми та мережі обмежені, що ще більше зменшує поверхню атаки для скомпрометованих хостів.

ZTNA вважає, що жодні користувачі чи пристрої не є довіреними, доки брокер довіри не підтвердить, що пристрій та користувач є тими, ким вони є, а їхній рівень безпеки відповідає стандартам компанії. Це значно зменшує несанкціонований доступ з невідомого пристрою з викраденими обліковими даними та ймовірність доступу скомпрометованого хоста до захищених ресурсів. Контроль доступу на основі ролей зменшує горизонтальні переміщення та підтримує аналогічний контроль доступу на основі рівнів доступу незалежно від місцезнаходження.

FortiGate є основою Fortinet Security Fabric, незалежно від того, чи розгорнуто воно на периферії, у хмарі чи як внутрішній сегментаційний мережевий екран. В архітектурі ZTNA FortiGate діє як брокер довіри для консолідації вхідних даних, їх обробки, прийняття інтелектуальних рішень щодо політики на основі алгоритму довіри та забезпечення дотримання політики.

Як NGFW, FortiGate здатний сканувати трафік для виявлення аномалій, шкідливого програмного забезпечення, вірусів та найновіших загроз. Контроль програм дозволяє FortiGate детально ідентифікувати програму на основі шаблонів трафіку, щоб правильно контролювати програму та протокол.

На рисунку 2.1 наведено приклад архітектури ZTNA та показано місце FortiGate NGFW в ній. Незалежно від того, чи знаходяться користувачі в корпоративній мережі в штаб-квартирі, чи віддалено в кавярні, вдома чи у філії, вони можуть безпечно отримувати доступ до внутрішніх ресурсів за допомогою ZTNA без додаткових VPN-підключень. Проксі-сервер доступу FortiGate перевіряє ідентифікацію пристрою, ідентифікацію користувача, стан пристрою, геолокацію,

час і дозволи програм, перш ніж дозволити доступ, щоб забезпечити узгоджений користувацький досвід всередині та за межами корпоративної мережі [14].

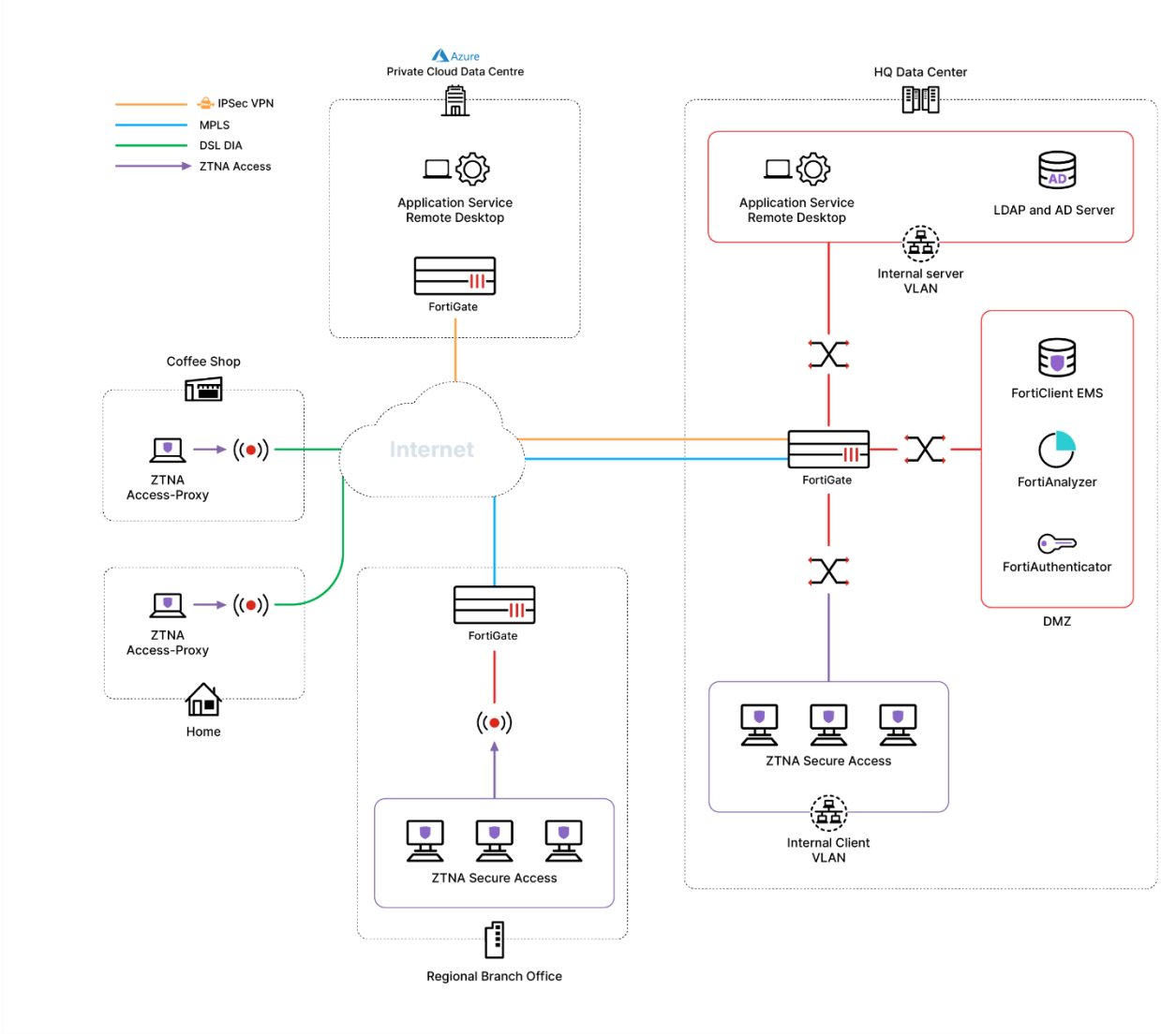

Рис. 2.1. Приклад архітектури ZTNA та місце FortiGate NGFW в ній [14]

Мережеві екрани Fortinet на базі штучного інтелекту розроблені для забезпечення комплексних та інтегрованих рішень кібербезпеки для різних типів організацій. Мережеві екрани FortiGate NGFW об’єднують функції екрана, SD-WAN, розширеної маршрутизації та шлюзу застосунків з нульовою довірою до мережі (ZTNA) в одне інтегроване рішення, яке задовольняє різні розміри та вимоги мереж. Незалежно від того, розгорнуті вони локально, у філіях, центрах обробки даних чи в хмарі, вони забезпечують узгоджені політики безпеки в гібридних середовищах. На відміну від традиційних точкових рішень, Fortinet застосовує цілісний підхід до кібербезпеки з інтегрованою платформою Fortinet

Security Fabric, що забезпечує безперебійну та ефективну взаємодію між продуктами Fortinet з послідовним та консолідованим захистом на базі штучного інтелекту в сучасних гібридних середовищах. Як ядро Fortinet Security Fabric, NGFW FortiGate координує свою роботу з іншими пристроями безпеки, збираючи та аналізуючи дані безпеки по всій мережі, щоб допомогти організаціям зменшити складність, усунути ізольовані системи безпеки та оптимізувати взаємодію з користувачем [12].

Підтримка та захист гібридних архітектур вимагає єдиного комплексного контролю по всій розподіленій мережі. Це включає знання про кожного користувача та пристрій у мережі, а також про програми та ресурси, до яких вони отримують доступ. Крім того, необхідно виявляти аномальну поведінку та шкідливу активність всюди. Концентрація всіх необхідних ресурсів безпеки для своєчасного та скоординованого реагування також є життєво важливою для зупинки загроз [11].

Для підтримки сучасних мереж, що розширюються, та їхніх численних периферійних зон багато компаній почали впроваджувати різнорідні рішення для безпечного доступу до мережі на периферії (SASE), програмно-визначених глобальних мереж (SD-WAN) та доступу до мережі з нульовою довірою (ZTNA). Це створює складність, водночас порушуючи видимість, погіршуючи взаємодію з користувачем та обмежуючи можливості ефективного реагування на атаки. Інтеграція NGFW з цими функціями може забезпечити як надійний захист, так і стійкість мережі [11].

