ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ ФАЄРВОЛІВ SOPHOS XGS»

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Береза В.В.
(прізвище та ініціали)
Керівник Кожухівська О.А.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КСЗІ – Комплексна Система Захисту Інформації

ОС – Операційна Система

ПК – Персональний Комп’ютер

AI – Artificial Intelligence

BYOD – Bring Your Own Device

DMZ – Demilitarized Zone

DPI – Deep Packet Inspection

EDR – Endpoint Detection and Response

ISO – International Organization for Standartization

NGFW – Next Generation Firewall

PCI DSS – Payment Card Industry Data Security Standard

RBAC – Role Based Access Control

SSL – Secure Sockets Layer

VPN – Virtual Private Network

VLAN – Virtual Local Area Network

ВСТУП

Актуальність дослідження. Задля підвищення ефективності бізнес-процесів будь-якого сучасного підприємства відбувається впровадження та застосування сучасних інформаційних технологій. Збільшення кількості інформаційних ресурсів та їх різноманіття обумовлює ускладнення взаємозв'язків між ними, а масовий перехід на віддалений чи змішаний режими роботи, а також використання хмарних середовищ призводять до розширення периметру інформаційної системи.

Застосування сучасних технологій управління доступом до інформаційних ресурсів на базі фаєрволу призведе до більш якісного управління розподіленням доступів, покращення видимості мережі, створення єдиного місця керування периметром мережі, спрощення та оптимізації процесу адміністрування.

……

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження щодо технології управління доступом до інформаційних ресурсів підприємства на базі фаєрволів Sophos XGS.

Об'єкт дослідження – процес управління доступом до інформаційної системи організації на базі фаєрволів Sophos XGS

Предмет дослідження – технологія управління доступом до інформаційної системи підприємства.

Мета роботи – розробити варіант технології управління доступом до інформаційної системи організації, розробка рекомендацій щодо застосування технології управління доступом на підприємстві.

Наукові завдання:

дослідити сутність проблеми управління доступом до корпоративних мереж передачі даних та інформаційних систем;

проаналізувати існуючі технології надання захищеного доступу до корпоративних ресурсів;

проаналізувати методи та засоби забезпечення доступу до корпоративних ресурсів;

встановити сутність завдання управління доступом до корпоративних інформаційних ресурсів;

розробити рекомендації щодо управління доступом до інформаційної системи.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання топології системи управління доступом до інформаційної системи підприємства

Практичне значення одержаних результатів полягає в розробці варіанта технології управління доступом до інформаційних ресурсів підприємства на базі фаєрволів Sophos XGS, а також у розробці рекомендацій щодо застосування технології надання захищеного доступу до корпоративних ресурсів підприємства.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ДОСТУПОМ ДО РЕСУРСІВ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Структура, функції та призначення корпоративної мережі передачі даних

Локальна обчислювальна мережа підприємства – це різновид локальних мереж, що відрізняється від класичних мереж доступу тим, що абонентами такої мережі є співробітники підприємства, якому вона належить. До основних функцій мережі на підприємстві можна віднести:

- концентрацію потоків даних (інформаційних потоків) від абонентів до інформаційних ресурсів підприємства, незалежно від фізичного розташування ресурсів і користувачів;
- забезпечення можливості спільного використання інформаційних ресурсів;
- забезпечення оптимального використання мережевого ПЗ;
- підвищення інформаційної безпеки;
- гнучке розподілення обчислювальних можливостей;
- забезпечення гнучкого адміністрування, включно з управлінням доступом до мережевих ресурсів;

Для подібних мереж, що мають в своїй основі IPv4 адресацію і побудовані відповідно до класичних підходів проектування характерні наявність чітко вираженого периметру, свого роду кордону мережі і декількох відділених одне від одного сегментів мережі (зон), на перетині цих зон встановлюється міжмережевий екран (фаєрвол). Як правило виділяють такі окремі сегменти мережі: WAN, LAN, DMZ, Wi-Fi, серверний сегмент.

LAN – умовно довірена зона, в якій знаходяться ПК співробітників. Прийнято розділяти (сегментувати) таку зону на декілька підмереж та ізолювати їх одне від одного з метою зменшення площі атаки у разі компрометації одного з хостів. Сегментацію можна виконувати за територіальним принципом (користувачі знаходяться в одному приміщенні) або виділяти окремі сегменти опираючись на організаційно-штатну структуру підприємства (окремі підмережі для бухгалтерії, відділу продажів, HR тощо).

DMZ – демілітаризована зона, сегмент мережі, що містить загальнодоступні (публічні) сервіси і відділяє їх від приватних. В якості таких сервісів можуть бути: веб-сервіс (для забезпечення доступності веб-ресурсів, що хостяться локально на сервері, а також балансування навантаження між ними), mail-relay (центральний вузол отримання та пересилки електронних листів, може також перевіряти вхідні листи на спам та наявність вірусів), SBC (контролер сесій IP-телефонії, що забезпечує безпеку та стабільність сервісу).

Серверний сегмент – сегмент мережі, в якому розміщаються корпоративні інформаційні ресурси. До них можна віднести: файлові сховища, CRM-системи, платформи фінансового обліку, системи електронного документообігу, автоматизовані системи управління та моніторингу, сервіси IP-телефонії, електронну пошту.

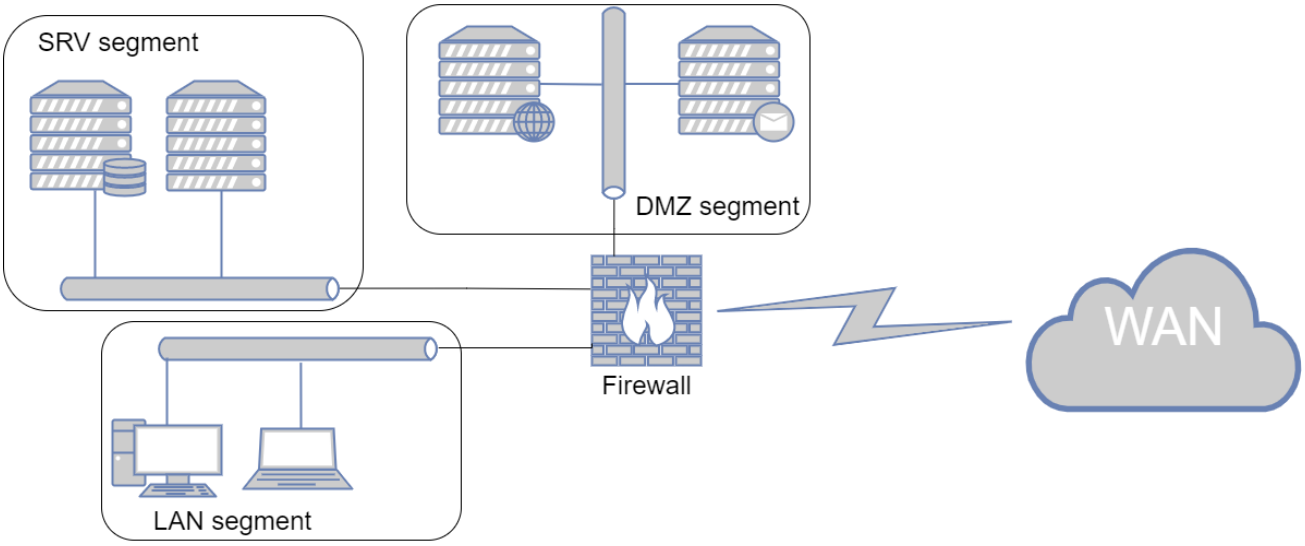


Рисунок 1.1. Приклад сегментування мережі

Фаєрвол (брандмауер, міжмережевий екран) – це система безпеки мережі (інформаційної системи), яка відстежує та контролює вхідний та вихідний мережевий трафік на основі заздалегідь визначених правил. Зазвичай фаєрвол встановлює бар'єр між надійною мережею (довіреною зоною) та ненадійною, такою як Інтернет. Фаєрволи можна умовно розділити на два типи: мережеві та хост-системи (Host-based

firewall). Мережеві брандмауери розташовані між двома або більше мережами [1]. Це програмний або апаратний пристрій, що працює на апаратному забезпеченні загального призначення (звичайних x86 процесорах), апаратному забезпеченні спеціального призначення (виконані по 2-х процесорній схемі з використанням ASIC, FPGA або NPU) або на віртуальному хості під керуванням гіпервізора (VMware ESXi, Microsoft Hyper-V, KVM/QEMU). Сучасні фаєрволи окрім функціоналу пов'язаного з підвищенням безпеки, також можуть виконувати й деякі мережеві функції, такі як служби DHCP, DNS, VPN [2].

За методом розгортання фаєрволи поділяються на:

- Програмні;
- Апаратні;
- Хмарні;

Умовно можна розділити типи фаєрволів на декілька категорій на основі їх загальної структури та методу роботи:

- Брандмауери з фільтрацією пакетів;
- Шлюзи рівня каналів (Circuit-level gateways);
- Брандмауери з перевіркою сесій (Stateful inspection firewalls);
- Шлюзи на рівні додатків (Application-level gateways або брандмауери проксі);
- Фаєрволи наступного покоління (Next Generation Firewall) [3];

Найбільш «базовим» і найстарішим типом архітектури брандамауера є брандмауери з фільтрацією пакетів, які можуть бути запущеними на маршрутизаторі або комутаторі ядра. Такий брандмауер виконує просту перевірку пакетів даних, що надходять через маршрутизатор, перевіряючи таку інформацію, як IP-адреса джерела та призначення, тип пакета (TCP, UDP, ICMP), номер порту та інші деталі мережевого та транспортного рівня, не відкриваючи пакет для перевірки його вмісту [4]. Якщо пакет не пройшов перевірку він може бути відкинутий. Перевагою таких брандмауерів є те, що вони не дуже ресурсомісткі. Використання меншої кількості ресурсів означає, що вони відносно прості та не суттєво впливають на продуктивність системи. Однак їх також можна відносно легко обійти порівняно з брандмауерами, які мають більш

поглиблену перевірку [5]. До брандмауерів подібного типу відносяться: Cisco ACL (Standard/Extended), Linux IPFW, Linux iptables, FreeBSD PF.

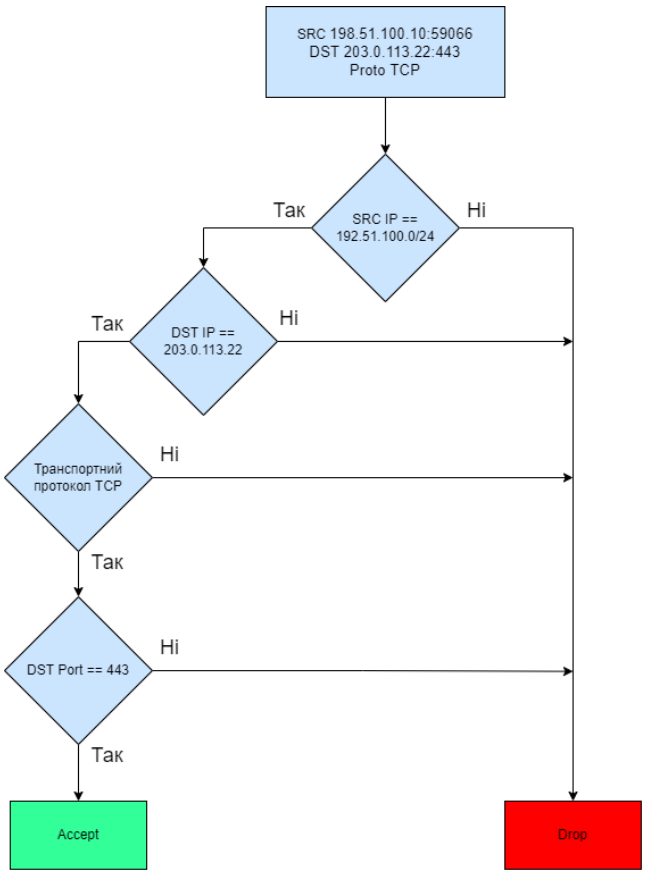


Рисунок 1.2. Приклад алгоритму роботи пакетного фільтра

Шлюзи рівня каналів – спрощений тип брандмауера, призначений для швидкого і спрощеного схвалення або відхилення трафіку без споживання значних обчислювальних ресурсів. Подібні шлюзи працюють шляхом перевірки протоколу TCP, направленої на підтвердження законності сеансу, з якого надходить пакет. До мінусів даної технології можна віднести те, що подібні засоби не перевіряють вміст пакету.

Фаєрволи зі збереженням сесій – цей тип брандмауера поєднує в собі функціонал фаєрволів з фільтрацією пакетів та шлюзів рівня каналів, крім того подібні системи відстежують стан встановлених з’єднань. Простіше кажучи, коли користувач встановлює з’єднання брандмауер створює таблицю стану. Таблиця використовується для зберігання інформації про сеанс, такої як IP-адреса джерела та

призначення, порти джерела та призначення, тощо. Використовуючи цю таблицю брандмауер створює динамічні тимчасові правила для зворотнього трафіку. Подібні фаєрволи здатні визначати наступні подія, як аномалії: поле TTL має значення 0, IP заголовок довжини пакета замалий чи завеликий, неправильна контрольна сума, неправильні опції IP, адреса джерела – broadcast або multicast, адреса джерела відповідає адресі призначення, невірні мітки TCP, порт джерела чи призначення дорівнює 0, невірна контрольна сума TCP або UDP [4].

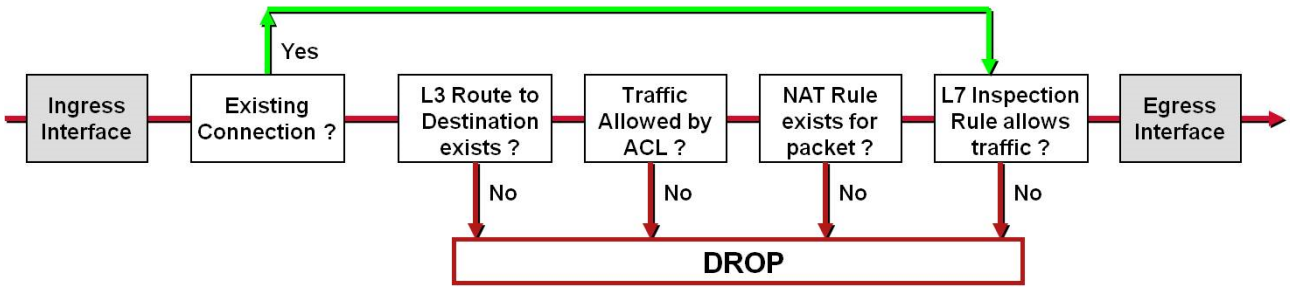


Рисунок 1.3. Приклад алгоритму роботи фаєрволу зі збереженням стану (https://community.cisco.com/t5/security-knowledge-base/revisiting-firewall-performance-parameters/ta-p/3122547)

Проксі брандмауери – працюють на прикладному рівні щоб фільтрувати вхідний трафік. Ці фаєрволи постачаються, як правило, через хмарні рішення або інший проксі-пристрій. Замість того, щоб дозволяти трафіку проходити напряму проксі спочатку встановлює з'єднання з джерелом трафіку та перевіряє вхідний потік даних, а вже потім перенаправляє його адресату. Подібні пристрої можуть виконувати перевірку глибокого рівня (DPI), перевіряючи фактичний вміст пакета. Недоліком таких мережевих екранів є те, що вони можуть значно уповільнювати роботу веб-додатків.

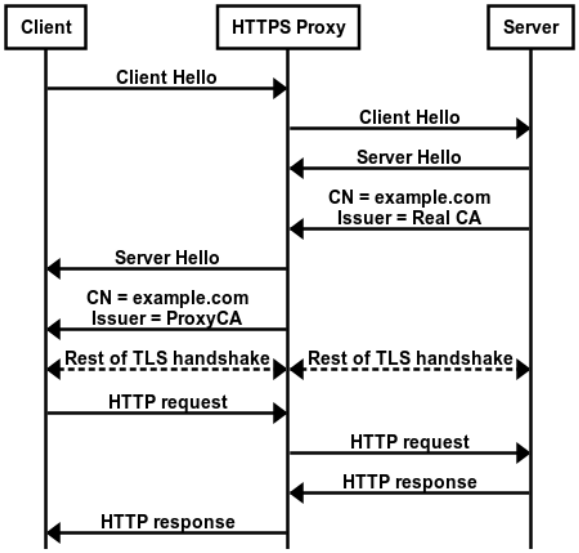


Рисунок 1.4. Принцип роботи брандмауера рівня додатків на прикладі HTTPS-proxy (https://serverfault.com/questions/1012579/how-is-a-proxy-able-to-decrypt-https-traffic-without-the-server-certificates)

Фаєрвол наступного покоління (NGFW) – це різновид фаєрволу, що поєднує у собі можливості брандмауерів, що були розглянуті раніше, а також має додаткові функції направлені на посилення безпеки. Функціонал подібних пристроїв виходить за рамки звичайної інспекції пакетів та блокування на основі протоколів та портів, тут додається інспекція на сьомому рівні OSI, функціонал IPS/IDS, антивірус та інтеграція з іншими системами. NGFW поєднує функції інших типів фаєрволів в єдине рішення, не впливаючи на продуктивність мережі, вони надійніші та пропонують ширшу та глибшу безпеку ніж будь-які інші типи брандмауерів. На додаток до проведення глибоких перевірок пакетів для виявлення аномалій і зловмисного програмного забезпечення, NGFW оснащено функціоналом розпізнавання програм для інтелектуального аналізу трафіку та ресурсів. Ці брандмауери в деякій мірі здатні блокувати DDoS-атаки, мають функцію розшифровки SSL, щоб отримати повну видимість мережевого трафіку. Такі фаєрволи можуть ідентифікувати користувачів і їх ролі, що дозволяє гнучко керувати правами доступу до корпоративних ресурсів [3].