Завдяки централізованому управлінню для забезпечення дотримання єдиної політики в режимі реального часу, ця комбінація може допомогти зменшити ризики як від внутрішніх збоїв, так і від зовнішніх атак на всіх поверхнях. Завдяки своїй вбудованій сумісності, цей підхід спрощує операції, забезпечує відповідність вимогам, зменшує складність і дозволяє здійснювати широку автоматизацію для підвищення операційної ефективності сучасних гібридних бізнес-моделей. Підвищена цінність полягає в централізованому та єдиному управлінні всіма розгортаннями мережевих екранів [11].

NGFW FortiGate універсальні та підтримують різноманітні сценарії для підвищення безпеки та продуктивності мережі. Ось деякі поширені випадки використання [12]:

безпека периметра: виступає першою лінією захисту мережі для фільтрації вхідного та вихідного трафіку, блокування несанкціонованого доступу та зменшення загроз;

компонент Secure SD-WAN: забезпечує безпечне та оптимізоване підключення для філій, гарантуючи при цьому продуктивність додатків;

віддалений доступ: забезпечує безпечний віддалений доступ до корпоративних ресурсів незалежно від місцезнаходження співробітників;

контроль застосунку: контролює та відстежує використання додатків у мережі, запобігаючи несанкціонованому доступу та зменшуючи загрози від ризикованих програм;

внутрішня сегментація: сегментує різні частини мережі, щоб зменшити площі атак, ізолюючи конфіденційні дані або критичні системи для запобігання порушенням;

хмарна безпека: захищає хмарні робочі навантаження, безпеку даних і програм, забезпечуючи дотримання політик безпеки;

безпека Інтернету речей: забезпечує безпеку пристроїв, підключених до мережі, забезпечуючи ефективний моніторинг та управління цими пристроями для запобігання вразливостям.

2.2. Архітектура рішення FortiGate NGFW

Розглянемо побудову FortiGate NGFW на прикладі FortiGate 100F. NGFW серії FortiGate 100F поєднує в собі безпеку на базі штучного інтелекту (ШІ) та машинного навчання (ML) для забезпечення захисту від загроз будь-якого масштабу. FortiGate 100F дозволяє отримати глибший огляд корпоративної мережі та переглядати програми, користувачів і пристрої, перш ніж вони стануть загрозами [13, 15].

Завдяки багатому набору можливостей безпеки на основі штучного інтелекту/машинного навчання, що поєднуються в інтегровану платформу безпеки, FortiGate серії 100F забезпечує безпечну мережу, яка є широкою, глибокою та автоматизованою. Рішення захищає корпоративну мережу від початку до кінця за допомогою розширеного захисту на межі мережі, що включає безпеку веб-сайтів, контенту та пристроїв, а сегментація мережі та безпечна SD-WAN зменшують складність та ризики в гібридних IT-мережах. Ця структура безпеки безперешкодно поширюється на все корпоративне середовище, включаючи архітектуру гібридного сітчастого брандмауера, забезпечуючи послідовне застосування політик та захист від загроз у всіх сегментах мережі [13, 15].

Універсальний мережевий доступ з нульовою довірою (ZTNA) автоматично контролює, перевіряє та полегшує доступ користувачів до додатків, зменшуючи непрямі загрози, надаючи доступ лише перевіреним користувачам. Надзвичайно швидкий захист від загроз та перевірка SSL забезпечують безпеку на периферії, яку можна бачити, не впливаючи на продуктивність.

Варіант використання NGFW:

пакет послуг безпеки на базі штучного інтелекту від FortiGuard Labs, інтегрований з корпоративною мережею NGFW, захищає вебсторінки, контент і пристрої, а також захищає мережі від програм-вимагачів, шкідливого програмного забезпечення, атак нульового дня та складних кібератак на базі штучного інтелекту;

перевірка SSL у режимі реального часу (включно з TLS 1.3) забезпечує повну видимість користувачів, пристроїв та програм на всій поверхні атаки;

запатентована технологія SPU від Fortinet забезпечує провідний у галузі високопродуктивний захист.

Варіант використання Secure SD-WAN:

FortiGate WAN Edge, що працює на базі однієї ОС та єдиної системи безпеки та управління, трансформує та захищає глобальні мережі;

забезпечує високу якість взаємодії та ефективну систему безпеки для гібридних робочих моделей, SDBranch та випадків використання хмарно-орієнтованих WAN;

забезпечує операційну ефективність будь-якого масштабу завдяки автоматизації, глибокій аналітиці та самовідновленню.

Варіант використання універсальний ZTNA:

контроль доступу до програм незалежно від того, де знаходиться користувач і де розміщено програму, для універсального застосування політик доступу;

забезпечує розширену автентифікацію, перевірки та застосовувати політики перед кожним наданням доступу до додатка;

доступ на основі агентів за допомогою FortiClient або безагентний доступ через проксі-портал для гостя або BYOD.

Варіант використання сегментація:

динамічна сегментація адаптується до будь-якої топології мережі, забезпечуючи справжню комплексну безпеку від філії до центру обробки даних та в багатохмарних середовищах;

ультрамасштабована сегментація VXLAN з низькою затримкою з’єднує фізичні та віртуальні домени за допомогою правил брандмауера 4-го рівня;

запобігає горизонтальному переміщенню по мережі завдяки розширеному, скоординованому захисту від FortiGuard Security Services, виявляє та запобігає відомим, нульовим та невідомим атакам

Сервіси безпеки FortiGuard на базі штучного інтелекту є частиною багаторівневого захисту Fortinet і тісно інтегровані в FortiGate NGFW та інші продукти. Завдяки новітнім даним про загрози від FortiGuard Labs, ці сервіси захищають організації від сучасних векторів атак і загроз, включаючи атаки нульового дня та складні атаки на базі штучного інтелекту.

Послуги мережевої та файлової безпеки захищають від мережевих та файлових загроз. Маючи понад 18 000 сигнатур, система запобігання вторгненням (IPS) використовує моделі штучного інтелекту/машинного навчання для глибокої перевірки пакетів/SSL, виявлення та блокування шкідливого контенту, а також застосування віртуальних патчів для нещодавно виявлених вразливостей.

Захист від шкідливого програмного забезпечення захищає як від відомих, так і від невідомих файлових загроз, поєднуючи антивірус та «пісочницю» для

багаторівневого захисту. Контроль програм покращує відповідність вимогам безпеки та забезпечує видимість програм та їх використання в режимі реального часу.

Сервіси веб/DNS-безпеки захищають від атак на основі DNS, шкідливих URL-адрес (включно з тими, що містяться в електронних листах) та зв'язку ботнетів. DNS-фільтрація блокує повний спектр атак на основі DNS, тоді як URL-фільтрація використовує базу даних із понад 300 мільйонів URL-адрес для виявлення та блокування шкідливих посилань. Тим часом сервіси репутації IP-адрес та захисту від ботнетів захищають від активності ботнетів та DDoS-атак. FortiGuard Labs блокує понад 500 мільйонів шкідливих/фішингових/ спам-URL-адрес щотижня та блокує 32 000 спроб керування ботнетами щохвилини, демонструючи надійний захист, що пропонується Fortinet.

SaaS-послуги та послуги безпеки даних охоплюють ключові потреби безпеки для використання програм та захисту даних. Це включає запобігання втратам даних для забезпечення видимості, керування та захисту (блокування витоку) даних під час руху через мережі, хмари та користувачів. Вбудована служба брокера безпеки доступу до хмари захищає дані під час руху, у стані спокою та в хмарі, забезпечуючи дотримання стандартів відповідності та керуючи використанням облікових записів, користувачів і хмарних додатків. Послуги також оцінюють інфраструктуру, перевіряють конфігурації та виявляють ризики та вразливості, включаючи виявлення пристроїв Інтернету речей та кореляцію вразливостей.

Запобігання загрозам нульового дня досягається за допомогою вбудованої профілактики шкідливих програм на базі штучного інтелекту, яка аналізує вміст файлів для виявлення та блокування невідомого шкідливого програмного забезпечення в режимі реального часу, забезпечуючи захист за менш ніж секунду на всіх мережах NGFW. Сервіс також інтегрує матрицю MITRE ATT&CK для пришвидшення розслідувань. Інтегрований у мережі NGFW FortiGate, сервіс забезпечує комплексний захист, блокуючи невідомі загрози, оптимізуючи реагування на інциденти та зменшуючи накладні витрати на безпеку.

Маючи понад 1000 віртуальних патчів, понад 1100 OT-застосунків та понад

3300 правил протоколів, інтегровані можливості безпеки OT виявляють загрози, спрямовані на OT-інфраструктуру, виконують кореляцію вразливостей, застосовують віртуальні патчі та використовують галузеві декодери протоколів для надійного захисту OT-середовищ та пристроїв.

Серія FortiGate 100F поєднує можливості мережевого екрана наступного покоління та SD-WAN для розподілених об'єктів середніх та великих підприємств. Завдяки спеціально розробленій захищеній SD-WAN ASIC, FortiGate 100F забезпечує оптимальну продуктивність для критично важливих бізнес-додатків разом із найкращою ефективністю безпеки [15].

Система безпеки Security Fabric забезпечує широку видимість, інтегроване запобігання порушенням на основі штучного інтелекту, а також автоматизовані операції, оркестрацію та реагування на всі системи Fortinet та її екосистеми. Це дозволяє системі безпеки динамічно розширюватися та адаптуватися до додавання все більшої кількості робочих навантажень і даних. Безпека безперешкодно відстежує та захищає дані, користувачів і програми, коли вони переміщуються між Інтернетом речей, пристроями та хмарними середовищами по всій мережі. Все це обєднано в єдину панель управління, що значно покращує можливості безпеки в усьому середовищі, а також значно зменшує складність [15].

FortiGate є основою Security Fabric, розширюючи безпеку завдяки видимості та контролю завдяки тісній інтеграції з іншими продуктами безпеки Fortinet та рішеннями партнерів, готових до роботи з Fabric.

FortiOS – це операційна система, що працює на платформі Fortinet Security Fabric, що забезпечує забезпечення дотримання політик безпеки та цілісний контроль над усією поверхнею атаки. FortiOS надає єдину платформу для керування та захисту мереж, хмарних, гібридних або конвергенції IT, OT та IoT. FortiOS забезпечує безперебійну та ефективну взаємодію між продуктами Fortinet із послідовним та консолідованим захистом на базі штучного інтелекту в сучасних гібридних середовищах [13].

На відміну від традиційних точкових рішень, Fortinet застосовує цілісний підхід до кібербезпеки, прагнучи зменшити складність, усунути ізольовані системи

безпеки та підвищити операційну ефективність. Об’єднуючи функції безпеки в єдину платформу, FortiOS спрощує управління, знижує витрати та покращує загальний рівень безпеки. Разом FortiGate та FortiOS створюють інтелектуальний, адаптивний захист, який допомагає організаціям зменшити складність, усунути ізольовані системи безпеки та оптимізувати взаємодію з користувачем [13].

Завдяки інтеграції генеративного штучного інтелекту (GenAI), FortiOS ще більше покращує можливості аналізу мережевого трафіку та розвідки загроз, ефективніше виявляє відхилення або аномалії та надає точніші рекомендації щодо усунення наслідків, забезпечуючи мінімальний вплив на продуктивність без шкоди для безпеки [13].

FortiGate NGFW працює на єдиному спеціально розробленому SPU. Традиційні мережеві екрани не можуть захистити від сучасних загроз, пов’язаних з контентом та з’єднаннями, оскільки вони покладаються на готові центральні процесори (ЦП) загального призначення, що залишає небезпечну прогалину в безпеці.

Спеціальні SPU від Fortinet забезпечують потужність, необхідну для радикального збільшення швидкості, масштабування та ефективності, водночас значно покращуючи взаємодію з користувачем та зменшуючи вимоги до розміру та живлення. SPU від Fortinet забезпечують до 520 Гбіт/с захищеної пропускної здатності для виявлення нових загроз та блокування шкідливого контенту, гарантуючи, що корпоративне рішення для мережевої безпеки не стане вузьким місцем у продуктивності.

ASIC-чіпи Fortinet розроблені з урахуванням енергоефективності, що призводить до зниження енергоспоживання та покращення загальної вартості володіння. Вони забезпечують провідну в галузі пропускну здатність, обробляють більший трафік та швидше виконують перевірки безпеки, зменшують затримку для швидшої обробки пакетів і мінімізують затримки в мережі. Блоки захисту Fortinet SPU розроблені з інтегрованими функціями безпеки, такими як нульова довіра, SSL, IPS та VXLAN, і це лише деякі з них, що значно покращує продуктивність цих функцій, які конкуренти традиційно реалізують у програмному забезпеченні [13].

Централізоване управління масштабу для розподілених підприємств FortiManager, що працює на базі FortiAI, – це централізоване рішення для управління Fortinet Security Fabric. Воно спрощує масове налаштування та управління політиками для FortiGate, FortiGate VM, хмарної безпеки, SD-WAN, SD-Branch, FortiSASE та ZTNA в гібридних середовищах. Крім того, FortiManager забезпечує моніторинг усієї керованої інфраструктури в режимі реального часу та автоматизує робочі процеси мережевих операцій [13].

Використовуючи GenAI у FortiAI, він ще більше покращує конфігурації та налаштування Day 0–1, а також усунення несправностей та обслуговування Day N, розкриваючи весь потенціал Fortinet Security Fabric та значно підвищуючи операційну ефективність [13].

2.3. Основні можливості рішення FortiGate NGFW

Рішення Fortinet FortiGate 100F забезпечує захист корпоративного рівня для невеликих мереж. Розглянемо варіанти розгортання Fortinet FortiGate 100F.

Варіант розгортання як мережевого екрана наступного покоління (NGFW) показано на рисунку 2.2.

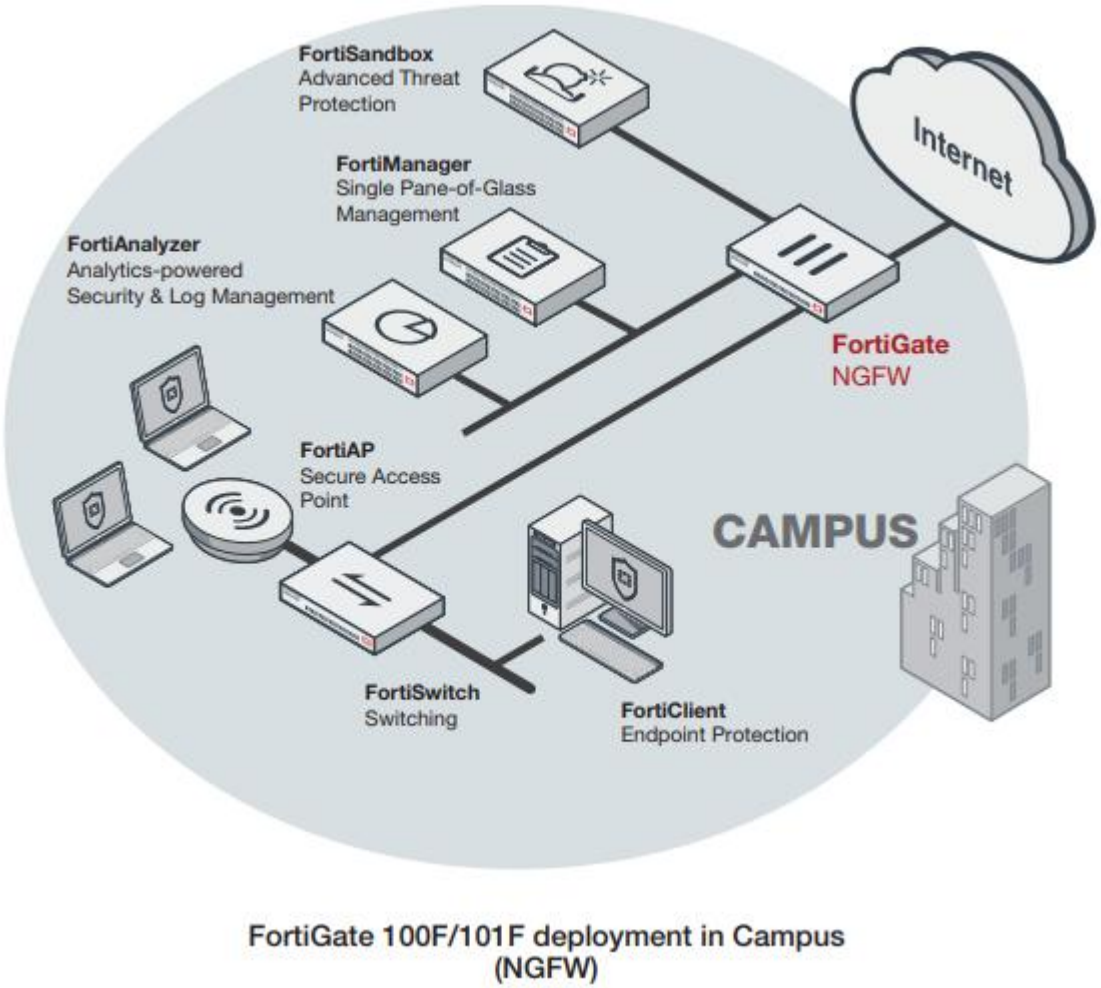

Рис. 2.2. Варіант розгортання Fortinet FortiGate 100F як мережевого екрана наступного покоління [15]

Варіант розгортання Fortinet FortiGate 100F як мережевого екрана наступного покоління (NGFW) забезпечує [15]:

зменшення складності, об’єднавши можливості захисту від загроз в єдиний високопродуктивний пристрій мережевої безпеки;

виявлення та зупинку загрози за допомогою потужного захисту від вторгнень, що виходить за рамки портів та протоколів, та аналізує фактичні додатки у мережевому трафіку організації;

найвищу в галузі продуктивність SSL-інспекції, використовуючи шифри, що встановлені галуззю, та максимізує рентабельність інвестицій;

проактивне блокування нещодавно виявлених складних атак в режимі реального часу за допомогою розширеного захисту від загроз.