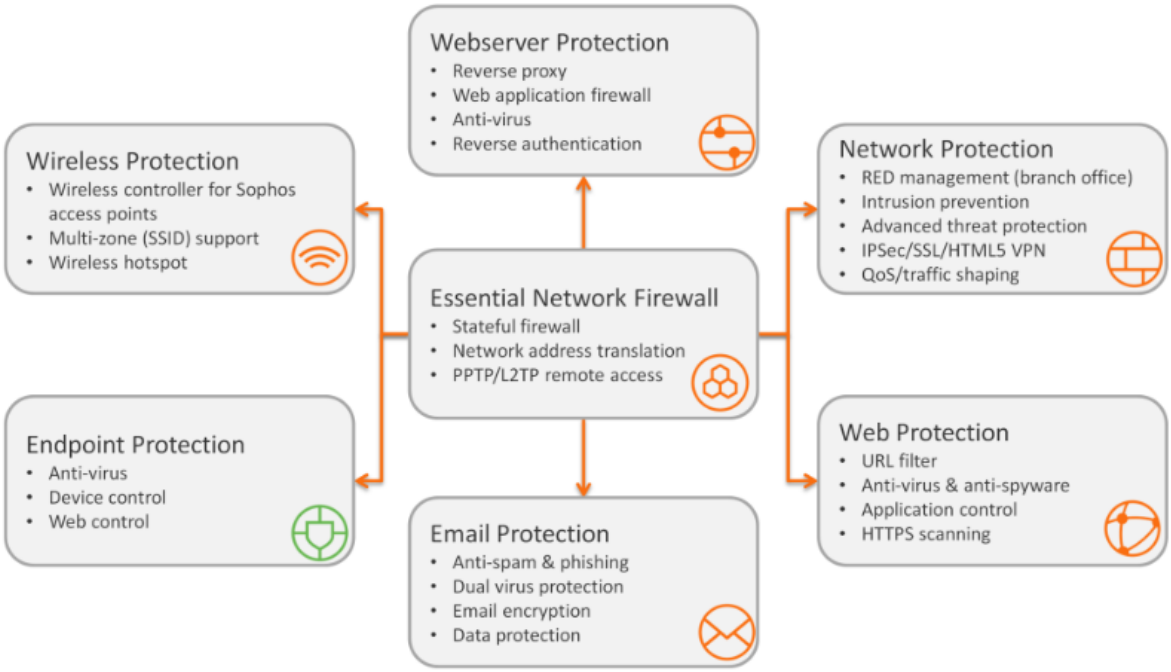


Рисунок 1.5. Можливий набір функцій NGFW (https://www.nekton-ict.com/networksecurity/)

1.2. Аналіз проблеми забезпечення захищеного доступу до корпоративних інформаційних ресурсів

Мережі передачі даних більшості сучасних підприємств вже важко назвати локальними, на це впливають два фактори, перше – це те, що бізнес частково або повністю переносить свої інформаційні ресурси на хмарні платформи. Другим, але не за важливістю є фактор масового переходу на дистанційний або змішаний режим роботи, що тягне за собою необхідність централізованого впровадження технологій забезпечення віддаленого доступу, загалом з початку пандемії кількість атак на сервіси віддаленого доступу зросла на 600% (згідно висновку PurpleSec від 2021 року). Для запобігання подібним атакам необхідне відпрацювання єдиного структурного підходу до контролю доступу та управління користувачами, що в свою чергу призводить ускладнення мережевої інфраструктури, збільшення стеку технологій та відповідно, збільшення вірогідності помилки адміністратора. Згідно аналітичного звіту компанії «Tessian» від 2021 року, 88% порушень даних є прямим результатом людської помилки. Для спрощення управління доступом до

інформаційної системи можна використовувати фаєрвол в якості єдиного центру обробки та управління потоками даних.

Також, останнім часом багато підприємств почало допускати використання співробітниками особистих пристроїв для виконання операційних задач (BYOD). Велика кількість додатків та пристроїв розширює кордони мережі, це призводить до того, що якщо раніше периметром мережі вважався перетин LAN та WAN зон, то зараз починає з'являтися поняття так званого внутрішнього периметру, зона LAN, яку раніше вважали довіреною, стає вразливою. Тому організації більше не можуть довіряти користувачам незалежно від того, знаходяться вони за межами чи всередині мережі. Спеціалісти відділів інформаційної безпеки повинні виходити з того, що кожен пристрій в мережі може бути заражений, а кожен користувач може спеціально чи випадково скомпрометувати критично важливі ресурси.

Критично важливим є питання авторизації та валідації користувачів. Організація повинна знати кожного користувача, що намагається отримати доступ до мережі та її ресурсів. Для підтвердження особи треба ім’я користувача, пароль, двофакторна автентифікація. Також варто використовувати сертифікати для примусового підтвердження. Параметри користувача можуть бути пов’язані з контролем доступу на основі ролей (RBAC), щоб користувач, що пройшов авторизацію, отримував доступ до певних ресурсів. Це називається контролем доступу на основі принципу нульової довіри: користувачі повинні отримувати рівно такий рівень доступу та привілегії при яких вони можуть виконувати свої службові задачі. Після того, як особа користувача засвідчена, політики доступу визначаються його роллю в організації. Не мало важливим фактором також є можливість інтеграції системи надання доступу до мережі зі сторонніми AAA сервісами (RADIUS, AD, LDAP).

Детальне відстеження активності в мережі на основі IP-адрес та облікових записів, також є важливим важливою проблемою з якою часто стикаються адміністратори при проведенні розслідування кіберінцидентів або при аналізі трафіку мережі. Більшість систем безпеки залишають IP-адресу в записах журналу, але не можуть пов’язувати цю IP-адресу з користувачем або пристроєм. Це означає, що в середовищах зі змінними IP-адресами важко визначити, який пристрій або користувач

може бути відповідальним за порушення безпеки, пов'язане з IP. Рішення, що забезпечує управління доступом до інформаційних ресурсів організації повинно відстежувати всі підключені кінцеві точки шляхом постійного моніторингу мережі та надавати різну інформацію про кінцеву точку, яка використовувала IP-адресу в певний момент часу в минулому.

Також можна додати те, що з погляду на сучасні тенденції технологія управління доступу та рішення, яке її реалізує повинне вміти самостійно чи в кооперації з іншими рішеннями протистояти ряду загроз орієнтованих на кінцеві точки та їх користувачів, на рис. 1.6. зображена статистика зібрана агентством «CyberPeace Institute», атак на різні типи підприємств та організацій [6].

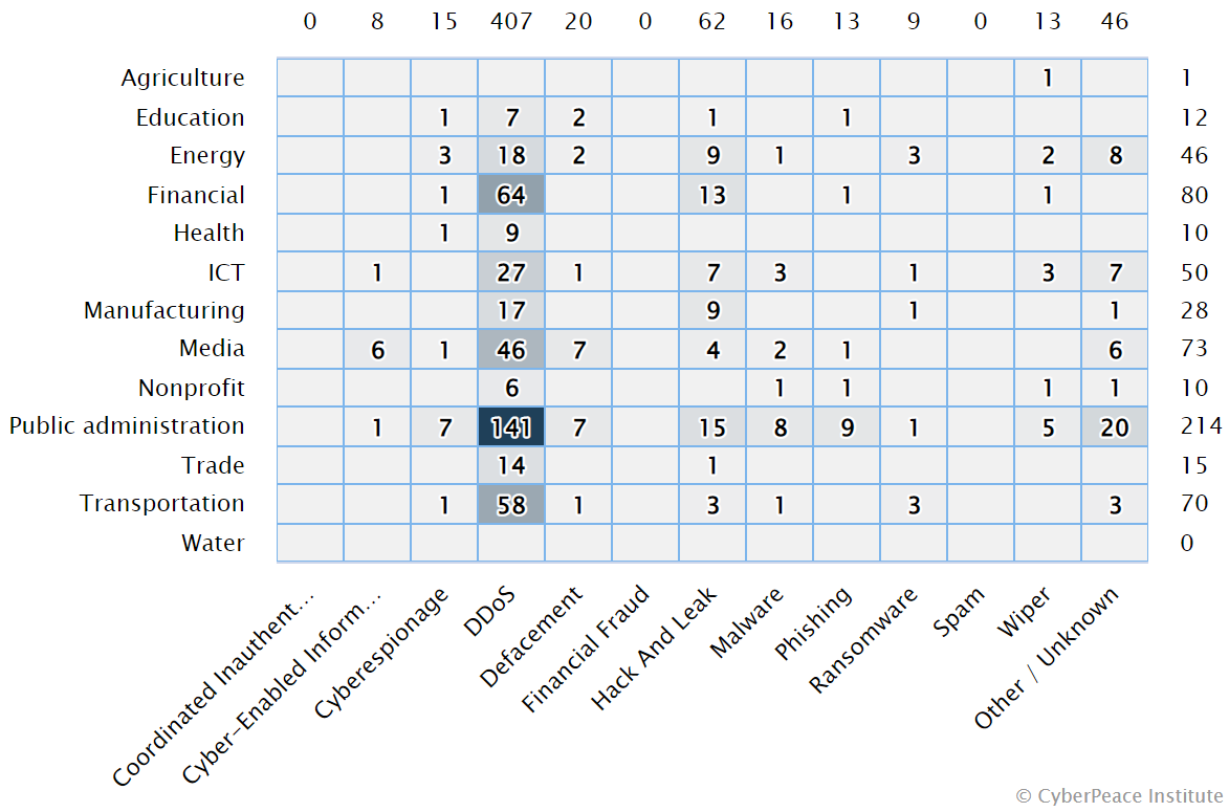


Рисунок 1.6. Статистика кібератак на різні типи організацій (https://cyberconflicts.cyberpeaceinstitute.org/impact)

Загалом можна виділити такі вимоги до системи забезпечення доступу до корпоративних ресурсів інформаційної системи організації:

- Підтримка технологій VPN;
- Двофакторна автентифікація;

- Контроль доступу на основі ролей користувачів;
- Облік та моніторинг підключень користувачів;
- Детальне відстеження переміщення користувачів по мережі з прив'язкою до IP та облікових записів;
- Наявність антивірусу;
- URL-фільтрація;
- Підтримка функцій пріорітезації трафіку (QoS);
- Можливість управління та балансування кількох каналів зв'язку (SD-WAN);

Спеціалісти прогнозують, що ринок рішень управління доступом до інформаційної системи зросте на 27,5%, це пояснюється зростанням впровадження хмарних рішень безпеки різними організаціями для захисту від потенційних кіберзагроз.

1.3. Мета та завдання управління доступом до корпоративної мережі передачі даних

Управління доступом до ресурсів в організації є показником того, наскільки добре організація функціонує. Управління доступом – процес, відповідальний за надання доступу лише авторизованим користувачам дод певних ресурсів та IT-служб, одночасно запобігаючи доступу неавторизованих користувачів. Мета управління доступом – це захист даних від доступу неавторизованих користувачів чи скомпрометованих хостів шляхом обмеження доступу, реєстрації та документування будь-яких дій користувачів; забезпечення доступності інформаційних ресурсів незалежно від часу та місця знаходження клієнтів; забезпечення цілісності інформаційних ресурсів; зменшення можливих негативних наслідків у випадку компрометації одного чи декількох учасників процесу передачі даних.

Завданням керування полягає у тому, щоб для кожної пари «об'єкт-обєкт» чи «суб'єкт-об'єкт» визначити множину допустимих операцій і контролювати виконання встановленого порядку. Відношення «суб'єкт-об'єкт» можна представити у вигляді

матриці, в рядках якої перелік суб’єктів, а у стовбцях – об’єктів, в клітинках на перетині записані додаткові умови і дозволені види доступу.

Система керування доступом до мережі організації повинна виконувати такі функції:

- Гарантувати збереження конфіденційності інформації шляхом контролю доступу до різних IT-ресурсів;
- Гарантувати те, що працівники мають лише необхідний рівень доступу для ефективного виконання своїх задач;
- Зменшення площі атаки у разі компрометації одного з ресурсів;
- Надання засобів перевірки IT-інфраструктури і відстеження будь-якого зловживання послугами;
- Гарантія того, що доступ до служби для певного користувача може бути скасований, коли це необхідно для дотримання вимог безпеки.

Враховуючи проблеми управління доступом до корпоративних ресурсів можна виділити наступні задачі, які повинен виконувати сучасний комплекс керування доступом:

- Керування життєвим циклом політик безпеки;
- Перевірка стану безпеки: оцінка відповідності політиці безпеки по типу користувача, типу пристрою та операційній системі;
- Керування ідентифікацією і доступом;
- Протистояння атакам нульового дня;
- Авторизація, автентифікація та облік мережевих з’єднань (AAA);
- Контроль доступу на основі профілів користувачів;
- Профілювання: виявлення скомпрометованих пристроїв до того, як шкідливий код зможе завдати шкоди;
- Реагування на інциденти: нейтралізація мережевих загроз застосуванням політик безпеки, що блокують небажаний трафік ізолюють скомпрометованих користувачів та ресурси, відновлюють працездатність сервісів;
- Генерація звітів і аналітичних даних про спроби доступу.

1.4. Аналіз існуючих технологій управління доступом до ресурсів корпоративної інформаційної системи

На сьогоднішній день для вирішення проблеми управління доступом до інформаційної системи існує два базових підходи: побудова інфраструктури навколо фаєрволу з можливостями контролю доступу та використання спеціалізованого рішення NAC (Network Access Control).

NAC – це підхід до інформаційної безпеки, який дозволяє адміністраторам забезпечувати єдиний контроль доступу у всіх типах мереж та складається з двох основних елементів:

- Протокол 802.1X – стандарт IEEE для керування доступом до мережі на основ портів у дротових та бездротових мережах. 802.1X визначає елементи керування автентифікацією для будь-якого користувача або пристрою, який намагається отримати доступ до інформаційної системи;
- NAC – мережева концепція, яка ідентифікує користувачів і пристрої, контролюючи доступ до мережі. NAC контролює доступ до корпоративних ресурсів за допомогою авторизації та застосування політик безпеки.

NAC забезпечує контроль за тим, до яких сегментів мережі та до яких додатків отримує доступ користувач на основі:

- Інформації про користувача, що підключається;
- Інформації про стан комп’ютера;
- Часу підключення;
- Точки підключення.

Конкретні реалізації NAC можуть враховувати всі ці критерії, частину з них чи враховувати додаткові. Призначення правил контролю доступу спецефічних для конкретного користувача, з урахуванням цих критеріїв, відбувається тільки коли він проходить всі необхідні перевірки. Після застосування правил контролю доступу відбуваються періодичні повторні перевірки відповідності політикам контролю

доступу. Архітектурно подібне рішення відрізняється від рішення на базі фаєрволу наявністю сервера контролю доступу, на якому здійснюється управління доступом [7].

Дане рішення може суттєво посилити систему інформаційної безпеки але має ряд недоліків пов’язаних зі складністю інтеграції, вартістю, масштабованістю та відмовостійкістю системи. Окремо слід виділити те, що подібна система вимагає великих трудовитрат при щоденній експлуатації та наявності окремого спеціаліста, який буде займатися її обслуговуванням, що є неприйнятним для підприємств великого та середнього бізнесу [8].

Альтернативою спеціалізованим рішенням є побудова системи NAC довкола фаєрволу наступного покоління, що має можливість інтеграції з рішеннями захисту кінцевих точок (антивірусами), одним з таких рішень є міжмережевий екран наступного покоління Sophos XGS. Така схема допомагає: спростити управління системою захисту інформаційної системи за рахунок створення єдиного центру управління мережею на базі фаєрволу; здешевити систему в цілому. В подібній схемі можна виділити такі основні елементи: фаєрвол; антивірусне ПЗ встановлене на кінцевих точках; консоль управління антивірусом; AAA-сервіс (опціонально).

При управлінні доступом до інформаційних ресурсів важливим елементом є управління обліковими записами. Більшість систем надання доступу на базі фаєрволів мають можливість «забирати» облікові записи з чотирьох різних джерел:

- Локально;
- LDAP;
- Active Directory;
- RADIUS.

Найпоширенішим варіантом ведення обліку користувачів є локальна база даних, при такому методі всі облікові записи та їх параметри створюються адміністратором системи та зберігаються безпосередньо в сховищі фаєрволу. При створенні користувача обов’язково потрібно вказати такі параметри, як: логін; ім’я; пароль; адресу електронної пошти; групу; час, коли цей користувач активний; політики для віддаленого доступу (SSL VPN, L2TP, PPTP, IPsec). Також є ряд додаткових

налаштувань, а саме: «Surfing quota» (скільки часу користувач може провести в Інтернеті); обмеження полоси пропускання; MAC та IP-адреси пристроїв з яких цей користувач може «залогінитись». Важливо перед створенням локальних користувачів потурбуватись про створення груп, до яких вони належать, гарною практикою в такому випадку є розділити користувачів по групам за типом задач, які вони виконують і інформаційними ресурсами, які їм для цього потрібно, в такому випадку можна спиратися на організаційно-штатну структуру підприємства. Ведення обліку користувачів локально на фаєрволі є найпростішим варіантом і має менше трудовитрат в адмініструванні у порівнянні з інтеграцією сторонніх AAA-сервісів. Але подібна система має ряд недоліків пов'язаних з масштабуванням системи у випадку додавання нового фаєрволу на іншій локації та відновленням її у разі виникнення надзвичайних ситуацій (наприклад, фаєрвол вийшов з ладу). Подібна схема підходить скоріш для невеликих підприємств з кількістю співробітників до 50 осіб.

Альтернативою для локального збереження користувачів є ведення їх обліку централізовано в сторонніх AAA сервісах. Подібна модель робить систему більш масштабованою, гнучкою та відмовостійкою. Досвідчені адміністратори та IT-команди використовують подібні системи для створення «конвеєрів», коли при створенні нового користувача, наприклад в AD, для нього автоматично створюються параметри доступу до мережі, обліковий запис 802.1x, обліковий запис електронної пошти, акаунт в корпоративній телефонній мережі та ін.