Варіант розгортання як безпечної SD-WAN показано на рисунку 2.3.

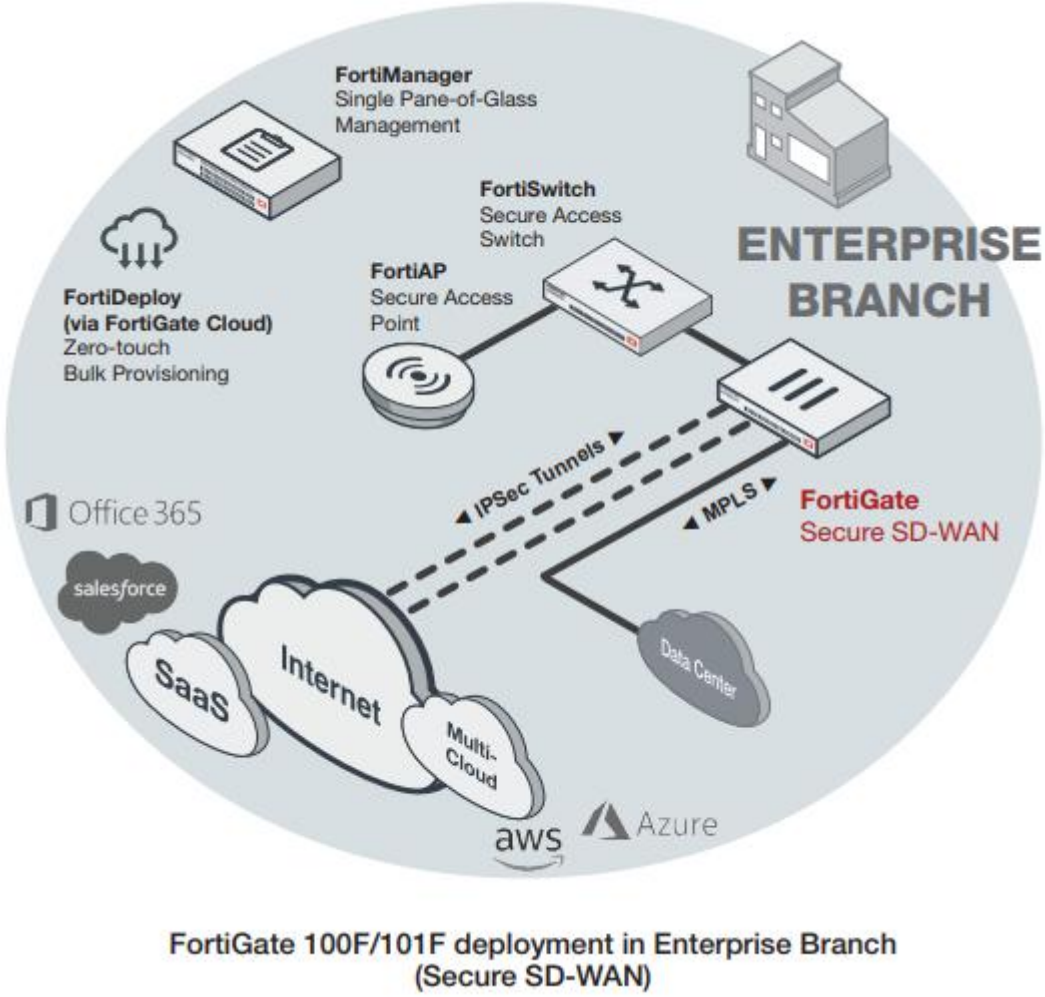

Рис. 2.3. Варіант розгортання Fortinet FortiGate 100F як безпечної SD-WAN [15]

Варіант розгортання Fortinet FortiGate 100F як безпечної SD-WAN забезпечує [15]:

безпечний прямий доступ до Інтернету для хмарних додатків для покращення затримки та зменшення витрат на WAN;

високопродуктивні та економічно ефективні можливості захисту від загроз;

реалізує контролер шляху WAN та моніторинг стану каналу зв'язку для кращої продуктивності застосунків;

реалізує процесор безпеки забезпечує найкращу в галузі продуктивність IPsec VPN та SSL-інспекції;

спрощене управління та розгортання без втручання.

3 РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ FORTIGATE NGFW

3.1. Порядок створення системи захисту корпоративної мережі на базі FortiGate NGFW

Як правило, організація має мережевий екран наступного покоління (NGFW), який захищає її мережу або центр обробки даних від Інтернету та діє як шлюз за замовчуванням до Інтернету через одне або кілька каналів WAN, як показано на рисунку 3.1 [5].

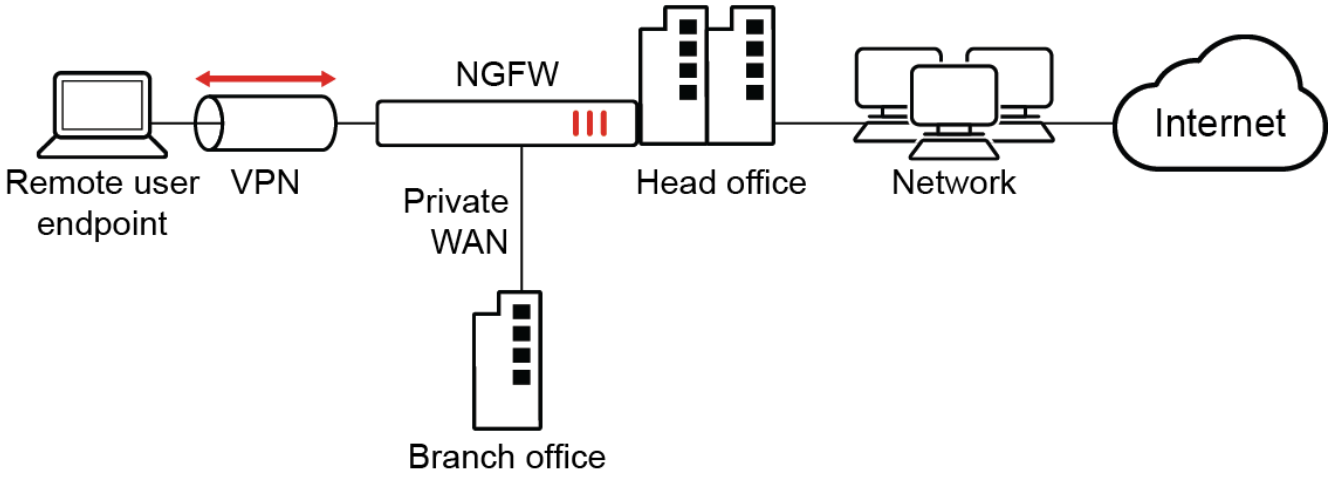

Рис. 3.1. Схема архітектури NGFW [5]

NGFW зазвичай є фізичним або віртуальним пристроєм, розташованим на краю мережі організації.

Віртуальна приватна мережа (VPN) – це галузевий стандарт рішення, яке забезпечує віддалений доступ, автентифікацію та можливості шифрування за допомогою програмного клієнта або агента для захисту трафіку між користувачем в Інтернеті та шлюзом VPN, захищаючи мережу організації. VPN віддаленого доступу покладаються на реалізацію VPN на основі IPsec або SSL [5].