AAA розшифровується, як «Authentication, Authorization, Accounting», автентифікація, авторизація, облік. Автентифікація надає спосіб ідентифікації користувача, зазвичай шляхом введення дійсних імені користувача та пароля перед наданням доступу до мережі. Автентифікація базується на наявності у кожного користувача унікального набору облікових даних для входу в мережу чи систему. Сервер AAA порівнює облікові дані користувача з обліковими даними інших користувачів, які зберігаються в базі даних; у різних випадках цією базою даних можуть бути AD, LDAP, RADIUS. Якщо облікові дані користувача збігаються, користувачеві надається доступ до мережі. Якщо облікові дані не збігаються,

автентифікація не вдається, і доступ до мережі буде заборонено. Після автентифікації користувач повинен отримати авторизацію для виконання певних завдань. Після входу в систему, наприклад, користувач може спробувати видавати команди. Процес авторизації визначає, чи має користувач повноваження видавати такі команди. Простіше кажучи, авторизація — це процес забезпечення виконання політик — визначення того, які типи чи якості дій, ресурсів або послуг дозволено користувачеві. Зазвичай авторизація відбувається в контексті автентифікації. Після того, як ви автентифікували користувача, він може бути авторизований для різних типів доступу або діяльності. Що стосується автентифікації мережі через RADIUS і 802.1x, авторизацію можна використовувати для визначення VLAN, списку контролю доступу (ACL) або ролі користувача, до якої належить користувач. Останньою частиною структури AAA є облік, який відстежує ресурси, які користувач споживає під час доступу до мережі. Це може включати кількість системного часу або кількість даних, надісланих і отриманих під час сеансу. Облік здійснюється шляхом реєстрації статистики сеансу та інформації про використання. Він використовується для контролю авторизації, виставлення рахунків, аналізу тенденцій, використання ресурсів і планування обсягу даних, необхідного для бізнес-операцій. ClearPass Policy Manager функціонує як сервер обліку та отримує облікову інформацію про користувача від сервера доступу до мережі (NAS). NAS має бути налаштований на використання диспетчера політик ClearPass як сервера обліку, і саме NAS має надати точну облікову інформацію менеджеру політик ClearPass.

LDAP (Lightweight Directory Access Protocol) – це відкритий, нейтральний до виробника галузевий стандартний прикладний протокол для доступу та підтримки розподілених інформаційних служб каталогу через IP-мережу. Служби каталогів відіграють важливу роль у розробці додатків внутрішньої мережі та Інтернету, дозволяючи обмінюватися інформацією про користувачів, системи, мережі, служби та програми по всій мережі. Як приклад, служби каталогів можуть надавати будь-який організований набір записів, часто з ієрархічною структурою, як-от корпоративний каталог електронної пошти. Так само телефонний довідник — це список абонентів із зазначенням адреси та номера телефону. Зазвичай LDAP використовується для

забезпечення центрального місця для зберігання імен користувачів і паролів. Це дозволяє багатьом додаткам і службам підключатися до сервера LDAP для перевірки користувачів.

AD (Active Directory) – це служба каталогів, розроблена Microsoft для доменних мереж Windows. Він включений до більшості операційних систем Windows Server як набір процесів і служб. Спочатку Active Directory використовувався лише для централізованого керування доменом. Однак Active Directory згодом стала загальною назвою для широкого спектру служб ідентифікації на основі каталогів. Сервер, на якому виконується роль доменної служби AD, називається контролером домену. Він автентифікує та авторизує всіх користувачів і комп'ютери в мережі типу домену Windows, призначаючи та впроваджуючи політики безпеки для всіх комп'ютерів, а також інсталюючи або оновлюючи програмне забезпечення. Наприклад, коли користувач входить до комп'ютера, який є частиною домену Windows, Active Directory перевіряє подані ім'я користувача та пароль і визначає, чи є користувач системним адміністратором чи звичайним користувачем. Крім того, він дозволяє керувати інформацією та зберігати її, надає механізми автентифікації та авторизації та встановлює структуру для розгортання інших пов'язаних служб: служб сертифікації, служб об'єднання AD, полегшених служб каталогів і служб керування правами. Active Directory використовує LDAP версій 2 і 3, версію Microsoft Kerberos і DNS. Важливо відмітити, що рішення вендору Sophos мають велику кількість глибоких інтеграцій з рішеннями Microsoft, однією з таких інтеграцій є «Sophos Transparent Authentication Suite» (STAS). STAS дозволяє користувачам у домені Windows автоматично ідентифікуватись на XGS Firewall під час входу в Windows. Це усуває необхідність багаторазового входу та клієнтів SSO на кожному клієнтському пристрої. STAS складається з агента та колектора. Агент відстежує запити на автентифікацію користувачів і надсилає інформацію збирачеві для автентифікації. Колектор збирає запити на автентифікацію користувача від агента, обробляє запити, а потім надсилає їх на брандмауер для автентифікації.

RADIUS (Remote Authentication Dial-In User Service) – це мережевий протокол, який забезпечує централізоване керування автентифікацією, авторизацією та

обліковим записом (AAA) для користувачів, які підключаються та використовують мережеву службу. RADIUS — це клієнт/серверний протокол, який працює на прикладному рівні та може використовувати TCP або UDP. Сервери доступу до мережі, які контролюють доступ до мережі, зазвичай містять клієнтський компонент, який спілкується з сервером. RADIUS часто є базовою системою вибору для автентифікації 802.1x. Загалом основною відмінністю даного протоколу від попередніх є те, що він підтримує більшу кількість атрибутів (що в корпоративних мережах не є важливою вимогою) та зазвичай розгортається на UNIX-подібній платформі, у той час коли LDAP та AD більш поширені в Windows-сумісних середовищах й мають глибокий рівень інтеграції з ОС компанії Microsoft [9].

Загальний принцип авторизації користувачів з використанням AAA-серверу, на прикладі протоколу RADIUS, зображено на рис. 1.7.

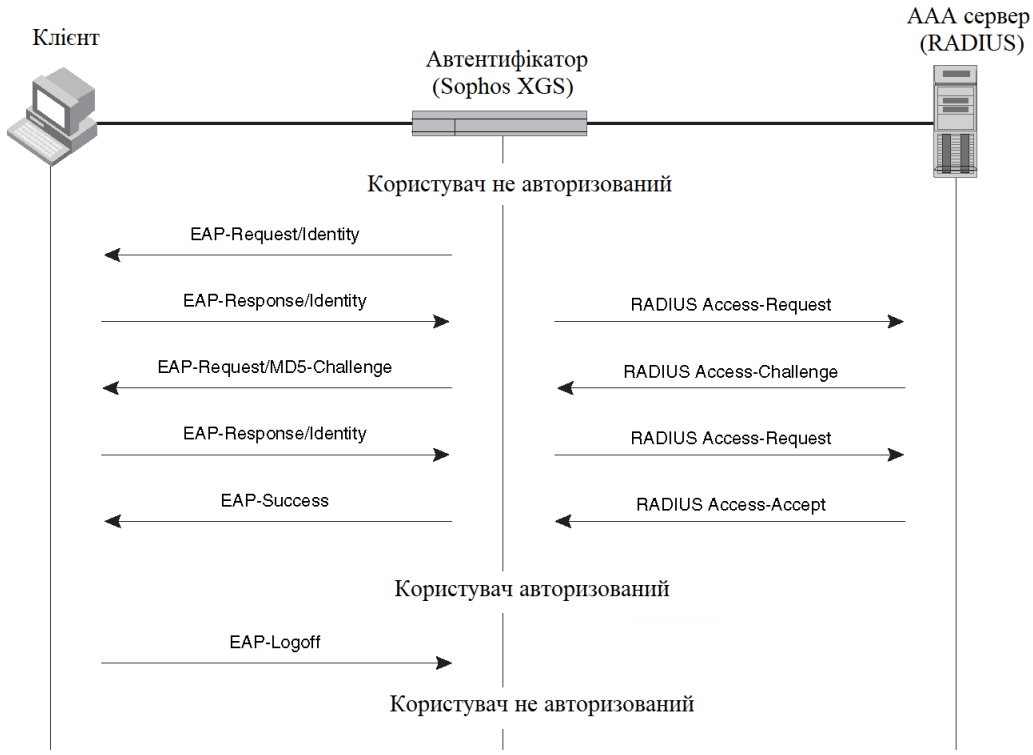


Рисунок 1.7. Приклад авторизації користувача з використанням RADIUS (https://helpiks.org/9-55277.html)

Загалом можна сказати, що з метою спрощення системи, економії фінансових ресурсів та економії часу більш доцільно використовувати технологію управління доступом до інформаційної системи підприємства на базі фаєрволів з використанням інтеграції зі сторонніми сервісами захисту інформації.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ ФАЄРВОЛІВ SOPHOS XGS

2.1. Призначення, можливості та функції Sophos XGS

В наш час відбувається зміна в архітектурі загроз та різке збільшення кількості та складності систем безпеки, і звичайно відбувається еволюція в розробці засобів захисту, в тому числі міжмережевих екранів.

Міжмережеві екрани нового покоління (Next-Generation Firewall, NGFW) — інтегровані платформи, в яких класичні фаєрволи і маршрутизація поєднуються з новітніми ідеями для фільтрації трафіку, такими як системи глибокого аналізу трафіку (Deep Packet Inspection, DPI), автентифікація користувача будь-яким способом, система попередження вторгнень (Intrusion Prevention System IPS) та ін.

Раніше, міжмережеві екрани працювали на нижніх рівнях мережевого стеку, забезпечуючи базову маршрутизацію, а також фільтрацію пакетів на основі перевірки

портів і протоколів для переадресації або блокування трафіку. Вони були ефективні для свого часу. Оскільки загрози перейшли від атаки безпосередньо на мережу до ураження внутрішньої системи, як правило, за допомогою вразливостей у додатках і серверах або використання соціальної інженерії, рішення мережевого захисту повинні розвиватися, щоб протистояти новим векторам атаки. Організації, будучи вимушеними постійно додавати та оновлювати парк пристроїв безпеки у своєму мережевому периметрі для запобігання вторгненням, веб-фільтрації, захисту від спаму та захисту веб-додатків (WAF) несуть значні грошові та часові витрати. Необхідність управління масивом продуктів мережевої безпеки привела до створення Unified Threat Management (UTM) — такі рішення дозволять організаціям об'єднати все в одному пристрої. Технологія міжмережевих екранів також еволюціонувала, піднімаючись вище по стеку OSI до сьомого рівня, щоб уміти ідентифікувати та контролювати трафік від програм. Фаєрволи також стали включати технології для більш глибокого вивчення вмісту мережевих пакетів і пошуку загроз. Вони отримали можливість класифікувати і керувати трафіком, створеним користувачем або додатком, і не покладатися тільки на протоколи і порти. Цей перехід породив нову мережеву категорію: мережеві екрани наступного (NGFW).

NGFW поєднує в собі традиційні методи поряд з глибокою перевіркою пакетів, що включає запобігання вторгненням, отримання відомостей про додатки, політики користувача і можливість перевірки зашифрованого трафіку. Мережева безпека продовжує послідовно змінюватися і рости щоб протистояти постійним змінам. Сучасні загрози, такі як вимагачі та ботнети є більш просунутими, невловимими та цілеспрямованими, ніж будь-коли раніше. Ці просунуті загрози (Advanced Threats APTs) використовують zero-day методи і їх надзвичайно складно виявити. Загалом можна сказати, що характер нинішніх загроз та сучасної мережевої інфраструктури створюють необхідність в фундаментальних змінах підходів до мережевої безпеки:

- Системи мережевої безпеки повинні мати інтеграції з новими технологіями для виявлення шкідливої поведінки серед корисного навантаження на мережу без використання традиційних антивірусних сигнатур. Такі технології, як пісочниця, донедавна були рішеннями, які могли дозволити собі лише великі

компанії, стали доступними для невеликих та середніх організацій і є невід'ємною частиною ефективного захисту від сучасних шкідливих програм;

- Системи безпеки, які раніше були ізольованими та незалежними, такі як міжмережевий екран та антивірус, тепер потребують інтеграції та спільної роботи для швидкого та ефективного виявлення, ідентифікації та реагування на просунуті загрози, перш ніж вони можуть завдати значної шкоди;
- Нові динамічні технології керування додатками необхідні для правильної ідентифікації та керування невідомими додатками, враховуючи неефективність сигнатурних механізмів для ідентифікації нових додатків, додатків користувачів та додатків, що використовують загальні протоколи HTTP/HTTPS;
- Системи мережевої безпеки повинні мати вбудовані механізми для керування доступом користувачів до інформаційної системи організації; вміти моніторити, вчасно виявляти аномалії в поведінці користувачів та реагувати на інциденти безпеки в автоматичному чи напівавтоматичному режимі.

Sophos XGS Firewall був розроблений для вирішення сучасних проблем, а також для забезпечення платформи, що адаптується під зміну мережевої архітектури. Sophos XGS пропонує новий підхід до виявлення прихованих ризиків, захисту мережі, виявлення загроз та реагування на них.

Sophos XGS забезпечує видимість користувачів із групи ризику, небажаних програм, підозрілих даних та постійних загроз. Він має повний набір сучасних технологій захисту від загроз, і при цьому простий у налаштуванні та обслуговуванні. На відміну від будь-якого іншого міжмережевого екрану до нього, Sophos XGS взаємодіє з іншими системами безпеки в мережі, що дозволяє йому ефективно стати надійною точкою захисту, стримувати загрози, блокувати шкідливе програмне забезпечення від поширення або ексфільтрації даних з мережі – автоматично, в режимі реального часу. Sophos XGS має чотири основні переваги у порівнянні з іншими міжмережевими екранами:

- Виявлення прихованих ризиків;
- Блокування невідомих загроз;

- Автоматичне реагування на інциденти;
- Можливість тонкого налаштування та розподілення прав доступу користувачів мережі.

Критично важливо, щоб сучасний фаєрвол міг аналізувати великі обсяги даних, які він збирає, корелював їх і виділяв лише найважливіше, що потребує дій.

Сьогодні проблема управління додатками в NGFW заключається в тому, що більшість трафіку програм залишається нерозпізнаним. Ця проблема має просту причину: всі механізми контролю додатків використовують сигнатури і шаблони для їх ідентифікації і дуже багато меркетингових додатків, таких як медичні чи фінансові додатки, не мають своїх сигнатур, деякі типи додатків (напр. клієнти bittorent чи VoIP) постійно змінюють свою поведінку і сигнатури. Багато сервісів використовують шифрування, щоб запобігти виявленню, в той час як деякі просто використовують «загальні» підключення подібні до веб браузера й використовують порти 80 та 443. Кінцевим результатом є повна відсутність видимості додатків у мережі, а адміністратор не може контролювати те, чого не бачить. Рішенням цієї проблеми від Sophos є «Synchronized Application Control», що використовує унікальну технологію Synchronized Security у зв'язці продуктами Sophos на кінцевих станціях («Sophos Intercept X» та «Sophos Intercept X for Servers»). Коли Sophos XGS бачить трафік, який не може ідентифікувати по сигнатурі, він може запитати кінцеву точку, який додаток генерує цей трафік. Потім ПЗ на кінцевій точці може переглянути виконуваний файл, шлях і визначити категорію програми, передати цю інформацію назад в XGS. Потім міжмережевий екран у більшості випадків, може використовувати цю інформацію для автоматичної класифікації та керування додатком. Якщо Sophos XGS не може автоматично визначити відповідну категорію програми, адміністратор може встановити потрібну категорію або призначити програмі існуючу політику вручну. Після класифікації додатку — неважливо, автоматичним способом, або адміністратором мережі — додаток піддається тим самим політикам, що й інші додатки у цій категорії, що дозволяє легко блокувати всі невідомі додатки у яких немає необхідності, і пріоритизувати критичні застосунки.

Користувачі є найслабшою ланкою в ланцюзі безпеки, і моделі поведінки людини можуть використовуватися для прогнозування та запобігання атакам. Крім того, шаблони використання можуть допомогти проілюструвати ефективність використання корпоративних ресурсів та необхідність тонкого настроювання політик користувачів. Користувацький коефіцієнт загроз (UTQ) допомагає адміністратору безпеки виявляти користувачів, які становлять ризики на основі підозрілої поведінки в інтернеті та історії загроз та заражень. Висока оцінка ризику UTQ користувача може бути ознакою ненавмисних (або навмисних) дій через відсутність поінформованості про безпеку, зараження шкідливим програмним забезпеченням. Усвідомлення дій користувача, які викликали ризик, може допомогти адміністратору мережевої безпеки вжити необхідних дій.

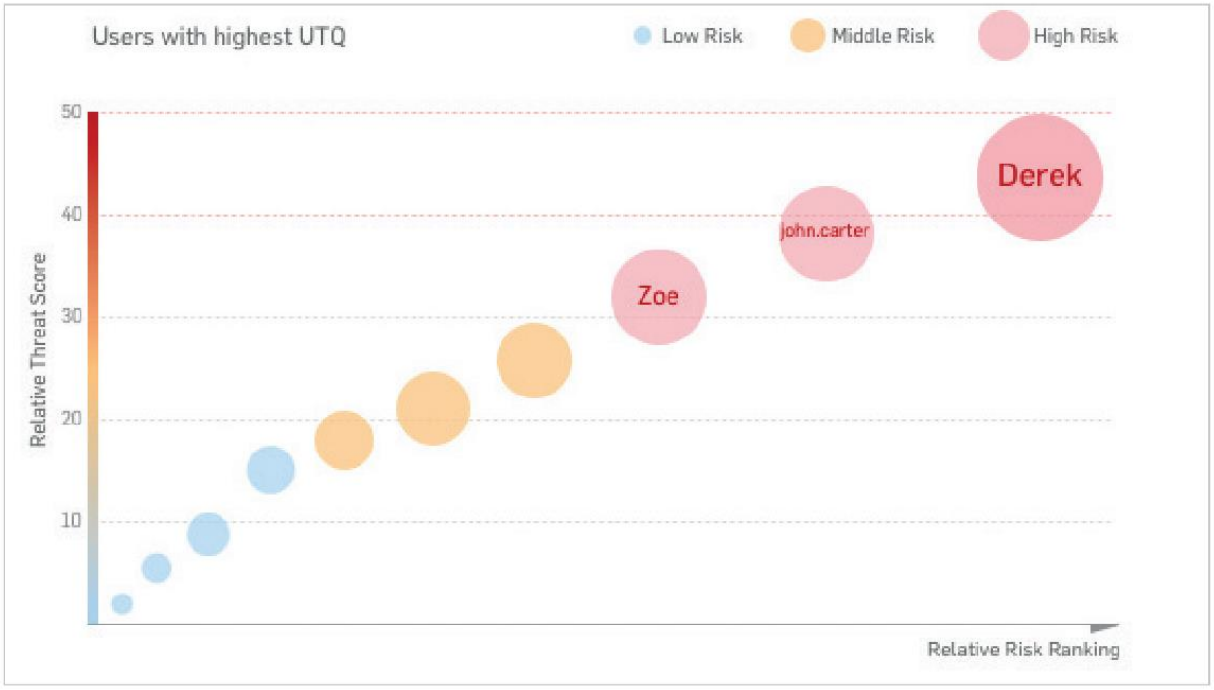


Рисунок 2.1. Приклад звіту UTQ
(https://www.sophos.com/en-us/products/next-gen-firewall)

Веб-фільтрація та контроль є основним елементом будь-якого міжмережевого екрану, але, на жаль, у більшості продуктів реалізація цієї функції виявляється другорядною. В Sophos XGS вбудована нова модель політик веб-фільтрації з великою кількістю попередньо налаштованих шаблонів та політик, це дозволяє адміністратору

тонко налаштовувати правила фільтрації. Веб-політики включають можливість реєстрації, моніторингу та застосування політик, пов’язаних з динамічним вмістом на основі списків ключових слів. Ця функція особливо важлива в навчальних закладах для забезпечення безпеки в інтернеті. Бібліотеки ключових слів можуть бути завантажені в Sophos XGS і застосовані до будь-якої політики веб-фільтрації як додаткові критерії з діями для реєстрації, моніторингу, блокування результатів пошуку або веб-сайтів, що містять ключові слова.