Як правило, організація надає своїм віддаленим користувачам захищений

доступ до своєї мережі через з’єднання VPN або надає користувачам філії захищений доступ за допомогою інших технологій глобальної мережі, таких як багатопротокольна комутація за мітками (MPLS) [5].

Організації розширюють цей сценарій, щоб гарантувати своїм віддаленим користувачам безпечний доступ до Інтернету, застосувавши VPN-з’єднання з увімкненим повним тунелюванням. Завдяки VPN з повним тунелюванням через VPN проходить такий трафік [5]:

трафік, призначений для внутрішньої мережі організації;

трафік, призначений для Інтернету, надсилається в Інтернет через VPN до NGFW для виявлення та пом’якшення загроз

Таким чином, Інтернет-трафік віддаленого користувача не тільки проходить через його власного локального провайдера для встановлення VPN-з’єднання з NGFW, але також проходить через WAN-з’єднання NGFW. Ця операція відома як ретрансляція WAN.

FortiGate – це складний пристрій безпеки з багатьма параметрами конфігурації. Нижче наведено перші кроки, які необхідно виконати під час підготовки нового FortiGate до розгортання [7]:

реєстрація;

базова конфігурація;

ресурси.

Порядок реєстрації.

Рішення FortiGate, а потім його контракт на обслуговування, необхідно зареєструвати, щоб мати повний доступ до служби підтримки клієнтів Fortinet і послуг FortiGuard. FortiGate можна зареєструвати або в графічному інтерфейсі FortiGate, або на порталі підтримки FortiCloud. Договір про надання послуг можна зареєструвати на порталі підтримки FortiCloud.

Щоб перевірити статус ліцензії на FortiGate, перейдіть до *System* > *FortiGuard* і перевірте таблицю *License Information* (рисунок 3.2). Між реєстрацією пристрою та оновленням інформації про ліцензію на FortiGate може виникнути затримка в кілька годин.

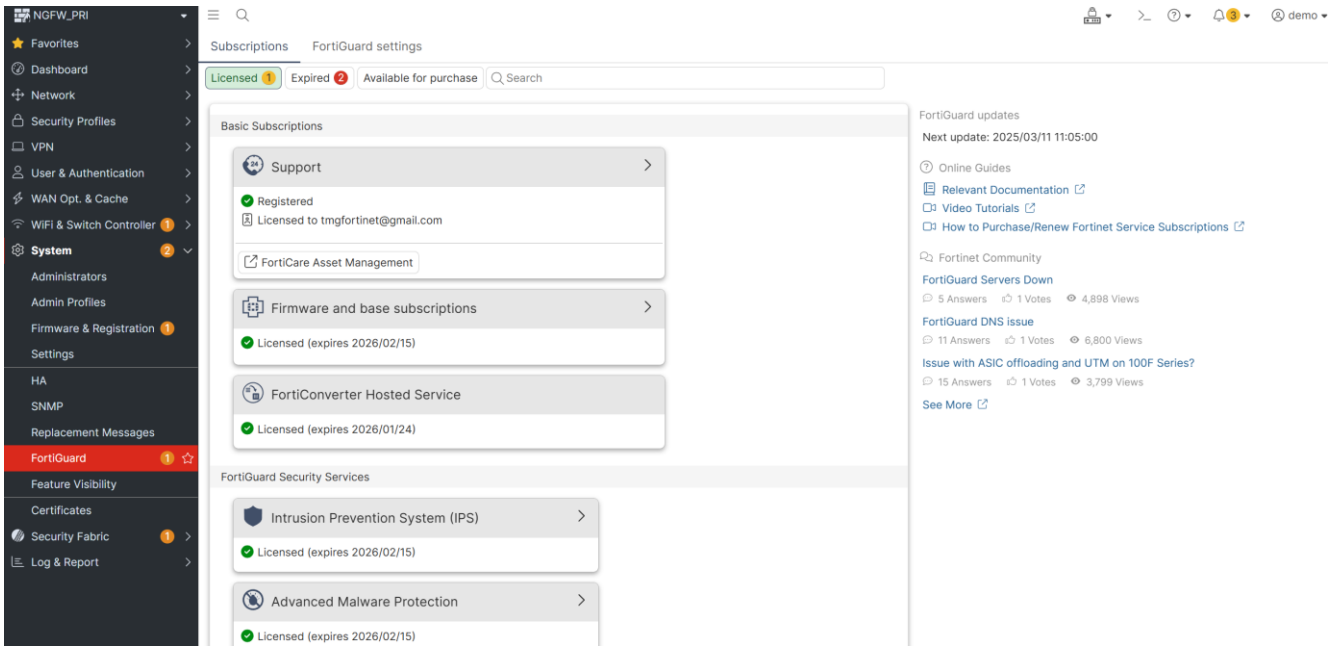

Рис. 3.2. Статус ліцензії на FortiGate

Таблицю «Інформація про ліцензію» можна використовувати для підтвердження того, що FortiGate отримує останні оновлення. Можна розгорнути службу в таблиці та навести курсор на версію, щоб побачити день її останнього оновлення. Деякі служби оновлюються щодня, але інші залишатимуться незмінними протягом тривалого періоду часу. Наприклад, механізм AV може залишатися незмінним місяцями, тоді як база даних AV-сигнатур може отримувати кілька оновлень на день.

Налаштування базової конфігурації.

Як перший крок до нового розгортання, необхідно переглянути параметри за замовчуванням, такі як паролі адміністраторів, сертифікати для доступу GUI та SSL VPN, ключі SSH, відкриті адміністративні порти на інтерфейсах і політики брандмауера за замовчуванням [7].

Як тільки FortiGate підключається до Інтернету, він піддається зовнішнім ризикам, таким як несанкціонований доступ, атаки типу «людина посередині», спуфінг, атаки DoS та інші зловмисні дії з боку зловмисників. Ми можемо або скористатися майстром запуску, або вручну переконфігурувати параметри за замовчуванням, щоб посилити захист із самого початку.

Режим роботи – з міркувань безпеки краще використовувати режим NAT.

Політики режиму NAT перетворюють адреси в більш безпечну зону від користувачів, які знаходяться в менш безпечній зоні, використовуючи NATed IP-адресу або пул IP-адрес. Цей рівень обфускації не дозволяє зловмисникам в Інтернеті знати IP-адреси ресурсів у корпоративній локальній мережі та DMZ.

Використовується прозорий режим, якщо мережа складна і не допускає змін у схемі IP-адресації.

Прошивка – якщо надіслане мікропрограмне забезпечення не є тим, яке ми будемо використовувати, ми завантажуємо необхідне мікропрограмне забезпечення, перш ніж виконувати будь-які налаштування, або встановлюємо віддалений доступ для додаткових параметрів завантаження мікропрограмного забезпечення (SFTP, FTP, SCP, HTTPs), а потім завантажуємо необхідне мікропрограмне забезпечення.

Ім’я хоста – необхідно використовувати значуще ім’я хоста. Він використовується в запиті CLI як ім’я системи SNMP, як ім’я пристрою FortiGate Cloud і як ім’я пристрою в конфігурації HA.

Системний час – кілька функцій FortiGate покладаються на точний системний час, як-от функції реєстрації та сертифікатів. Для встановлення системного часу рекомендовано використовувати сервер мережевого протоколу часу (NTP) або протоколу точного часу (PTP). При необхідності системний час можна встановити вручну.

Пароль адміністратора необхідно встановити під час першого входу до FortiGate. Пароль має бути унікальним і мати відповідну складність.

Інтерфейс управління – необхідно налаштувати IP-адресу, маску підмережі та лише необхідні служби адміністративного доступу (наприклад, HTTPs і SSH) в інтерфейсі керування.

FortiOS – це операційна система, яка працює на брандмауері FortiGate наступного покоління (NGFW) Fortinet. Він підтримує різні платформи, зокрема [6]:

фізичні прилади;

гіпервізори;

платформи хмарних обчислень.

FortiOS забезпечує безпеку як гібридний мережевий брандмауер, який охоплює сітчасту топологію локальних і хмарних середовищ. Завдяки службам безпеки FortiGuard на базі штучного інтелекту FortiOS забезпечує захист на всій поверхні атаки за допомогою IPS, розширеного захисту від шкідливого програмного забезпечення, веб-безпеки, вбудованого захисту від шкідливого програмного забезпечення, запобігання втраті даних тощо.