Такі просунуті загрози, як віруси вимагачі, стають більш цілеспрямованими і прихованими, існує гостра необхідність у поведінковому аналізі корисного навантаження (файлів, що скачуються і одержуються поштою). Донедавна технологія пісочниці, необхідна забезпечення цього захисту, була доступна лише найбільшим компаніям. Але тепер завдяки хмарним рішенням для пісочниці, таким як «Sophos Sandstorm», це доступно навіть для малого бізнесу. «Sophos Sandstorm» надає потужне рішення пісочниці в хмарі, просте та доступне, забезпечуючи при цьому необхідний захист від загроз нульового дня, що ховаються в електронній пошті та веб-трафіку – основних векторах атак. Він тісно інтегрований в Sophos XGS і простий у налаштуванні, і оскільки він хмарний, для нього не потрібне додаткове програмне або апаратне забезпечення і він не впливає на продуктивність міжмережевого екрану. Підозрілі вкладення електронної пошти та файли, що завантажуються, автоматично аналізуються та запускаються в хмарній пісочниці, щоб визначити їхню поведінку, перш ніж вони будуть дозволені до завантаження у мережу. «Sophos Sandstorm» надає висновки аналізу корисного навантаження на Sophos XGS Control Center і має широкий набір докладної звітності за всіма файлами та загрозами, що аналізуються та обробляються міжмережевим екраном.

Рисунок 2.2. Приклад звіту пісочниці

Advanced Threat Protection необхідна для виявлення просунутих загроз, ботів та інших шкідливих програм, що ховаються у мережі. Sophos XGS використовує складну комбінацію виявлення шкідливого трафіку, виявлення бот-мереж та трафіку до C&C. Він об'єднує аналіз IPS, DNS та URL-адрес, щоб виявити шкідливий трафік і негайно ідентифікувати не тільки заражений хост, а й користувача та процес [11].

Фаєрволи Sophos XGS мають широкі можливості як для встановлення в новій мережі, так і для інтеграції в існуючу інфраструктуру, на рис. 2.3. зображено три можливі варіанти встановлення фаєрволу, у якості шлюза безпеки, в «прозорому» режимі та в режимі моніторингу мережі.

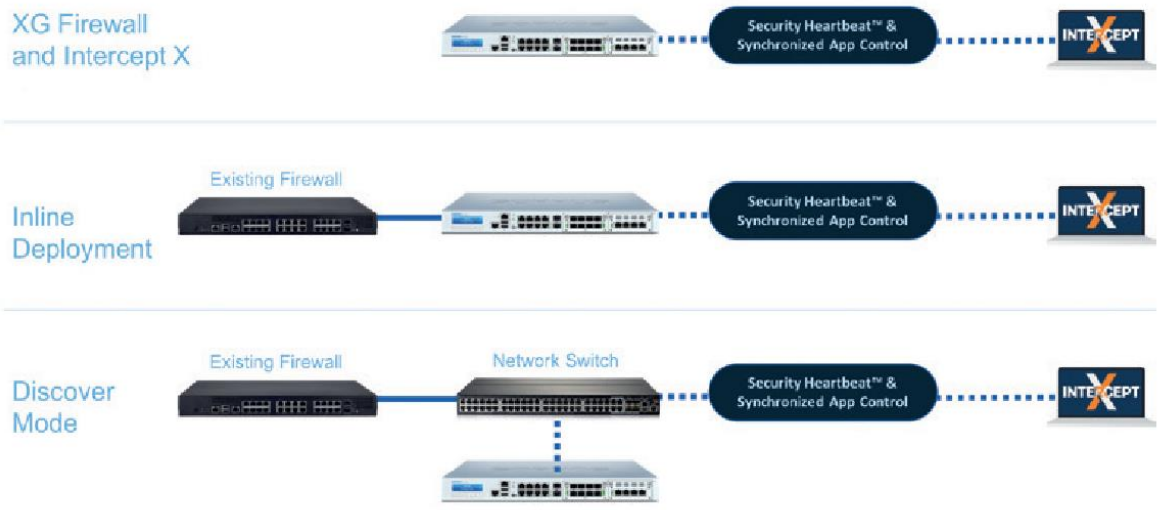


Рисунок 2.3. Варіанти включення Sophos XGS
(https://www.enterpriseav.com/59486/sophos-xg-firewall)

При розгортанні Sophos XGS, як міст третього рівня (у режимі шлюзу), адміністратору доступні до використання всі його функції безпеки, а також використання фаєрволу для маршрутизації трафіку, фаєрвол підтримує усі основні протоколи маршрутизації (статичні маршрути, OSPF, BGP, RIP), має функціонал SD-WAN, MPLS, функціонал пріоритезації трафіку QOS, «Policy Based Routing», подібний набір можливостей значно розширює можливості фаєрволу та дозволяє зекономити на встановленні додаткового маршрутизатора. В подібній схемі брандмауер Sophos XGS буде використовуватися в режимі шлюзу, де йому потрібно керувати маршрутизацією між кількома мережами та зонами, і він є точкою входу та виходу для мережі, даний вид архітектури є рекомендованим для використання всього функціоналу пристрою, але є доволі трудомістким при інтеграції фаєрволу в існуючу мережу. У прикладі наведеному на рис. 2.4. зображена мережа з брандмауером, який служить шлюзом.

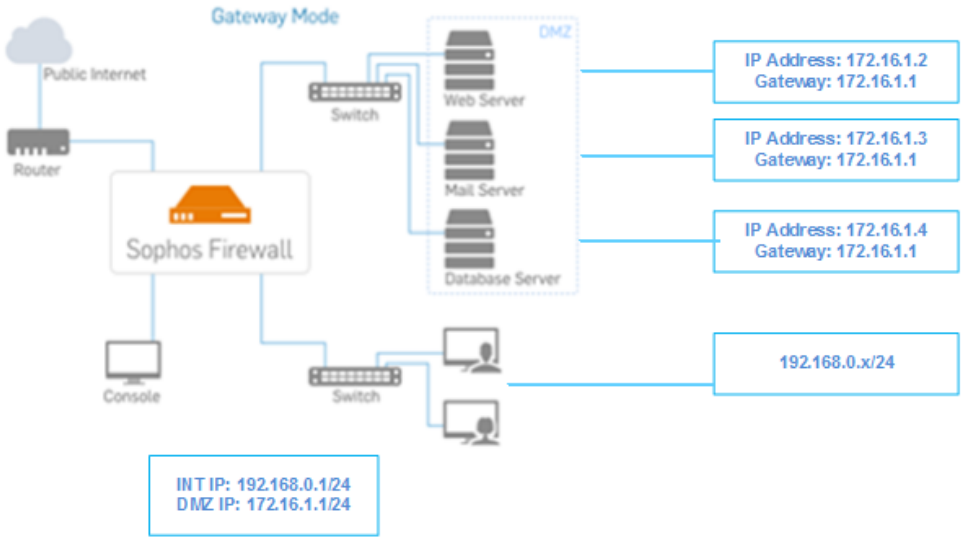


Рисунок 2.4. Розгортання фаєрволу в режимі шлюза (https://docs.sophos.com/nsg/sophos-firewall/19.5)

При налаштуванні Sophos XGS, як міст другого рівня (у режимі мосту), до використання доступні такі функції, як глибока перевірка пакетів, система запобігання вторгненням, сканування зловмисного програмного забезпечення та сканування вмісту електронної пошти. На рис. 2.5. наведено мережу, де наявний брандмауер або

маршрутизатор присутній на периметрі мережі та Sophos XGS розгорнутий в режимі моста. Подібна схема дозволяє інтегрувати фаєрвол у мережу не змінюючи її дизайн, тобто, фаєрвол ніяк не участує в IP-плані маршрутизації. Режим моста є ідеальним рішенням для мереж, у яких уже є брандмауер або маршрутизатор, що виконує роль шлюзу, і де клієнт не бажає замінювати брандмауер, але все ж бажає додати додатковий захист за допомогою глибокої перевірки пакетів пристрою, запобігання вторгненню; використовувати системні, шлюзові антивірусні та антиспам-сервіси. Режим моста також підтримує протокол Spanning Tree.

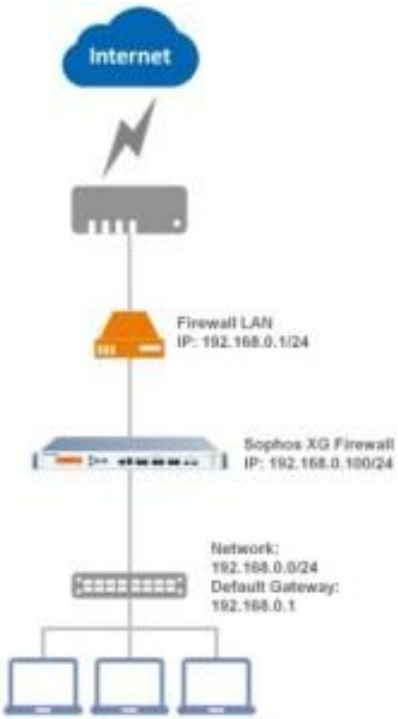


Рисунок 2.5. Розгортання фаєрволу в режимі моста
(https://docs.sophos.com/nsg/sophos-firewall/19.5)

При розгортанні Sophos XGS у режимі виявлення, можна контролювати мережевий трафік, не вносячи жодних змін у мережеву схему. В подібній схемі Sophos XGS виявляє мережевий трафік за допомогою інтерфейсу TAP і надсилає звіти про перевірку безпеки (SAR) електронною поштою. На рис. 2.6. зображено подібну схему, коли комутатор виконує «Port Mirroring» й перенаправляє копію всього мережевого трафіку на фаєрвол, слід зазначити, що зняття копії трафіку заме з

комутатора ядра є опціональним і за необхідності можна аналізувати трафік з зовнішнього інтерфейсу прикордонного маршрутизатора (фаєрвола), чи від окремого сегменту мережі налаштувавши «Port Mirroring» на комутаторі доступу чи агрегації [14].

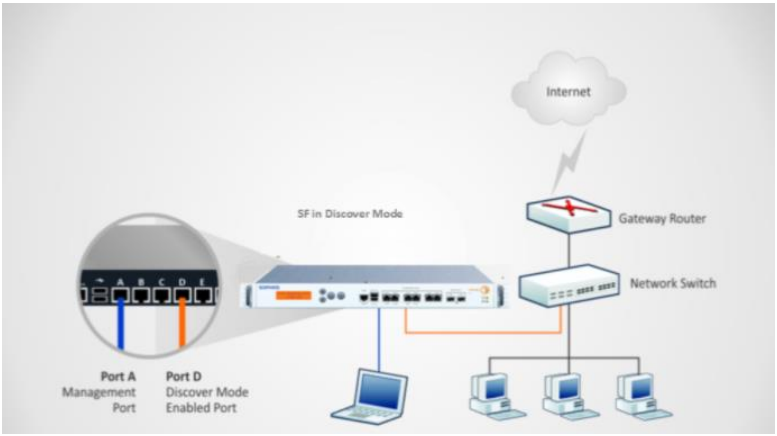


Рисунок 2.6. Розгортання фаєрволу в режимі виявлення (https://docs.sophos.com/mtr/networksensor)

Змішаний режим — це поєднання режиму моста та шлюзу, де кілька портів працюють у режимі мосту, а інші порти залишаються працювати в режимі маршрутизатора (або режимі шлюзу) [13].

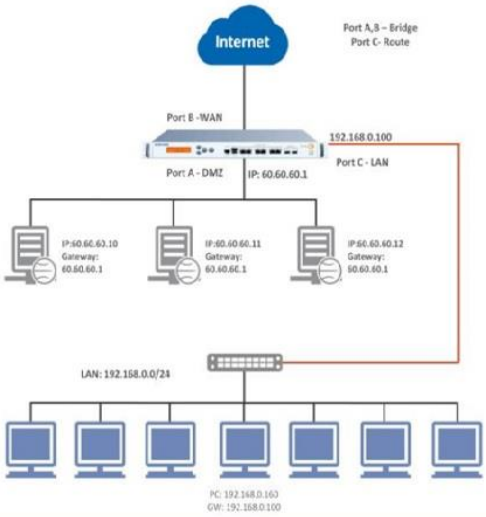


Рисунок 2.7. Розгортання фаєрволу в змішаному режимі (https://techbast.com/2016/07/sophos-deployment-mode.html)

Фаєрволи Sophos мають доволі високий рівень інтеграції з різними хмарними платформами, на маркетплейсах хмарних платформ «Microsoft Azure» та «Amazon Web Services» присутні шаблони для спрощення розгортання брандмауерів в VPC, для прикладу на рис 2.8 зображено варіант інтеграції двох фаєрволів у режимі «High Availability» в хмарі «Microsoft Azure».

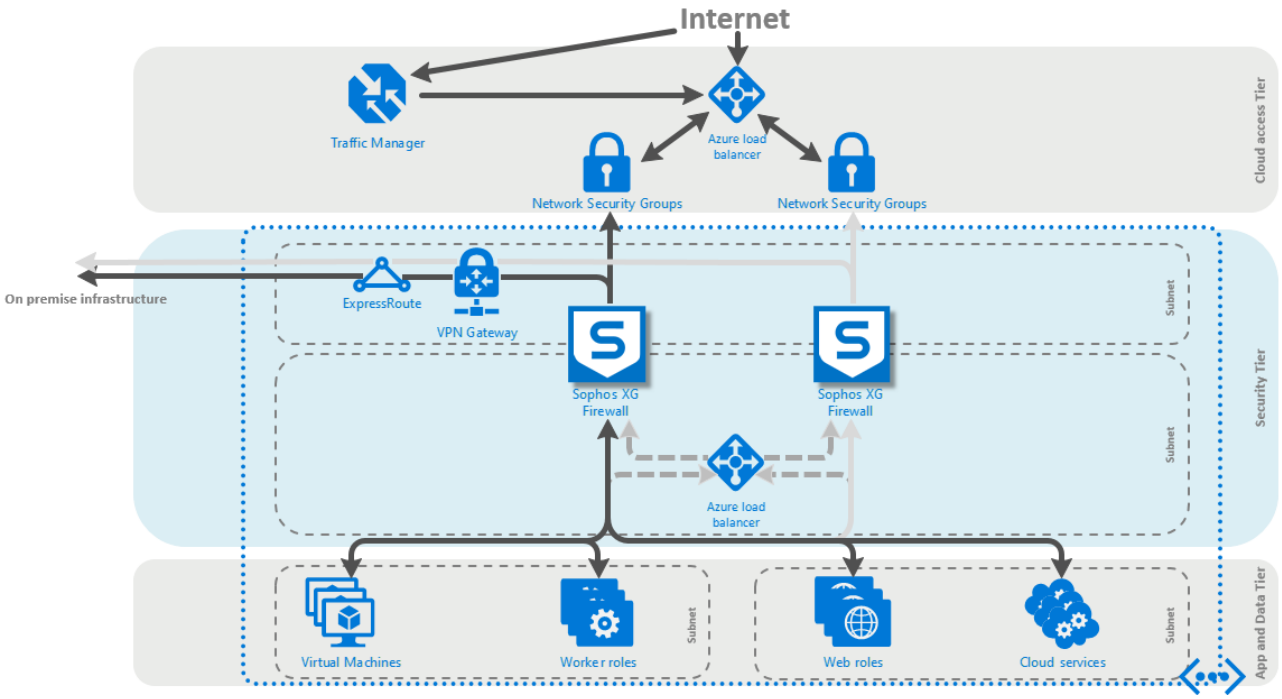


Рисунок 2.8. Варіант розгортання Sophos XGS на хмарній платформі (https://support.sophos.com/support/s/article/KB-000037098?language=en_US)

Брандмауер також має різні варіанти розгортання, це може бути повноцінний спеціалізований пристрій побудований на основі двохпроцесорної архітектури, хмарне рішення (є вбудовані можливості з інтеграцією хмарних ресурсів AWS та Microsoft Azure), віртуальна машина на будь-якій системі віртуалізації (VMware, Microsoft Hyper-V, Citrix, KVM) або є можливість встановлення фаєрволу апаратне забезпечення архітектури x86.

Варіант фаєрволу у вигляді спеціалізованого програмно-апаратного комплексу побудований на основі двохпроцесорної архітектури, де основний процесор – це стандартний чіп арітектури x86 від AMD, а співпроцесор «Xstream flow processor» – виготовлений на замовлення компанією Marvell, так званий NPU (Network Processor

Unit). Ідея використання Marvell NPU заключається в тому, що це майже CPU, котрий все ж розроблений під виконання мережевих задач і виготовляється спеціально під них [15]. Він, як і CPU складається з декількох ядер (в залежності від моделі, напр. в XGS-6500 – 24 ядра, 2,4GHz), кожне з яких відповідає за свій сегмент. NPU вигідно відрізняється від інших типів мережевих процесорів типу ASIC тим, що для зміни логіки достатньо переписати код. NPU займається майже всіма операціями пов'язаними з мережевою взаємодією, DPI, криптографією, IPS, веб-фільтрацією, TLS-інспектуванням, обробкою Control-Plane та Data-Plane в той час, як основний процесор виконує задачі управління, контролює Management-Plane, а також у випадку перегрузки системи може приймати на себе частину описаних вище операцій.

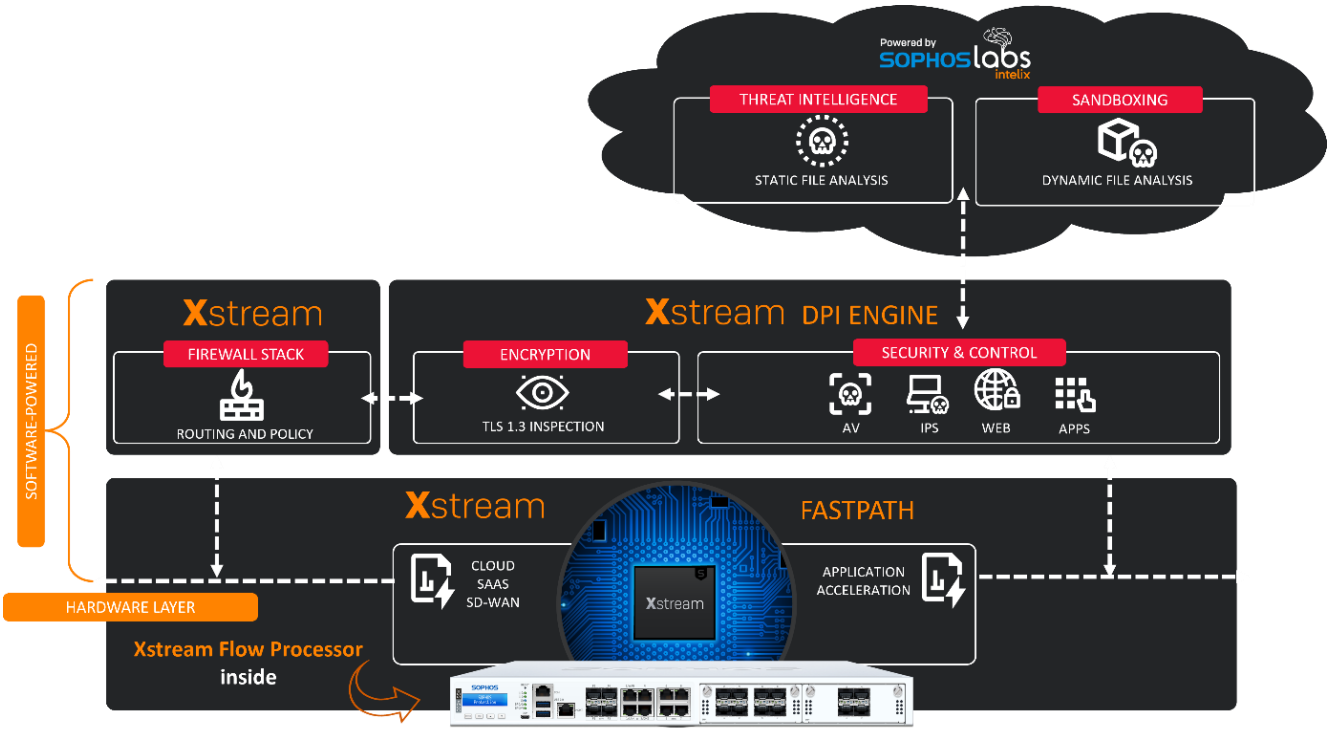


Рисунок 2.9. Схематичне зображення взаємодії співпроцесора [12]

2.2 Технології надання віддаленого доступу в Sophos XGS

Важливою частиною проектування сучасної системи управління доступом є вибір технології для підключення віддалених користувачів. Сьогодні фактичним лідером в цій сфері є технології VPN.

VPN (Virtual Private Network) – це узагальнена назва технологій, що дозволяють забезпечити одне або декілька мережевих з’єднань поверх іншої мережі, наприклад, Інтернету. Не дивлячись на те, що для комунікації використовуються мережі з малим рівнем довіри, рівень довіри до логічних мереж не залежить від цього завдяки використанню засобів криптографії (шифрування, автентифікації, інфраструктури відкритих ключів, засобів захисту від повторів і підміни повідомлень, що передаються).

VPN розширює приватну мережу через публічну мережу та дозволяє користувачам надсилати й отримувати дані через спільні чи загальнодоступні мережі так, якби їхні комп’ютери були підключені безпосередньо до приватної мережі. Переваги VPN включають збільшення функціональності, безпеки та керування приватною мережею. Він забезпечує доступ до ресурсів, недоступних у загальнодоступній мережі і зазвичай використовується для віддалених працівників. Шифрування є звичайним, хоча і не є невід’ємною частиною VPN-з’єднання.

Підключення віддаленого користувача до VPN здійснюється за допомогою сервера доступу, який підключений як до внутрішньої, так і зовнішньої (загальнодоступної) мережі, таким сервером може бути фаєрвол чи маршрутизатор, що стоїть на периметрі мережі. При підключенні віддаленого користувача (або під час встановлення з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

VPN створюється шляхом встановлення віртуального з’єднання «точка-точка» за допомогою виділених каналів або за допомогою протоколів тунелювання через існуючі мережі. Віртуальні приватні мережі можна розділити на віддалений доступ та «Site-to-site». Реалізація VPN у вигляді віддаленого доступу забезпечує доступ корпоративної мережі для віддалених користувачів. Конфігурація «Site-to-site» дозволяє з’єднувати дві або більше мережі, подібна конфігурація дозволяє розширити мережу географічно віддаленими офісами або групою офісів.

Фаєрволи Sophos XGS відрізняються від конкурентних рішень підтримкою досить великої кількості технологій VPN, таких, як IPsec, L2TP/IPsec, PPTP, SSL-VPN, проте на практиці все ж найчастіше застосовуються IPsec та SSL-VPN (OpenVPN), як такі, що мають найбільшу криптостійкість алгоритмів та продуктивність при роботі з великими навантаженнями, на рис. 2.10. зображено порівняння сучасних технологій VPN.

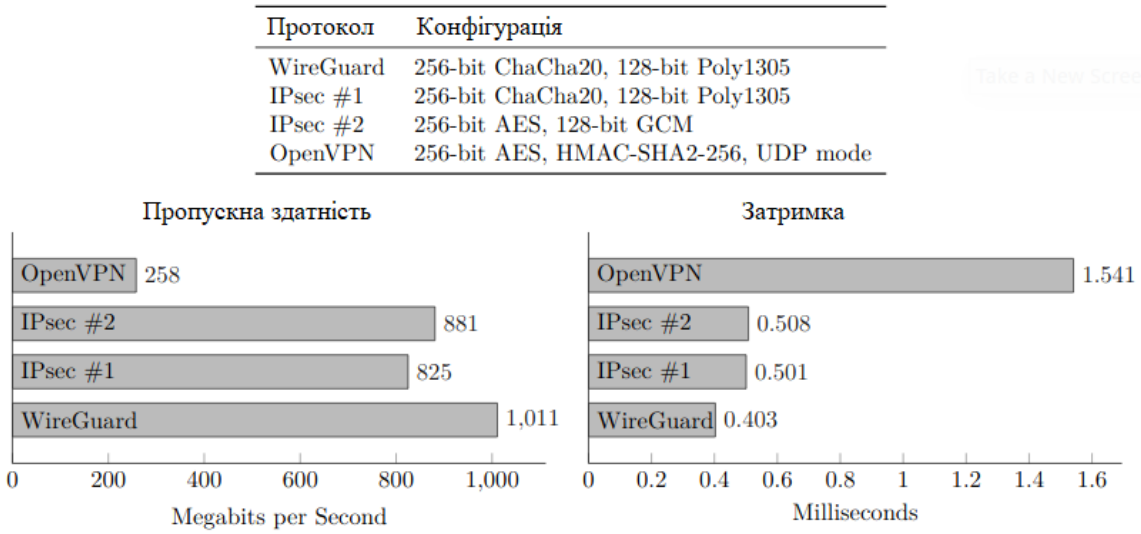


Рисунок 2.10. Порівняння сучасних технологій VPN (https://wittyjudge.github.io/posts/setup-wireguard-vpn/)

IPsec – це набір мережевих протоколів, що дозволяє виконувати автентифікацію та шифрування пакетів даних. IPsec включає протоколи для встановлення взаємної автентифікації між агентами на початку сеансу та узгодження криптографічних ключів для використання під час сеансу. IPsec може використовуватись для захисту потоків даних, як між хостами (організації віддаленого доступу) так і між парою шлюзів безпеки (для забезпечення безпечного з'єднання двох офісів) [16]. IPsec є відкритим стандартом і використовує наступні протоколи для виконання своїх задач:

- AH (Authentication Headers) – забезпечує цілісність даних без встановлення з'єднання та автентифікацію джерела даних для IP-дейтаграм і забезпечує від атак повторного відтворення;

- ESP (Encapsulating Security Payloads) – забезпечує конфіденційність, цілісність даних, автентифікацію даних і обмежену конфіденційність трафіку;
- ISAKMP (Internet Security Association and Key Management Protocol) – забезпечує структуру для автентифікації та обміну ключами шифрування. Його мета полягає в тому, щоб створити асоціації безпеки з пакетом алгоритмів і параметрів необхідних для операцій AH та ESP.

Протоколи IPsec AH та ESP можуть використовуватись транспортному (віддалений доступ) режимі та режимі тунелювання. У транспортному режимі шифрується та автентифікується зазвичай лише корисне навантаження IP-пакету. Маршрутизація в такому випадку залишається незмінна, оскільки IP-заголовок не модифікований і не зашифрований, однак, коли використовується AH, IP-адресу не можна змінити трансляцією мережевих адрес, оскільки це зробить значення хешу недійсним. Засоби для інкапсуляції пакетів IPsec для обходу NAT були визначені в RFC-3927 (NAT-T).

У режимі тунелювання весь IP-пакет шифрується та проходить автентифікацію. Потім він інкапсулюється в новий IP-пакет із новим IP-заголовком. Тунельний режим підтримує обхід NAT [17].

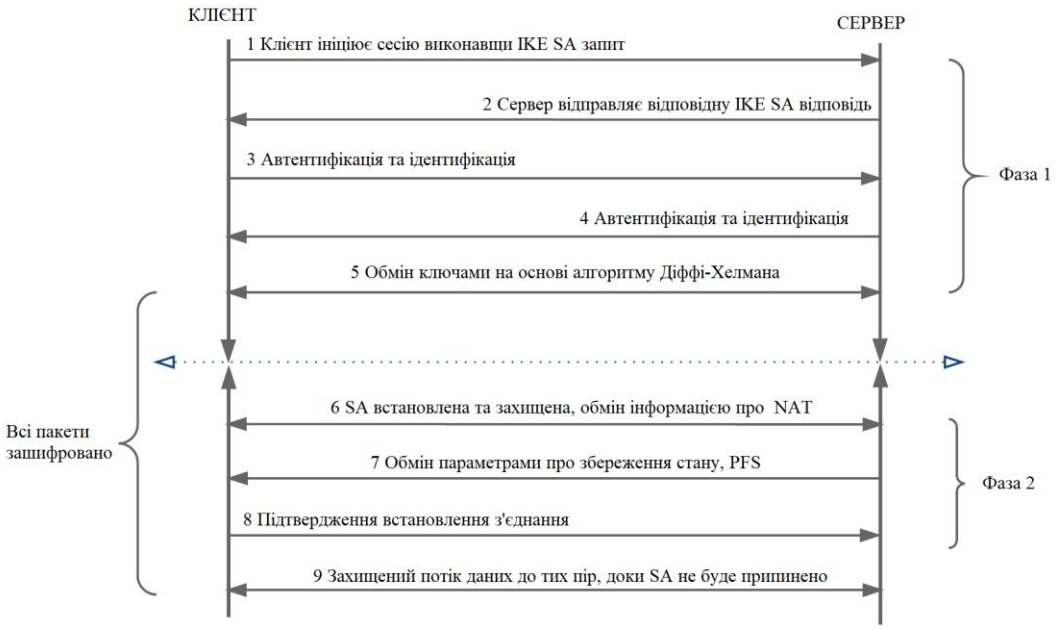


Рисунок 2.11. Процес встановлення з’єднання в IPsec

Таблиця 2.1.

Алгоритми, що використовуються в IPsec

Алгоритми шифрування	Алгоритми захищеного обміну ключами	Алгоритми автентифікації
HMAC-SHA1/SHA2	Diffie-Hellman	RSA
3DES-CBC	ECDH	ECDSA
AES-CBC/AES-CRT		PSK
AES-GCM		
ChaCha20-Poly1305		

До плюсів IPsec можна віднести:

- IPsec реалізовано в стеку IP всіх сучасних операційних систем, що дозволяє використовувати його для безпечного зв'язку без використання сторонніх програм;
- IPsec VPN має високі показники безпеки. Оскільки технологія працює на мережевому рівні, шифруються всі дані;
- Набір протоколів однаковий для всіх типів підключень.

До мінусів IPsec можна віднести:

- Низька комунікаційна продуктивність порівняно з іншими технолгіями;
- Наявність проблем пов'язаних з проходженням через NAT і міжмережеві екрани.

Загалом вендором Sophos рекомендовано використовувати IPsec для встановлення з'єднань між віддаленими локаціями типу «HQ-Branch» чи «Branch-Branch» або між офісом та VPC (Virtual Private Cloud), наприклад в Sophos XGS є інтеграція з AWS (Amazon Web Services), яка дозволяє побудувати тунель просто завантаживши в фаєрвол конфігураційний файл з консолі AWS. При налаштуванні IPsec слід пам'ятати, що ця технологія є дуже вимогливою до NAT, і при встановленні Sophos XGS не на периметрі мережі слід подбати про налаштування на прикордонному маршрутизаторі «One to one NAT» чи перенаправлення портів.

SSL-VPN – це технологія віддаленого доступу VPN на основі SSL/TLS. SSL-VPN дозволяє віддаленим користувачам встановлювати з'єднання з корпоративними ресурсами напряму з веб-браузера, що, як очікується має підвищувати продуктивність і доступність, а також зменшити IT-витрати на клієнтське програмне забезпечення. SSL-VPN може тунелювати трафік, як з усієї мережі, так і використовуватись для з'єднання віддалених працівників, в якості протокола транспортного рівня використовує TCP. Багато виробників мережевого обладнання включають в свої продукти різні реалізації SSL-VPN. Дана технологія може підключатись з місць де інші технології тунелювання будуть мати проблеми з трансляцією мережевих адрес і правилами брандмауера. Деякі реалізації SSL-VPN підтримують використання UDP в якості транспортного протоколу, в такому випадку за безпеку з'єднань відповідає протокол DTLS [18].

Для віддаленого доступу потрібні цифрові сертифікати, ім'я користувача та пароль. SSL-VPN в фаєрволах Sophos працює на базі відкритого стандарту OpenVPN. Це має ряд переваг у порівнянні з рішеннями конкурентів, наприклад, це дає змогу для досвідчених адміністраторів більш гнучко підлаштовувати параметри сервера під свої задачі, при цьому складність «базових» налаштувань залишається на такому рівні, що навіть молодший IT-спеціаліст з невеликим досвідом зможе протягом 10-15 хв. отримати робоче рішення.

OpenVPN широко використовує бібліотеку шифрування OpenSSL, а також протокол TLS і містить багато функцій контролю та безпеки, він використовує SSL/TLS для обміну ключами, здатний проходити транслятори мережевих адрес (NAT) і брандмауери. OpenVPN може працювати як по протоколу UDP так і по TCP, мультиплексуючи створені тунелі SSL на одному порту TCP/UDP.

OpenSSL – повноцінна криптографічна бібліотека з відкритим вихідним кодом, що підтримує всі низькорівневі алгоритми хешування, шифрування і електронно-цифрового підпису, а також реалізує більшість популярних криптографічних стандартів, в тому числі дозволяє створювати ключі RSA, DH, DSA, сертифікати X.509, підписувати їх, формувати CSR та CRT, шифрувати дані та тестувати SSL/TLS

з’єднання. Доступна у вигляді пакетів для UNIX-подібних операційних систем, ОС типу BSD а також для Microsoft Windows.

Компанія Sophos рекомендовандує використовувати в наступні параметри безпеки SSL-VPN: алгоритм шифрування – AES-256, алгоритм автентифікації – SHA2.

AES-256-CBC (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування з розміром блоку 256 біт заснований на алгоритмі Rijndael, має фіксований розмір вхідного блоку в 128 біт і розміром ключа 256 біт. AES базується на принципі розробки, відомому, як мережа заміни-перестановки і ефективний, як у програмному, так і в апаратному забезпеченні. Розмір ключа, який використовується для шифру AES, визначає кількість раундів перетворення, які перетворюють вхідні дані, які називають відкритим текстом, у кінцевий вихід, який називається зашифрованим текстом, для ключа розміром 256 біт кількість раундів 14. Кожен раунд складається з кількох етапів обробки, включаючи той, який залежить від самого ключа шифрування. Набір зворотних раундів застосовується для перетворення зашифрованого тексту назад у вихідний відкритий текст за допомогою того самого ключа шифрування.

SHA-2-512 (Secure Hash Algorithm Version 2) – криптографічний алгоритм однонаправленої хеш-функції призначений для створення «зліпків» чи «дайджестів» для повідомлень довільної довжини. Хеш-функція SHA-2 реалізована в деяких широко використовуваних програмах і протоколах безпеки, включаючи TLS і SSL, PGP, SSH, S/MIME та IPsec.