Крім того, FortiOS займає центральне місце в рішенні SD-WAN, забезпечуючи функціональні можливості та інтелектуальні можливості SD-WAN в одному FortiGate, мережі FortiGates або інтегрованій у середовище SASE. Він також є центральним у рішенні Zero Trust Network Access (ZTNA), оскільки приймає політичні рішення та застосовує примусове виконання політики на основі вхідних даних щодо безпеки [6].

Короткий опис кроків із налаштування нового розгортання рішення FortiGate.

Ці кроки підсумовують, як запустити FortiGate за допомогою графічного інтерфейсу користувача.

1. Необхідно налаштувати свій FortiGate для початкового доступу до керування за допомогою графічного інтерфейсу:

фізичні пристрої, такі як FortiGate (рисунок 3.3);

гіпервізори, такі як FortiGate-VM на ESXi, KVM, Hyper-V тощо.

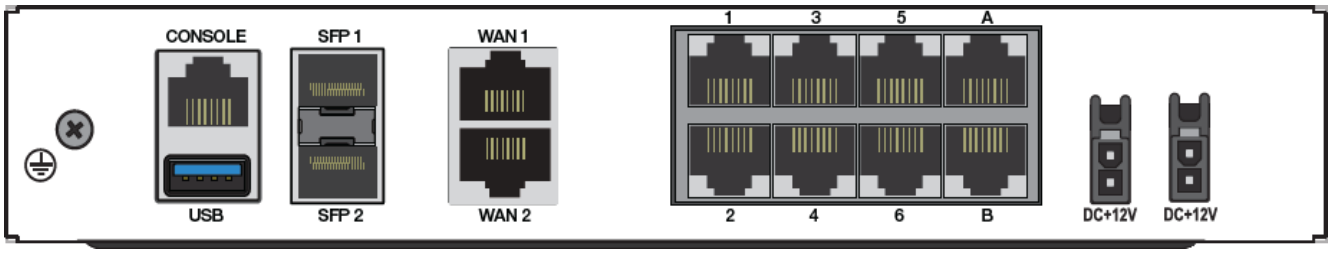

Рис. 3.3. Приклад для FortiGate 80F, який використовує port1 для початкового доступу до керування [6]

Залежно від топології та моделі FortiGate доступ до Інтернету може ще не налаштовано для FortiGate. Якщо немає доступу до Інтернету, ми не можемо

зареєструвати FortiGate у Fortinet до наступного етапу налаштування.

2. У графічному інтерфейсі необхідно дотримуватися вказівок майстра налаштування FortiGate, щоб змінити ім’я хоста, змінити пароль і вказати макет за замовчуванням для інформаційних панелей FortiOS.

3. Необхідно виконати базові кроки налаштування FortiOS. Після цього кроку всі моделі FortiGate мають мати доступ до Інтернету. У типовому розгортанні, де FortiGate NGFW налаштовано як периферійний брандмауер, адміністратор зазвичай налаштовує контроль доступу між інтерфейсами LAN та WAN, а також постійний доступ до керування через внутрішньосмугове або позасмугове керування.

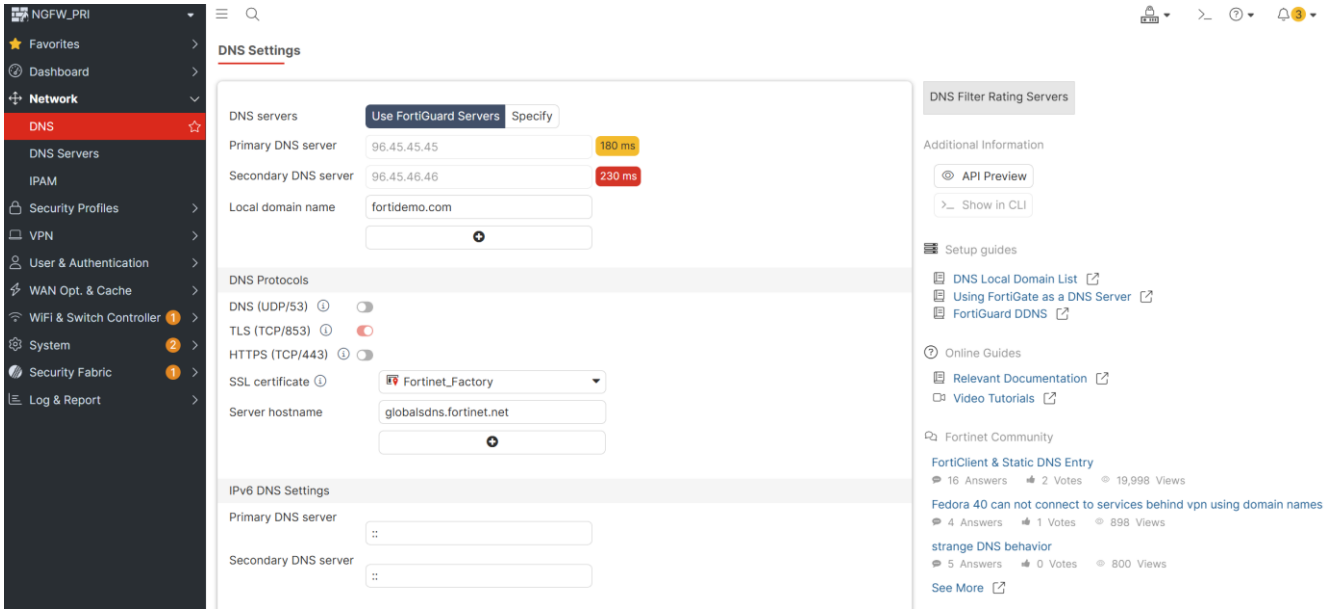

Рис. 3.4. Налаштування мережевих інтерфейсів

4. Необхідно зареєструвати рішення FortiGate у Fortinet, використовуючи свій обліковий запис FortiCare/FortiCloud у технічній підтримці Fortinet (https://support.fortinet.com).

5. Необхідно налаштувати політику для FortiGate, щоб надати клієнтам за FortiGate доступ до Інтернету.

6. Необхідно створити резервну копію конфігурації.

7. Якщо необхідно, то усуньте неполадки встановлення.

Після завершення розділу «Початок роботи» наступні кроки можуть включати:

знайомство з графічним інтерфейсом FortiOS і CLI;

налаштування функцій FortiOS. У таблиці 3.1 наведено кілька функцій, доступних у FortiOS. Доступно багато додаткових функцій.

Таблиця 3.1

Перелік основних функцій FortiOS

For	Go to
Security profiles	See antivirus, IPS, web filter, and application control.
VPN	See IPsec VPN.
Fortinet Security Fabric	See Fortinet Security Fabric.
User & Authentication	See User & Authentication.
Software-defined wide area network (SD-WAN)	See SD-WAN.
Zero Trust Network Access (ZTNA)	See Zero Trust Network Access.

Режим NGFW на основі профілю – це традиційний режим, у якому ми створюємо профіль (антивірус, веб-фільтр тощо), а потім застосовуємо профіль до політики.

У режимі NGFW на основі політики ми дозволяємо програмам і категоріям URL-адрес використовуватися безпосередньо в політиках безпеки, не вимагаючи веб-фільтра або профілів керування програмами. Однак можна вибрати та застосувати категорії та групи URL-адрес веб-фільтра.

У режимі на основі політики:

центральний NAT завжди ввімкнено. Якщо центральна політика SNAT не існує, її потрібно створити;

правила попереднього збігу визначаються окремо від політик безпеки та визначають ширші правила, такі як перевірка SSL та автентифікація користувача;

майстер IPsec не підтримується.

Якщо наш FortiGate працює в режимі NAT, а не вмикає вихідний NAT в окремих політиках NGFW, треба перейти до *Policy & Objects* > *Central SNAT* і додати вихідні політики NAT, які застосовуються до всього відповідного трафіку. У багатьох випадках нам може знадобитися лише одна політика SNAT для кожної пари інтерфейсів.

Режим NGFW встановлюється для кожного VDOM (virtual domains), і він доступний лише тоді, коли режим перевірки VDOM базується на потоках. Ми можемо керувати всім FortiGate або окремими VDOM у режимі політики NGFW. Порт програми за замовчуванням можна встановити як службовий порт у режимі NGFW за допомогою опції *default-app-port-as-service*.

У режимі NGFW адміністратори можуть налаштувати політику безпеки в режимі навчання для моніторингу трафіку.