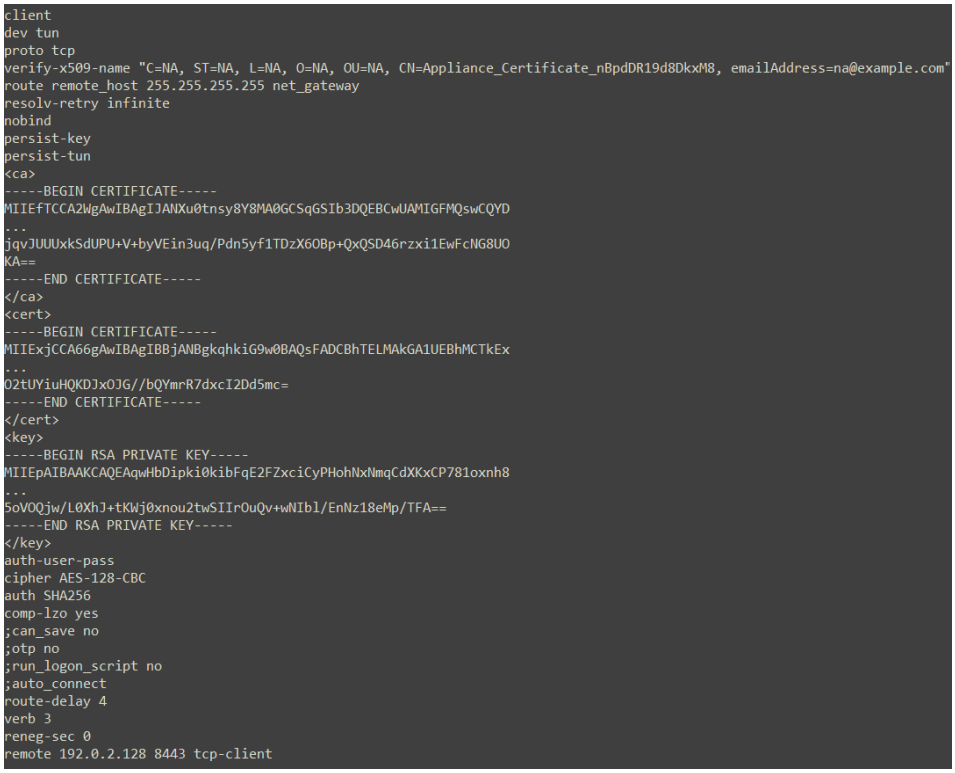
У процесі налаштування SSL-VPN для організації доступу до інформаційних ресурсів підприємства можна виділити наступні кроки:

- Постановка задачі да планування матриці доступу користувачів;
- Вибір параметрів сервера для підключення користувачів: транспортний протокол, криптографічні алгоритми шифрування та ін.;
- Створення чи актуалізація параметрів користувачів та груп користувачів;
- Створення правил підключень для окремих користувачів чи груп користувачів згідно визначеної раніше матриці доступу;
- Створення правил фаєрволу для доступу до відповідних ресурсів;

- Активація VPN на визначених інтерфейсах, за необхідності можна налаштувати обмеження джерел підключення по GeoIP;
- Встановлення спеціалізованого ПЗ на пристрої клієнта та доставка на нього параметрів підключення;
- Моніторинг та підтримка сервісу, підтримка актуальності схеми розподілення доступу та облікових записів користувачів.

При виборі параметрів сервера можна вибрати: транспортний протокол (TCP/UDP), порт (за замовчуванням 8443), SSL сертифікат для шифрування з'єднань, діапазон IPv4 чи IPv6 адрес з якого будуть призначатись адреси для користувачів, DNS-сервер, доменне ім'я та криптографічні параметри [19].

Для виконання з'єднання на клієнтському пристрої повинна бути встановлена відповідна програма, так званий VPN-клієнт. У якості такого клієнту можуть використовуватись додатки «Sophos SSL VPN Client» та «Sophos Connect», у такому випадку користувач може завантажити з клієнтського порталу додаток одразу налаштований під нього, що дає значне спрощення. Так як роботу «Sophos SSL-VPN» реалізовано на базі відкритого стандарту OpenVPN, то для виконання з'єднання можуть використовуватись й сторонні додатки, які підтримують цей стандарт, наприклад, «OpenVPN Connect». У такому випадку користувач може завантажити з порталу параметри клієнта у вигляді стандартизованого файлу формату «.ovpn».



```
client
dev tun
proto tcp
verify-x509-name "C=NA, ST=NA, L=NA, O=NA, OU=NA, CN=Appliance_Certificate_nBpdDR19d8DkxM8, emailAddress=na@example.com"
route remote_host 255.255.255.255 net_gateway
resolv-retry infinite
nobind
persist-key
persist-tun
<ca>
-----BEGIN CERTIFICATE-----
MIIEfTCCA2WgAwIBAgIJANXu0tnsy8Y8MA0GCSqGSIb3DQEBCwUAMIGFMQswCQYD
...
jqvJUUUxkSdUPU+V+byVEin3uq/Pdn5yf1TDzX6OBp+QxQSD46rzxi1EwFcNG8UO
KA==
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----
MIIExjCCA66gAwIBAgIBBjANBgkqhkiG9w0BAQsFADCBhTELMAkGA1UEBhMCTkEx
...
O2tUYiuHQKDJxOJG//bQYmrR7dxcI2Dd5mc=
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAqwHbDipki0kibFqE2FZxciCyPHohNxNmqCdXKxCP781oxnh8
...
5oVOQjw/L0XhJ+tKWj0xnou2twSIIrOuQv+wNIbl/EnNz18eMp/TFA==
-----END RSA PRIVATE KEY-----
</key>
auth-user-pass
cipher AES-128-CBC
auth SHA256
comp-lzo yes
;can_save no
;otp no
;run_logon_script no
;auto_connect
route-delay 4
verb 3
reneg-sec 0
remote 192.0.2.128 8443 tcp-client
```

Рисунок 2.12. Приклад конфігураційного файлу *.ovpn

Загалом виробником рекомендовано використовувати саме SSL-VPN для організації віддаленого доступу, так як дана технологія має наступні переваги: висока продуктивність, сучасні криптографічні алгоритми, не має проблем з проходженням через NAT.

Загалом слід додати, що VPN не може зробити з’єднання повністю анонімним, але він може підвищити конфіденційність і безпеку. Щоб запобігти розголошенню приватної інформації або перехопленню даних.

2.3. Можливості Sophos XGS щодо управління доступом

У розрізі надання та розподілення доступу до інформаційних ресурсів підприємства рішення на базі фаєрволів Sophos XGS вигідно відрізняються від конкурентів наявністю глибокої інтеграції з засобами захисту кінцевих точок (Security Heartbeat), наявність централізованої хмарної панелі керування та інтеграції з іншими рішеннями Sophos («Sophos Central»), підтримка великої кількості технологій надання віддаленого доступу: IPsec VPN, L2TP, PPTP, SSL-VPN, «Clientless access».

Окремо можна виділити технологію «Clientless access», що дозволяє надавати користувачам доступ до служб і ресурсів, а також спільний доступ до файлів за допомогою браузера, що допомагає спростити використання інформаційної системи для непідготованих користувачів. Щоб отримати безклієнтський доступ, користувачам не потрібно встановлювати VPN-клієнти, а просто зайти на клієнтський портал, ввести свої облікові дані та отримати доступ до необхідних ресурсів (RDP, VNC, файлові сховища xFTP/SMB та ін.). При цьому всі дії контролюються фаєрволом, це дозволяє створити єдине місце прийняття рішень про те, хто куди може мати доступ та у випадку виникнення критичних ситуацій спрощує пошук подій пов’язаних з інцидентом.

Однією з найбільш затребуваних функцій адміністраторів систем безпеки є можливість автоматичного реагування на інциденти безпеки в мережі. Фаєрволи Sophos можуть ідентифікувати джерело паразитного трафіку у мережі та автоматично обмежити доступ до інших мережних ресурсів у відповідь. Це стало можливим завдяки технології «Sophos Security Heartbeat», яка передає телеметрію та стан між кінцевими точками та міжмережевим екраном, таким чином відбувається інтеграція відомостей про працездатність підключених хостів у правила брандмауера, дозволяючи автоматично обмежувати доступ до конфіденційних мережевих ресурсів з будь-якої скомпрометованої системи, доки вона не буде очищена.

«Sophos Security Heartbeat» обмінюється відомостями в режимі реального часу, використовуючи безпечний зв'язок по https, між кінцевими точками і міжмережевим екраном. Цей метод синхронізації продуктів безпеки, які раніше працювали незалежно, створює ефективний захист від шкідливих програм та цільових атак.

«Security Heartbeat» може не тільки миттєво визначати наявність загроз, а і використовуватися для передачі важливої інформації про природу загрози, хост-систему та користувача і, можливо, найголовніше, «Security Heartbeat» також можна використовувати для автоматичного вжиття заходів щодо ізоляції або обмеження доступу скомпрометованої системи, доки вона не буде очищена.

«Security Heartbeat» працює на робочих місцях чи серверах. Heartbeat може бути в одному з трьох станів. Green Heartbeat статус вказує, що робоче місце справне і буде

дозволено доступ до всіх відповідних мережних ресурсів. Yellow Heartbeat статус вказує на попередження про те, що система може мати потенційно небажану програму (PUA), не відповідає вимогам або має будь-яку іншу проблему. Адміністратор може вибрати, до яких мережевих ресурсів дозволено звертатися системам із жовтим статусом, доки проблема не буде вирішена. Red Heartbeat статус вказує на систему, яка схильна до ризику зараження просунутими загрозами і може намагатися зв'язатися з ботнетом або сервером C&C. Використовуючи політики безпеки Heartbeat, можна легко ізолювати системи з цим статусом доти, доки вони не будуть очищені, щоб зменшити ризик втрати даних або подальшого зараження.

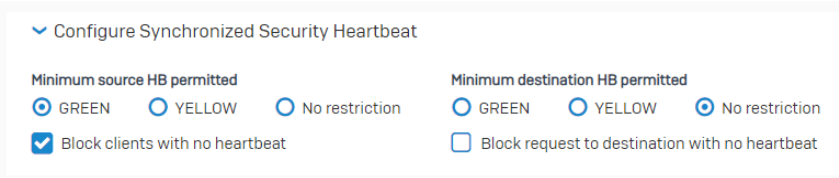


Рисунок 2.13. Приклад налаштування Security Heartbeat в політиці безпеки

Важливо зазначити, що найважливішим етапом створення доступу до корпоративних інформаційних ресурсів на базі будь-якого рішення є створення та підтримка актуальності матриці доступу користувачів. Це абстрактна, формальна модель безпеки, що характеризує права кожного суб’єкта (користувача чи групи користувачів) по відношенню до кожного об’єкту в інформаційній системі. У випадку надання доступу матриця повинна містити обліковий запис користувача, параметри цільової системи (IP-адреса чи FQDN), сервіс (HTTPS, SMB, RDP, TCP/3654 та ін.), параметри, яким повинна відповідати система користувача (HeartBeat Green/Yellow), час коли користувач може мати доступ. При розподіленні доступу важливо керуватись принципом «нульової довіри», коли користувачеві системи дається рівно стільки прав та привілей, скільки йому потрібно для виконання своїх службових задач, у такому випадку адміністраторові системи важливо розуміти хто чим займається і при опрацюванні системи розподілення доступу взаємодіяти з відділом кадрів та керівниками структурних підрозділів підприємства. Правильно складена матриця доступу актуальність якої постійно підтримуються дозволяє значно зменшити площу

атаки у випадку компрометації облікового запису. Дуже гарною практикою є, коли подібна таблиця існує не тільки «в голові» у адміністратора, а й є у вигляді формалізованого документу чи Excel-таблиці.

2.4. Можливості, функції та призначення «Sophos Central»

Для забезпечення більшої ефективності засобів інформаційної безпеки велику роль грає зв'язок її компонентів, він дозволяє перекрити, як зовнішні, так і внутрішні загрози. При проектуванні інфраструктури важливе значення має кожен засіб захисту і дуже важливо, щоб вони функціонували не тільки в рамках свого класу, а і мали можливість взаємодіяти між собою для спільної боротьби з загрозами.

Новий підхід до забезпечення кібербезпеки передбачає захист кожного рівня, в якому рішення, що використовуються на кожному з рівнів пов’язані одне з одним і мають можливість обмінюватись інформацією. Це призвело до створення системи Synchronized Security (SynSec). SynSec є процесом забезпечення інформаційної безпеки, як єдиної системи. У цьому випадку кожен компонент забезпечення інформаційної безпеки з'єднано один з одним у реальному часі, наприклад, рішення «Sophos Central» реалізовано за цим принципом. Технологія Security Heartbeat забезпечує зв'язок між компонентами безпеки, забезпечуючи спільне функціонування системи та її моніторинг. У «Sophos Central» інтегровані такі рішення: «Endpoin Protection» – класичний сигнатурний антивірус; «Server Protection» – спеціалізований антивірус для серверів; «Intercept-X» – антивірус нового покоління; «Data Protection» – засіб централізованого керування шифруванням даних; XGS Firewall – NGFW; «Mobility Management» – керування мобільними пристроями та контроль доступу до корпоративної пошти та файлів; «Web Security» – рішення для фільтрації веб-трафіку; «E-MAIL Security» – хмарне чи локальне антиспам/антивірус рішення; «Phish Threat» – рішення призначене для підвищення обізнаності співробітників, проведення тестових фішингових розсилок; «Cloud Optix» – аудит хмарних інфраструктур. Нескладно помітити, що «Sophos Central» підтримує досить широкий спектр рішень,

щодо інформаційної безпеки. У «Sophos Central» концепція SynSec базується на трьох важливих принципах: виявлення, аналіз та реагування.

Виявлення – продукти Sophos під керуванням «Sophos Central» в автоматичному режимі діляться інформацією між собою для виявлення ризиків та невідомих загроз, що включає: аналіз мережевого трафіку з можливістю ідентифікувати додатки з високим ризиком та шкідливий трафік; виявлення користувачів із групи ризику шляхом кореляційного аналізу їхніх дій у мережі.

Аналіз інцидентів в реальному часі забезпечує миттєве розуміння поточної ситуації у системі. Відображення повного ланцюжка подій, які призвели до інциденту, включаючи всі файли, ключі реєстру, URL-адреси і т.д.

Реагування – налаштування політик безпеки дозволяє автоматично за лічені секунди реагувати на зараження та інциденти. Це забезпечується: миттєвою ізоляцією заражених пристроїв та зупинкою атаки в режимі реального часу (навіть у межах однієї мережі/широкомовного домену); обмеження доступу до мережевих ресурсів компанії для пристроїв, які не відповідають політикам; віддалений запуск сканування пристрою при виявленні вихідного спаму.

Отже, «Sophos Central» — це єдине хмарне рішення для керування всіма технологіями наступного покоління. Завдяки уніфікованій консолі керування, обміну інформацією в режимі реального часу між продуктами та автоматичному реагуванню на інциденти «Sophos Central» робить процес забезпечення кібербезпеки простішим та ефективнішим [20], на рис. 2.14. зображено панель керування «Sophos Central».

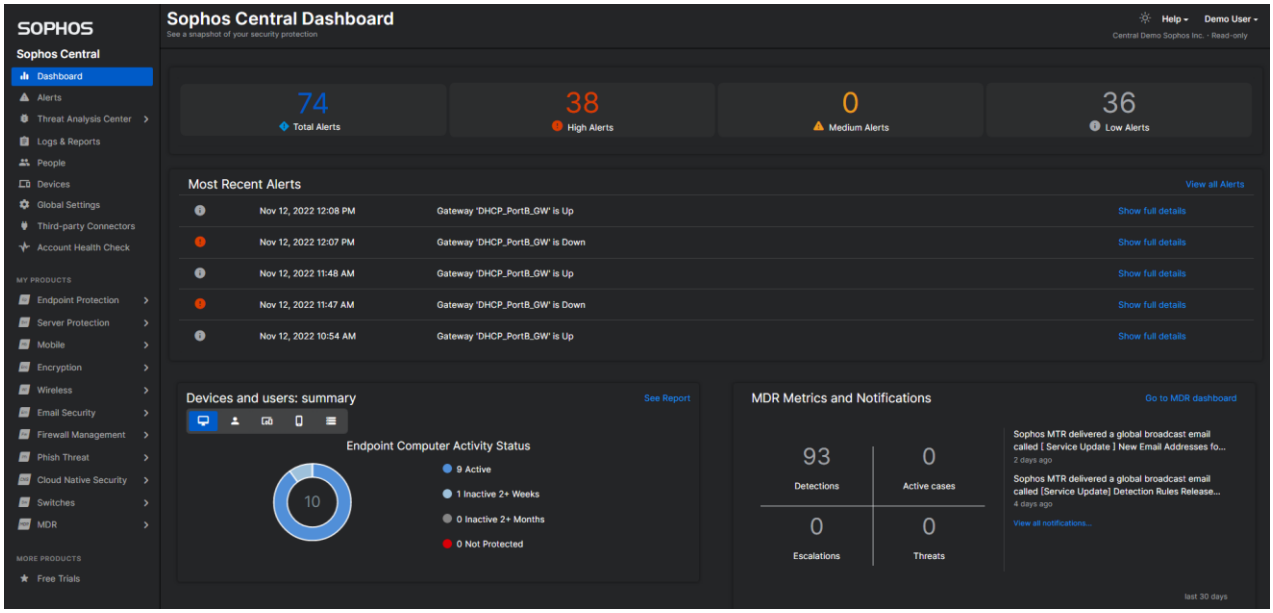


Рисунок 2.14. Панель сповіщень Sophos Central

На панелі керування відображаються останні повідомлення. Також у вигляді діаграм відображена зведена характеристика різних компонентів захисту. У цьому випадку відображаються дані щодо захисту персональних комп'ютерів. На цій панелі також є зведена інформація про спроби відвідування небезпечних ресурсів і ресурсів з неприйнятним змістом, статистика аналізу електронної пошти. «Sophos Central» підтримує відображення повідомлень за ступенем важливості, що не дозволить адміністратору пропустити критичні оповіщення системи безпеки. Крім лаконічно відображуваної зведеної інформації про стан системи захисту, «Sophos Central» підтримує логування подій, інтеграцію із SIEM-системами. Даний ресурс для багатьох компаній є платформою як внутрішнього SOC, так і надання послуг своїм замовникам — MSSP.

Важливим елементом в наш час є рішення «Sophos Cloud Optix», що є платформою безпеки, відповідності вимогам безпеки, інвентаризації та моніторингу публічних хмарних платформ. Вона забезпечує інвентаризацію серверів, сховищ та мережевих елементів в хмарі в режимі реального часу. Допомагає керувати ресурсами, контролювати безпеку та дотримуватися стандартів безпеки в одному простому інтерфейсі. Також, у поєднанні з «Intercept X for Server» забезпечує покращений

захист хмарних робочих навантажень та більш ефективне керування агентами безпеки.

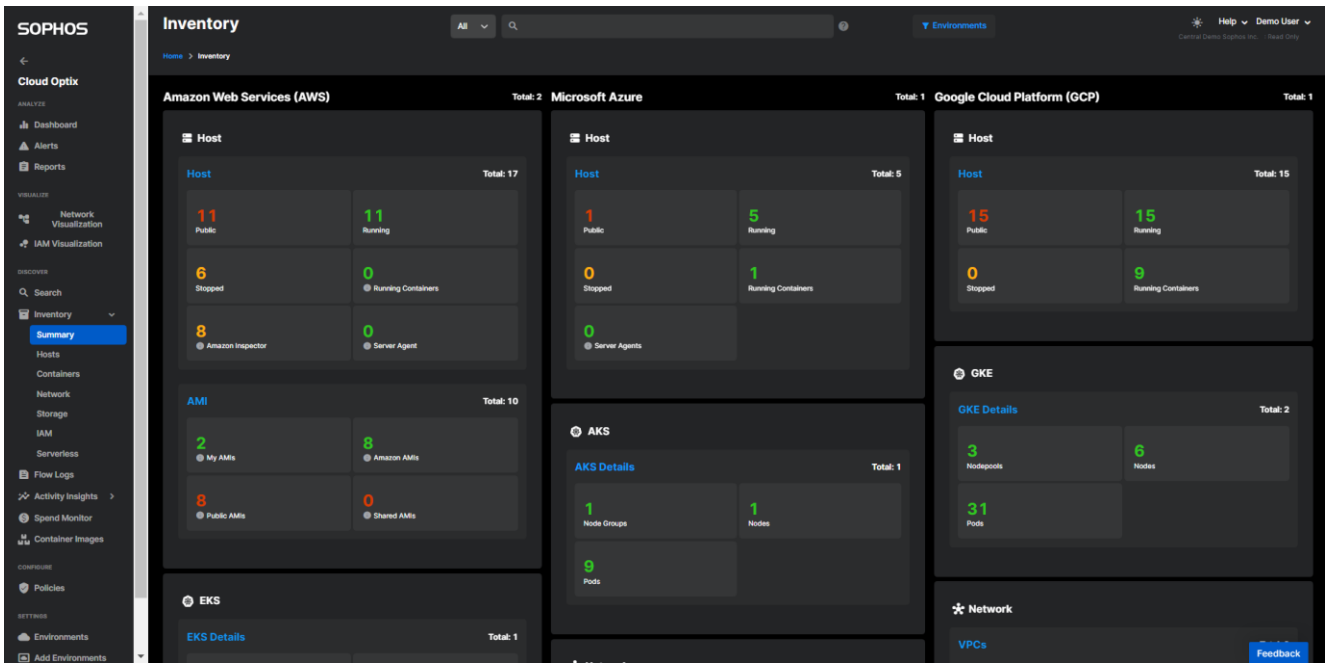


Рисунок 2.15. Панель керування «Sophos Cloud Optix» в «Sophos Cenral»

Одним із компонентів endpoint-захисту є антивірус нового покоління (NGAV) - Intercept X. За допомогою технологій глибокого машинного навчання антивірус здатний виявляти раніше невідомі загрози без використання сигнатур. Точність виявлення можна порівняти з сигнатурними аналогами, але на відміну від них забезпечує проактивний захист, запобігаючи атакам «нульового дня». Intercept X здатний працювати паралельно із сигнатурними антивірусами інших вендорів.

2.5. Можливості, функції та призначення «Sophos Intercept X Endpoint»

Рішення безпеки кінцевих точок (антивіруси), можуть включати різноманітні базові (традиційні) і сучасні (нового покоління) підходи до запобігання загрозам кінцевих точок. Оцінюючи ринок, важливо шукати рішення, які містять комплексний набір методів для протидії широкому спектру загроз. Також важливо розуміти загрози, яким ви намагаєтеся запобігти. Хоча ландшафт загроз постійно змінюється, є

ряд деякі ключові загрози для кінцевих точок, які слід враховувати при виборі рішень: портативні виконувані файли (Malware), потенційно небажані програми (PUA), програми-вимагачі (Ransomware), атаки на основі експлойтів.

Хоча вони можуть мати різні назви, антивірусні рішення існують уже деякий час і виявилися дуже ефективними проти відомих загроз, одним з таких рішень, яке дозволяє вирішувати описані вище проблеми є «Sophos Intercept X», спеціалізоване ПЗ для виявлення шкідливих та небажаних програм, відновлення заражених (модифікованих) такими програмами файлів і профілактики попередження компрометації (зараження чи модифікації) файлів або операційної системи в цілому.

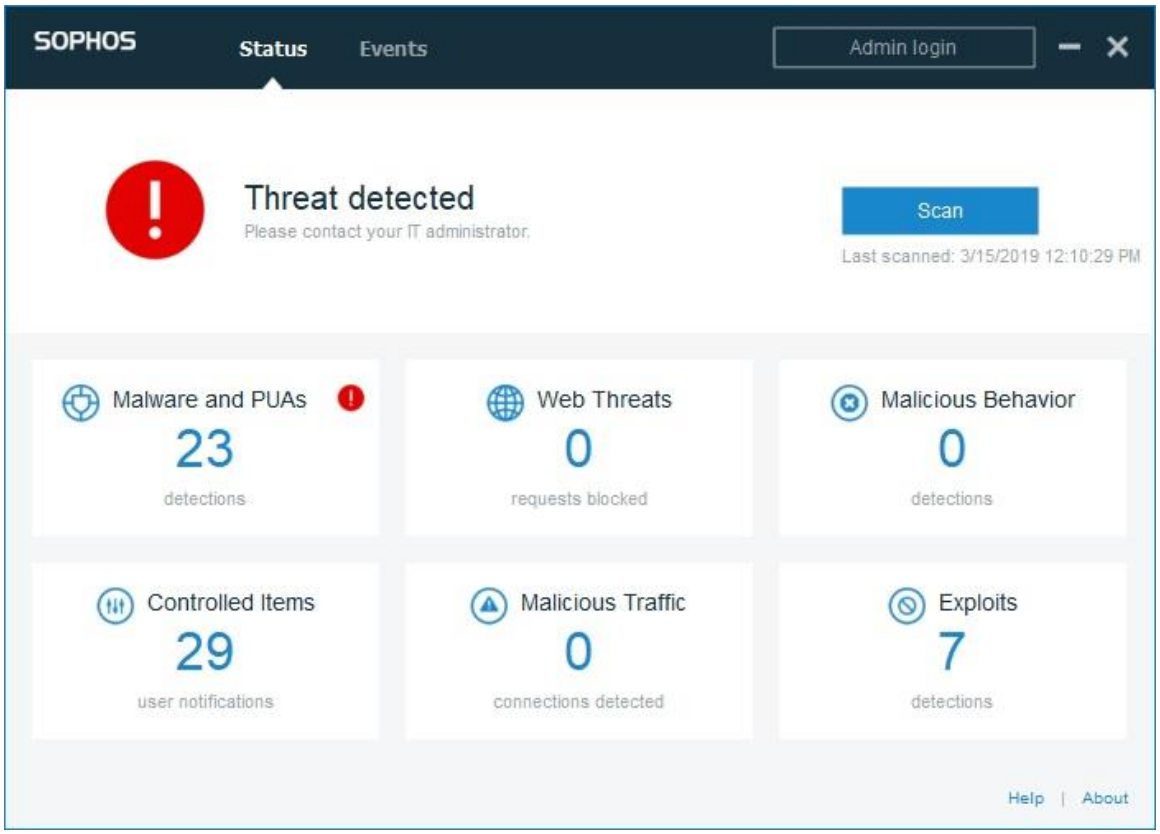


Рисунок 2.16. Центральна панель «Sophos Intercept X» сигналізує про виявлення шкідливого ПЗ на ПК

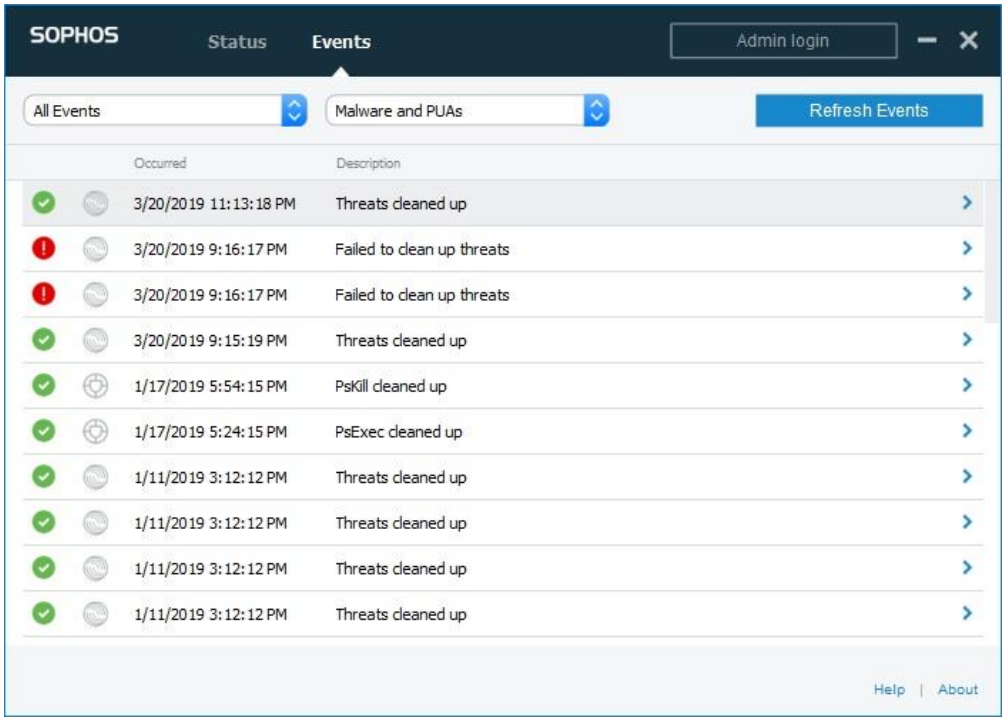


Рисунок 2.17. Панель надання звітів та журналів «Sophos Intercept X»

Існує безліч базових методів, на які спираються традиційні рішення для захисту кінцевих точок. Однак у міру того як ландшафт загроз змінився, невідомі загрози, такі як зловмисне програмне забезпечення, яке ніколи не було раніше, стають все більш поширеними. Через це на ринок вийшли нові технології. В «Sophos Intercept X» реалізовано поєднання як сучасних підходів (Next-Gen), так і перевірених базових підходів. Нижче перераховано можливості, які можна віднести до базового функціоналу рішення. Anti-malware/antivirus: Виявлення відомих шкідливих програм на основі сигнатур. Механізми зловмисного програмного забезпечення повинні мати можливість перевіряти не лише виконувані файли, але й інший код, наприклад шкідливий JavaScript, знайдений на веб-сайтах. Application lockdown: Запобігання зловмисній поведінці додатків, як-от заражений документ Office, який встановлює іншу програму та запускає її. Поведінковий моніторинг/Системи запобігання вторгнень (HIPS): Ця базова технологія захищає комп'ютери від невідомих вірусів і підозрілої поведінки. Вона повинна включати аналіз поведінки як перед виконанням, так і під час виконання. Веб-захист: пошук URL-адрес і блокування відомих шкідливих веб-сайтів. Заблоковані сайти мають включати ті, які можуть запускати

JavaScript для виконання криптомайнінгу, а також сайти, які збирають облікові дані користувача та інші конфіденційні дані. Веб-контроль: веб-фільтрація кінцевої точки дозволяє адміністраторам визначати, які типи файлів користувач може завантажувати з Інтернету. Запобігання втраті даних (DLP): якщо зловмисник може залишитися непоміченим, можливості DLP зможуть виявити та запобігти останній стадії деяких атак, коли зловмисник намагається викрасти дані. Це досягається шляхом моніторингу різних типів конфіденційних даних.

До функцій наступного покоління можна віднести можливості перераховані нижче. Машинне навчання, існує кілька типів методів машинного навчання, зокрема нейронні мережі глибокого навчання, «випадковий ліс», байєсівський метод і кластеризація. Незалежно від методології, механізми машинного навчання виявлення зловмисного програмного забезпечення повинні бути створені для виявлення як відомого, так і невідомого зловмисного програмного забезпечення, не покладаючись на сигнатури. Перевага машинного навчання полягає в тому, що воно може виявляти зловмисне програмне забезпечення, яке ніколи не було помічено раніше, в ідеалі підвищуючи загальний рівень виявлення зловмисного програмного забезпечення. Організації повинні оцінити рівень виявлення, рівень хибних спрацьовувань і вплив рішень на основі машинного навчання на продуктивність. Anti-Exploit – технологія захисту розроблена для запобігання зловмисникам шляхом блокування інструментів і методів, на які вони покладаються в ланцюжку атак. Наприклад, такі експлойти, як EternalBlue і DoublePulsar, використовувалися для запуску програм-вимагачів NotPetya і WannaCry. Технологія захисту від експлойтів зупиняє відносно невелику колекцію методів, які використовуються для розповсюдження зловмисного програмного забезпечення та проведення атак, захищаючи від багатьох атак нульового дня, не бачивши їх раніше. Рішення для захисту від шифрувальників (Ransomware-Specific) містять методи, спеціально розроблені для запобігання зловмисному шифруванню даних програмами-вимагачами. Часто спеціальні методи програм-вимагачів також виправляють усі пошкоджені файли. Рішення для програм-вимагачів мають зупиняти не лише програми-вимагачі для файлів, але й програми-вимагачі для дисків, які використовуються в деструктивних атаках очисників, які втручаються в

MBR. Endpoint detection and response (EDR): рішення EDR повинні мати можливість надавати детальну інформацію під час виявлення загроз, підтримки гігієни операцій IT-безпеки та аналізу виявлених інцидентів. Extended detection and response (XDR) виходить за межі кінцевої точки та сервера, включаючи інші джерела даних, такі як брандмауер, електронна пошта, хмара та мобільні пристрої. Його розроблено, щоб надати організаціям цілісне уявлення про все середовище з можливістю деталізації, де це необхідно. Уся ця інформація має бути зіставлена в централізованому місці, зазвичай відомому як озеро даних, де користувач може ставити та відповідати на важливі для бізнесу запитання. Також в рішенні «Intercept X» реалізовано функціонал захисту від викрадення облікових даних, захист від підвищення привілегій, автоматичне реагування на інциденти, MTR [21].

Згідно висновку Gartner рішення «Sophos Intercept X» є лідером серед платформ захисту кінцевих точок у дванадцятому звіті поспіль.

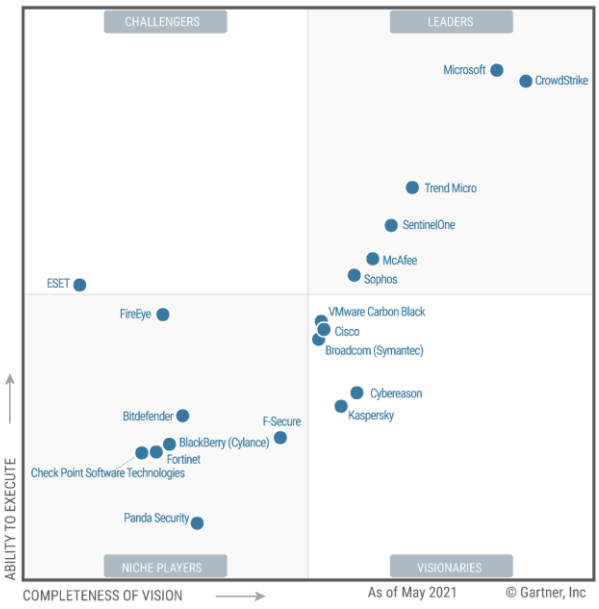


Рисунок 2.18. Звіт Gartner від травня 2021 року щодо аналізу ринку платформ захисту кінцевих точок (https://cutt.ly/U1OauLx)

Рішення доступне для встановлення на всі сучасні десктопні (Windows, MacOS, GNU/Linux) та мобільні (iOS, Android) операційні системи. Також, великою перевагою над рішеннями конкурентів є наявність централізованого керування та повна

інтеграція з усіма рішеннями Sophos реалізована через хмарну платформу «Sophos Central».

2.6. Адміністрування фаєрволів Sophos XGS

Важливим критерієм при виборі будь-якої IT-системи є методи управління нею, простота та зручність управління, можливості щодо резервування каналів управління та методи створення резервних копій конфігурації. В Sophos XGS можна виділити три основних методи управління: це веб-інтерфейс, консоль (CLI) та централізоване управління і оркестрація фаєрволів через хмарну платформу «Sophos Central».

Операційна система SFOS використовує простий у використанні графічний інтерфейс на основі WEB-2.0, який називається консоллю веб-адміністратора, для налаштування пристрою та керування ним. Адміністратор може отримати доступ до адміністрування пристрою зайшовши на нього з веб-браузера протоколом HTTPS по порту TCP/4444 (наприклад, https://172.16.16.16:4444/). Фаєрволи Sophos вигідно відрізняються від конкурентів тим, що 99% їхнього функціоналу доступно для налаштування через веб-інтерфейс, що значно спрощує первинне знайомство з системою та керування нею. Важливо пам'ятати, що фаєрволи Sophos одразу застосовують та зберігають всі зміни, тому важливо з особливою увагою відноситись до будь-якої зміни конфігурації.

CLI (Command Line Interface) – різновид текстового інтерфейсу між людиною та комп’ютерним пристроєм, в якому інструкції для пристрою даються методом вводу з клавіатури текстових рядків (команд). Консоль CLI надає набір інструментів для адміністрування, моніторингу та керування певними компонентами пристрою. До неї можна отримати доступ через протокол SSH, звичайним консольним з’єднанням через інтерфейс rs232, також більшість фаєрволів Sophos обладнані інтерфейсами HDMI або VGA до яких можна підключити монітор й керувати пристроєм безпосередньо з місця, даний метод управління є дещо застарілим та незручним, оскільки потребує перебування адміністратора безпосередньо біля пристрою, але іноді використовується при вирішенні проблем пов’язаних з невдалим оновленням або критичною помилкою

на пристрої. Значно частіше використовується текстовий метод управління через протокол SSH, з його допомогою можна виконувати деякі задачі пов’язані з автоматизацією, внесенням базової конфігурації, аналізом мережевого трафіку при встановленні помилок в мережі.