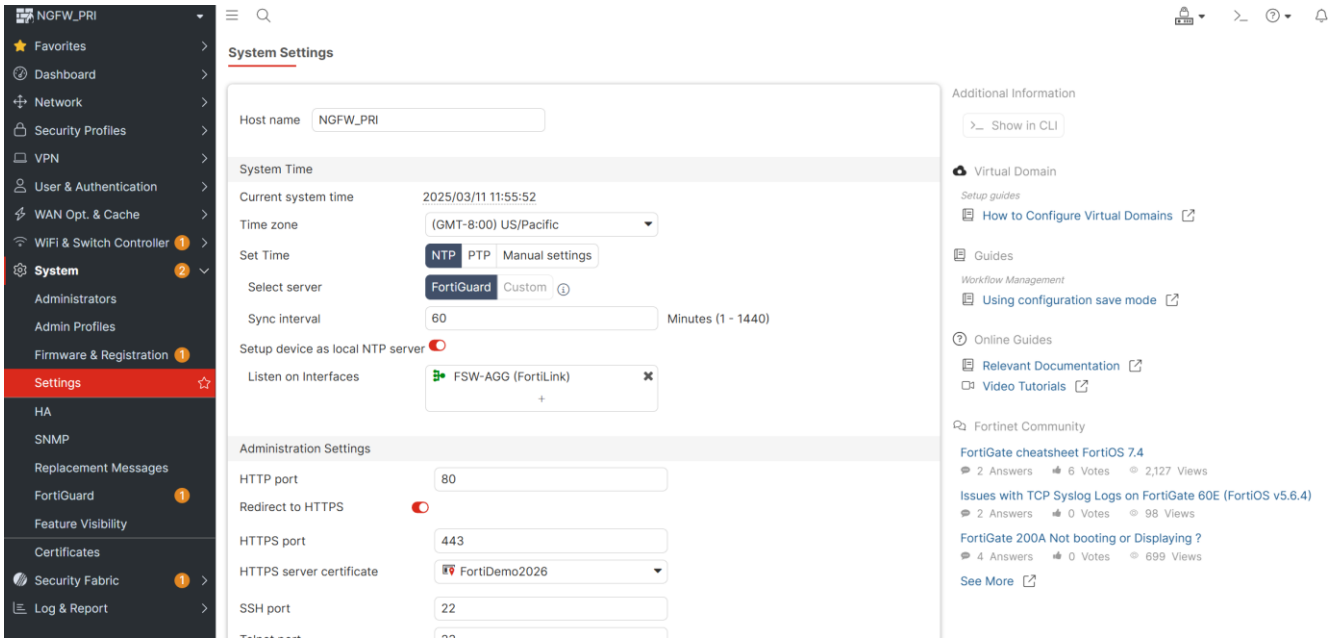

Рис. 3.5. Вкладка «Користувальницький простір»

5. У рядку, що відповідає віддаленому хосту, натискаємо посилання Items.

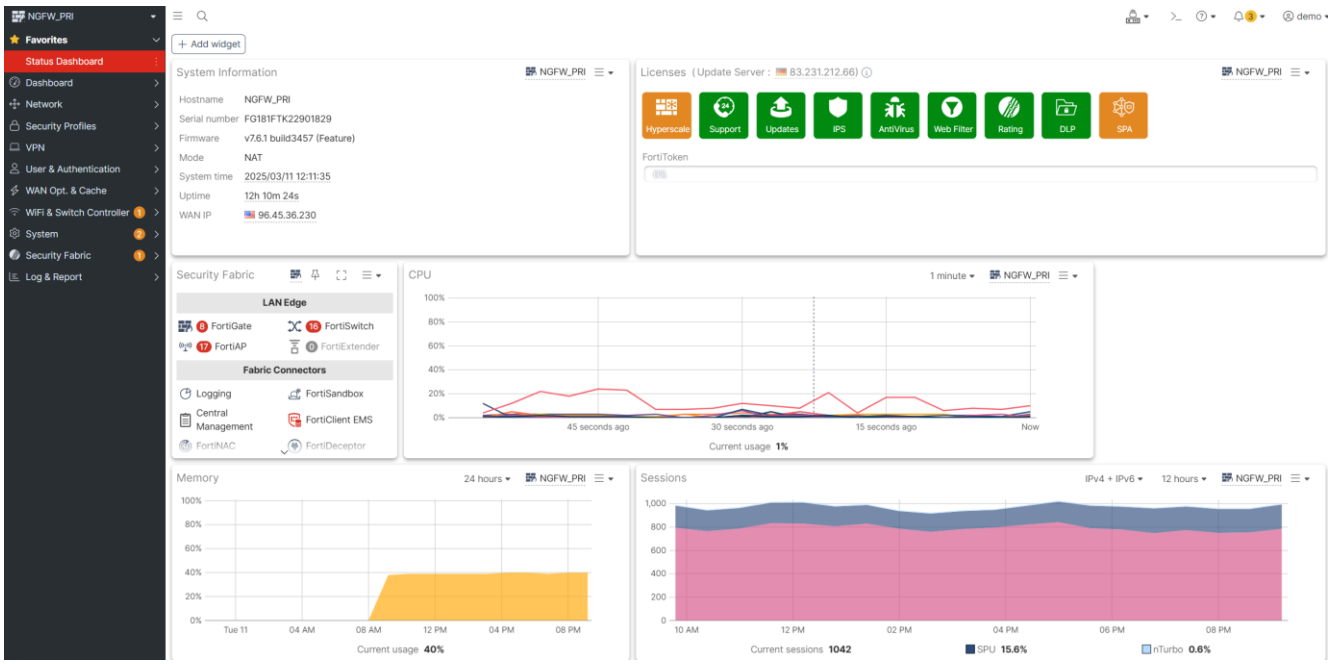

Рис. 3.6. Статус панелі інструментів

3.2. Рекомендації щодо захисту корпоративної мережі

Безпека мережевої інфраструктури стосується заходів та практик, що використовуються для захисту апаратного забезпечення, програмного забезпечення та даних, що складають мережу. Вона включає впровадження засобів контролю та протоколів безпеки для запобігання несанкціонованому доступу, захисту від зловмисних атак та забезпечення конфіденційності, цілісності та доступності мережевих ресурсів.

Безпека мережевої інфраструктури важлива, оскільки вона допомагає захистити конфіденційну інформацію від доступу або компрометації неавторизованими користувачами. Вона також допомагає запобігти перебоям у роботі мережі та гарантує, що критично важливі служби та ресурси доступні авторизованим користувачам за потреби.

Організації можуть посилити безпеку своєї мережі, впроваджуючи найкращі практики. Основними рекомендації щодо захисту корпоративної мережі можуть бути:

1. Необхідно розробити та втілити політику та стратегію безпеки. Чітко

визначена політика безпеки слугує основою для системи мережевої безпеки організації. Вона окреслює правила, процедури та обов'язки щодо захисту мережевих ресурсів і даних.

Ключові елементи політики безпеки включають:

правила контролю доступу: визначте, хто може отримувати доступ до мережевих ресурсів і за яких умов;

політика прийнятного використання: встановлення правил для співробітників щодо безпечного використання мережевих ресурсів;

протоколи реагування на інциденти: забезпечують структурований підхід до виявлення, реагування та пом'якшення порушень безпеки;

заходи захисту даних: вкажіть політики шифрування, резервного копіювання та зберігання для захисту конфіденційної інформації;

стратегію безпеки слід регулярно переглядати та оновлювати, щоб враховувати нові загрози та змінювані бізнес-вимоги.

2. Необхідно впровадити надійну автентифікацію та постійно реалізовувати контроль доступу. Несанкціонований доступ є однією з основних причин порушення безпеки мережі. Впровадження надійних механізмів автентифікації та контролю доступу мінімізує цей ризик.

Найкращі практики включають:

багатофакторна автентифікація (MFA): вимагає кількох форм перевірки (наприклад, пароль + біометричний або одноразовий пароль);

контроль доступу на основі ролей (RBAC): обмежує доступ на основі посадових ролей, щоб забезпечити користувачам лише необхідні дозволи;

дотримання принципу найменших привілеїв (PoLP): обмежує права доступу до мінімуму, необхідного для виконання завдань;

керування привілейованим доступом (PAM): контролює та захищає доступ до критично важливих систем для привілейованих користувачів.

3. Оновлюйте системи та керуйте вразливостями. Неоновлене програмне забезпечення та застарілі системи є основними цілями для кібератак. Регулярні оновлення та управління вразливостями зменшують ризики відомих експлойтів.

Рекомендовані дії:

реалізація автоматизованого керування виправленнями: забезпечення своєчасного отримання оновлень безпеки операційними системами, програмами та мікропрограмами;

регулярне сканування вразливостей: виявлення слабких місць в мережевій інфраструктурі та визначення пріоритетів усунення їх;

інтеграція інформації про загрози: використовуйте дані про загрози в режимі реального часу, щоб випереджати нові вразливості;

управління інвентаризацією активів: ведення оновленого списку всіх пристроїв та програмного забезпечення для відстеження стану безпеки.

4. Необхідно проводити навчання та підвищення обізнаності кінцевих користувачів. Людська помилка залишається значним ризиком для безпеки. Навчання співробітників передовим практикам допомагає запобігти атакам соціальної інженерії та іншим поширеним загрозам. Регулярні програми підвищення обізнаності щодо безпеки допомагають створити культуру безпеки в організації.

Основні теми навчання:

розпізнавання фішингових атак: навчіть користувачів, як розпізнавати підозрілі електронні листи, посилання та вкладення;

безпечні методи перегляду: заохочуйте використання безпечних веб-сайтів і застерігайте від завантаження неперевіреного контенту;

безпечне керування паролями: заохочуйте використання менеджерів паролів та не заохочуйте повторне використання паролів;

процедури повідомлення про інциденти: Переконайтеся, що співробітники знають, як швидко повідомляти про інциденти безпеки.

5. Забезпечення дотримання вимог стандартів та норм. Організації повинні дотримуватися галузевих норм та систем безпеки, щоб захистити конфіденційні дані та уникнути юридичних санкцій. Проведення регулярних аудитів та оцінок відповідності допомагає організаціям дотримуватися нормативних вимог.

Загальні рамки дотримання вимог включають:

Загальний регламент про захист даних (GDPR): регулює захист даних та конфіденційність у Європейському Союзі;

Закон про перенесення та підзвітність медичного страхування (HIPAA): регулює безпеку даних охорони здоров'я в США;

Стандарт безпеки даних індустрії платіжних карток (PCI DSS): забезпечує безпечну обробку даних платіжних карток;

ISO/IEC 27001: забезпечує глобальний стандарт для систем управління інформаційною безпекою.

6. Використовуйте мережеві екрани та системи виявлення вторгнень.

Мережеві екрани та системи виявлення вторгнень є ключовими компонентами безпеки мережевої інфраструктури. Вони допомагають контролювати, виявляти та блокувати несанкціонований доступ і кіберзагрози.

ВИСНОВКИ

В роботі досліджено проблему захисту корпоративної мережі. Встановлено, що безпека на основі периметра втрачає актуальність, а концепція нульової довіри стає новою тенденцією. Нульова довіра є однією з головних тенденцій кібербезпеки у 2025 році, оскільки все більше організацій впроваджують мікросегментацію, перевірку контексту користувачів та постійний моніторинг сеансів.

Визначено існуючі підходи до захисту корпоративної мережі. Мережева безпека передбачає захист мереж від несанкціонованого доступу, неправильного використання, несправностей, модифікації, знищення або неналежного розголошення. Вона забезпечує конфіденційність, цілісність та доступність мережевих даних і ресурсів. Ця дисципліна включає технології, процеси та політики для захисту мереж від внутрішніх та зовнішніх загроз.

Проаналізовано існуючі рішення для рішення для захисту корпоративної мережі. NGFW виступають першою лінією захисту організації від кіберзагроз. Вони перевіряють та фільтрують весь трафік, що входить та виходить з корпоративної мережі, щоб блокувати спроби зараження шкідливим програмним забезпеченням та витоку даних. NGFW розширюють можливості традиційних мережевих екранів, не лише виявляючи шкідливе програмне забезпечення, але й блокуючи його до того, як воно проникне в мережу. Завдяки розширеним функціям виявлення та реагування на загрози, NGFW забезпечують комплексний захист у центрах обробки даних, корпоративних мережах та хмарних середовищах, зміцнюючи свою роль як основи сучасних стратегій кібербезпеки.

Проаналізовано методи та засоби захисту корпоративної мережі на базі FortiGate NGFW. Так NGFW серії FortiGate 100F поєднує в собі безпеку на базі штучного інтелекту та машинного навчання для забезпечення захисту від загроз будь-якого масштабу. FortiGate 100F дозволяє отримати глибший огляд корпоративної мережі та переглядати додатки, користувачів і пристрої, перш ніж вони стануть загрозами. Спеціальні SPU від Fortinet забезпечують потужність,

необхідну для радикального збільшення швидкості, масштабування та ефективності, водночас значно покращуючи взаємодію з користувачем та зменшуючи вимоги до розміру та живлення.

В роботі розглянуто порядок створення системи захисту корпоративної мережі на базі FortiGate NGFW. Як правило, організація має NGFW, який захищає її мережу або центр обробки даних від Інтернету та діє як шлюз за замовчуванням до Інтернету через одне або кілька каналів WAN. Організація надає своїм віддаленим користувачам захищений доступ до своєї мережі через з'єднання VPN або надає користувачам філії захищений доступ за допомогою інших технологій глобальної мережі, таких як багатопротокольна комутація за мітками (MPLS).

Розроблено рекомендації фахівцям з кібербезпеки щодо захисту корпоративної мережі. Безпека мережевої інфраструктури стосується заходів та практик, що використовуються для захисту апаратного забезпечення, програмного забезпечення та даних, що складають мережу. Вона включає впровадження засобів контролю та протоколів безпеки для запобігання несанкціонованому доступу, захисту від зловмисних атак та забезпечення конфіденційності, цілісності та доступності мережевих ресурсів.

Безпека мережевої інфраструктури важлива, оскільки вона допомагає захистити конфіденційну інформацію від доступу або компрометації неавторизованими користувачами. Вона також допомагає запобігти перебоям у роботі мережі та гарантує, що критично важливі служби та ресурси доступні авторизованим користувачам за потреби.

ПЕРЕЛІК ПОСИЛАНЬ

1. Microsoft Digital Defense Report 2024. URL: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

2. 10 Cyber Security Trends For 2025. By SentinelOne. Updated: May 15, 2025. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/

3. Network Security in 2025: Threats, Security Models and Technologies. Faddom, February 20, 2025. URL: https://faddom.com/network-security-in-2025-threats-security-models-and-technologies/

4. Anand Oswal. 8 Trends Reshaping Network Security in 2025. Palo Alto Networks, Dec 12, 2024. URL: https://www.paloaltonetworks.com/blog/2024/12/8-trends-network-security-in-2025/

5. FortiSASE. Concept Guide. Last updated Feb 13, 2025. URL: https://docs.fortinet.com/product/fortisase

6. FortiGate/FortiOS. Administration Guide, 7.6.2. Last updated Mar 10, 2025. URL: https://docs.fortinet.com/product/fortigate/7.6

7. FortiGate/FortiOS. Best Practices, 7.6.0. Last updated Feb 21, 2025. URL: https://docs.fortinet.com/product/fortigate/7.6

8. Andrew Turner. SP360: Service Provider. Service Provider Security Architecture – Part 2. Cisco. URL: https://blogs.cisco.com/sp/service-provider-security-architecture-part-2

9. Enrico Bottos. Top 5 NGFW solutions for 2025. Nomios Netherlands, Dec 16, 2024. URL: https://www.nomios.com/news-blog/top-5-solutions-ngfw-2025/

10. Top 4 Next-Generation Firewalls (NGFWs) Compared. Check Point. URL: https://www.checkpoint.com/comparison/top-4-ngfw-compared/

11. Keeping Hackers Off Every Edge. Fortinet, 2024. URL: https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-protecting-every-edge.pdf

12. Winning with AI-Powered Network Firewalls. Fortinet, 2024. URL: https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-fortigate-customer-success.pdf

13. FortiGate 100F Series. Data Sheet. Fortinet, 2025. URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-100f-series.pdf

14. ZTNA Architecture 7.0.0. Fortinet. Last updated Mar 25, 2024. URL: https://docs.fortinet.com/document/fortigate/7.0.0/ztna-architecture/800134/what-is-ztna-architecture

15. Fortinet FortiGate 100F. Enterprise-Grade Protection for Smaller Networks. AVFirewalls. URL: https://www.avfirewalls.co.uk/FortiGate-100F.php

16. Karen Scarfone, Paul Hoffman. Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology. Special Publication 800-41, Revision 1. September 2009. 48 p.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)