Два попередні методи добре справляються зі своїми задачами, але якщо мова йде про адміністрування не одного а декількох фаєрволів чи про інтеграцію з іншим рішенням Sophos кращим варіантом буде виконувати адміністративні функції з хмарної консолі керування «Sophos Central». Вона надає простий та зрозумілий інтерфейс управління уніфікований зі стандартною веб-консоллю, надає функціонал моніторингу пристрою чи групи пристроїв, надання діагностичних та статистичних даних, сповіщення адміністртора по електронній пошті про помилки чи інциденти в мережі; надає додатковий функціонал пов’язаний зі створенням резервних копій конфігурації та управління доступом кількох адміністраторів. Також завдяки повній інтеграції з іншими продуктами Sophos, можливості інтеграції з Microsoft AD та централізованому збору журналів та статистичної інформації, «Sophos Central» значно спрощує процес розслідування кібер-інцидентів.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ ФАЄРВОЛІВ SOPHOS XGS

3.1. Розроблення варіанта топології мережі підприємства та методів надання доступу до неї на базі Sophos XGS

Постановка задачі: обрати та реалізувати технологію об’єднання локальної мережі підприємства та віддаленого серверного сегменту розташованого в хмарному ресурсі AWS, організувати розподілення доступу користувачів до мережевих ресурсів відповідно до їх посадових задач, обрати та реалізувати технологію надання захищеного віддаленого доступу співробітників до мережевих ресурсів підприємства. Кількість співробітників – 50; відділи: IT, SEO, sales, management; перелік інформаційних ресурсів: Active Directory, crm.example.local, wp.example.com, file.example.local; адреса користувацького сегменту мережі – 172.16.16.0/24, адреса локального серверного сегменту мережі – 172.18.0.0/24, адреса хмарного сегменту мережі – 172.30.0.0/24.

При розробці архітектури рішення для надання доступу до інформаційної системи слід враховувати ряд вимог пов’язаних з простотою управління, надійністю та відмовостійкістю системи, посиленню безпеки з можливим використанням сторонніх рішень цього вендору, можливістю інтеграції з рішеннями сторонніх виробників, гнучкістю та здатністю рішення до масштабування. Важливо розуміти, що проблема надання доступу сьогодні означає не тільки безпечний доступ для віддалених користувачів через мережу Інтернет, а й для користувачів, що знаходяться на місцях.

На рис. 3.1 зображено спрощену топологію мережі підприємства на прикладі якого потрібно впровадити технологію управління доступом до інформаційних ресурсів на базі фаєрволу Sophos XGS. Серед основних моментів варто виділити розділення локальної мережі на декілька сегментів, на цьому прикладі це користувацький сегмент, в який включаються комп’ютери локальних користувачів (мережа 172.16.16.0/24) та серверний сегмент мережі, в який включені серверні ресурси компанії. Серед них варто окремо виділити сервер Active Directory, який виконує задачі не тільки контролера домену, а й AAA-сервера та проводить авторизацію користувачів.

Досліджувана мережа має серверний сегмент розташований в хмарі (VPC – Virtual Private Cloud) AWS, фаєрволи Sophos мають вбудований механізм інтеграції з хмарними платформами Amazon, що дозволяє дуже просто об’єднувати VPC з локальною мережею, дана технологія працює на основі протоколу IPsec. Така схема з’єднання дозволяє сконцентрувати всі інформаційні потоки в одному місці та створити єдину точку входу в мережу, яку буде зручно контролювати та на якій можна зручно розмежовувати доступ за допомогою політик безпеки та правил міжмережевого екранування на фаєрволі Sophos XGS.

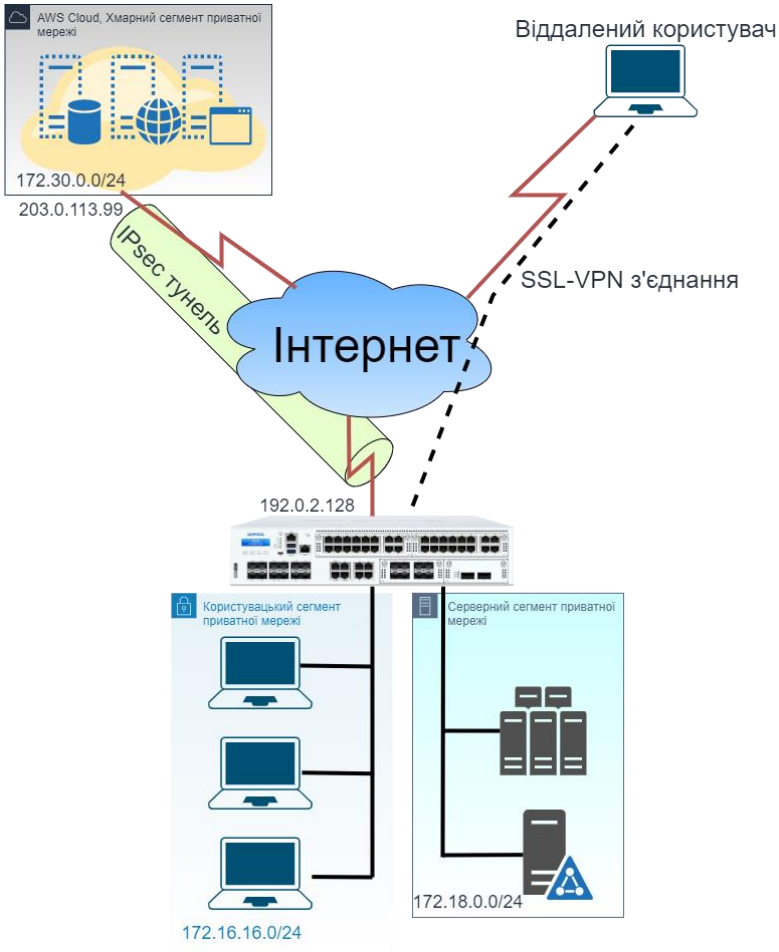


Рисунок 3.1. Варіант топології інформаційної системи підприємства

Що стосується доступу користувачів до інформаційних ресурсів, його краще всього реалізувати за допомогою технології SSL-VPN та термінувати всі з’єднання на центральному фаєрволі. Найкращим варіантом тут буде за допомогою групових правил домену Windows розповсюдити на всі ПК VPN-клієнти у вигляді програмного забезпечення «Sophos SSL VPN Connect» разом з необхідною конфігурацією та додати

дане ПЗ та процес запуску з’єднання в автостарт. Подібний варіант конфігурації спрощує експлуатацію інформаційної системи та робить систему в цілому прозорою для клієнта. В такому варіанті на клієнтському пристрої завжди запускається VPN з’єднання, навіть коли він знаходиться в локальній мережі, що може значно вплинути на навантаженість зовнішнього інтерфейсу. Для запообігання цій проблемі варто в налаштуваннях серверу вказати доменне ім'я і виконувати з'єднання за ним, тоді при правильній конфігурації клієнт підключаючись з локальної мережі отримає від DNS-сервера не зовнішню «білу» адресу шлюза (на прикладі це 192.0.2.128), а «сіру» адресу внутрішнього IP-інтерфейсу (наприклад, 172.16.16.16) та виконає з’єднання з нею.

В якості додаткового методу безпеки варто розглянути використання технології «Synchronized Heartbeat» та інтеграцію в систему надання доступу антивірусного ПЗ «Sophos Intercept X». При подібному підході клієнтський пристрій при встановленому з’єднанні виконуючи запит на доступ до певного ресурсу повинен пройти перевірку на відповідність корпоративним вимогам безпеки. Тобто антивірус повинен надати фаєрволу дані телеметрії. Процес встановлення з’єднання зображено на рис 3.2.

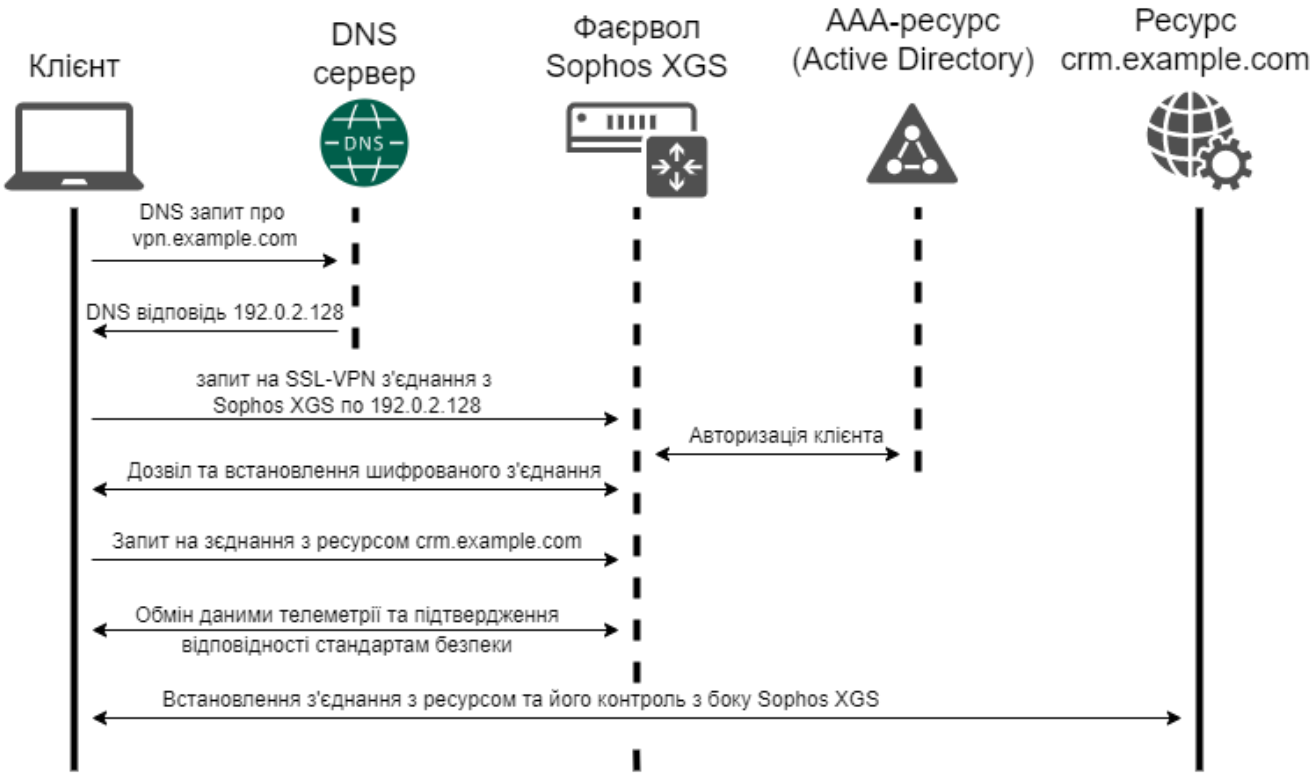


Рисунок 3.2. Процес встановлення з’єднання

Для розподілення доступу потрібно сформувати матрицю доступу, її частину наведено в табл. 3.1.

Таблиця 3.1

Приклад матриці доступу

ПІБ користувача	Обліковий запис	Група	Цільова система	Сервіс	Час
Береза Віталій	v.bereza	IT	172.18.0.0/24	SSH	необмежено
			172.16.16.16	TCP/4444	
Іван Комаров	i.komarov	Sales	crm.example.local	HTTPS	ПН. 8:30 – ПТ. 21:00
			file.example.local	SMB	
Юлія Андрєєва	j.andreeva	SEO	wp.exaple.local	HTTPS	8:00 – 18:00

Для прикладу в «Додатку А» зображено скріншот з правилом фаєрволу для першого рядка матриці доступу таблиці 3.1. Серед ключових аспектів даної політики слід зазначити наступне: назва політики стисло відображає її суть; встановлено опцію «Log firewall traffic», у такому випадку ведеться облік усіх сесій, що підпадають під цю політику, а не лише тих, що є небажаними, це забезпечує повну видимість системи та спрощує пошук можливих помилок; у політиці використовується прив’язка не лише за IP-адресами джерела та призначення, а й за обліковими записами користувачів, додатково можна вибрати опцію «Use web authentication» для того, щоб можна було автентифікувати нерозпізнаних користувачів за допомогою механізму «Captive portal»; у розділі «Synchronized Heartbeat» параметр «Minimum source HB permitted» встановлено на зелений, тобто, доступ буде дозволено лише кінцевим станціям, які відповідають вимогам безпеки; вибрана опція «Block clients with no heartbeat», що відповідає за те, що до політики допускаються лише ті пристрої, на яких встановлено антивірусне ПЗ і які обмінюються з фаєрволом даними телеметрії; застосована прив’язка до IPS, тобто, усі сесії, що будуть проходити через цю політику

будуть додатково передані механізму IPS для перевірки, вбудований набір правил включає велику базу індикаторів, що постійно оновлюється.

В табл 3.2. наведено параметри криптографії для SSL-VPN

Таблиця 3.2.

Параметри сервера SSL-VPN

Назва	Параметр
Алгоритм шифрування	AES-256-CBC
Алгоритм автентифікації	SHA-2-512
Розмір ключа	2048 біт
Час життя ключа	28 800 секунд

3.2. Розроблення рекомендацій щодо застосування технології управління доступом до мережі та управління фаєрволами

Управління доступом до інформаційної системи є доволі складною задачею, що має багато «підводних каменів». Не існує єдиного правильного рішення, яке могло-би забезпечити дійсно безпечний та контрольований доступ до інформаційних ресурсів, але є ряд рекомендацій, що допоможуть у покращити захист.

Актуальність матриці доступу – адміністраторові системи важливо розуміти хто чим займається і при опрацюванні системи розподілення доступу взаємодіяти з відділом кадрів та керівниками структурних підрозділів підприємства. Правильно складена матриця доступу актуальність якої постійно підтримуються дозволяє значно зменшити площу атаки у випадку компрометації облікового запису. Дуже гарною практикою є, коли подібна таблиця існує не тільки «в голові» у адміністратора, а й є у вигляді формалізованого документу чи Excel-таблиці. При створенні подібної системи важливо керуватися принципом нульової довіри, тобто кожен користувач незалежно

від своєї посади повинен мати рівно стільки прав, скільки йому треба для виконання своїх посадових обов'язків. Також принципи нульової довіри кажуть, що модель підходу до проектування мережі при якій внутрішня зона є захищеною і довіреною – застаріла, сучасні тенденції впровадження BYOD, коли будь-хто з користувачів може принести в офіс свій особистий комп'ютер, який може не відповідати корпоративним стандартам безпеки потенційно наражають на небезпеку мережу, побудовану за такими принципами, тому важливо ставитися з повною недовірою до будь-якого пристрою в мережі.

Важливо дотримуватись правил складності паролів та частоти їх зміни. Згідно рекомендацій викладених в стандарті PCI DSS частота зміни – 90 днів, але даний період може варіюватись в залежності від багатьох факторів. Наприклад, при використанні схеми в якій процес з'єднання є прозорим для клієнтів і вони не проходять додаткових методів перевірки шляхом вводу свого паролю час життя паролю можна збільшити, так як його зміна тягне за собою можливу перегенерацію сертифікату та зміну конфігураційного файлу ovpn. У випадку, коли користувачі щоразу при з'єднанні проходять процес автентифікації пароль повинен змінюватись частіше, але це все ж таки в деякій мірі залежить від технічної обізнаності клієнтів, нехай краще пароль буде сталий й користувач його пам'ятатиме, ніж він буде змінюватись раз на місяць й клієнт зберігатиме його у вигляді листка прикріпленого до монітора.

При організації віддаленого доступу важливо провести аналіз та зрозуміти звідки будуть підключатись користувачі, гарною практикою є налаштувати дозвіл на підключення лише з України, це можна реалізувати за допомогою технології GeoIP. Цей інструмент допоможе на 90% скоротити кількість атак на сервіс.

При адмініструванні будь-якої IT-системи важливий постійний її моніторинг та централізований збір журналів (логів). Фаєрволи Sophos XGS мають підтримку єдиної системи управління та моніторингу рішень вендору Sophos, «Sophos Central». З його допомогою, можна реалізувати багато сценаріїв пов'язаних з вимірюванням різних метрик, кореляцією логів, автоматичним реагуванням на інциденти, сповіщення про них та багато іншого, але у випадку використання хмарних платформ є ризик, що при

втраті Інтернет з'єднання чи якщо станеться інцидент пов'язаний з перевантаженням каналів, з'єднання з хмарною платформою буде втрачене. Тому важливо дублювати подібні системи і завчасно подбати про локальну систему моніторингу чи хоча б централізованого збору логів, зараз існує дуже багато подібних безкоштовних платформ з відкритим вихідним кодом, що працюють на основі відкритих протоколів, таких як Syslog чи SNMP (Zabbix, Rsyslog, LibreNMS, Grafana та ін.). Також фаєровли Sophos XGS мають простий та зрозумілий REST API інтерфейс, що може допомогти адміністратору у створенні сценаріїв автоматизації різної складності.

Документація є невід'ємною частиною роботи будь-якого інженера, при адмініструванні інформаційної системи важливо створювати та підтримувати в актуальному стані різного роду планів, схем, таблиць та описів різних систем, для того, щоб у випадку розширення IT-команди не виникало зайвих запитань у нових співробітників, також це значною мірою допомагає при усуванні несправностей у роботі систем. Сюди ж можна віднести і відпрацювання підходу до створенні «читаємої» чи самодокументованої конфігурації пристрою. Це значить, що будь-які об'єкти в конфігурації фаєрволу (правила, адреси, специфічні сервіси) мають містити короткі, лаконічні назви, які в той же час відображають їхню сутність та призначення. При створення правил фаєрволу гарною практикою є додавати до них короткий опис у полі «Description».

При адмініструванні фаєрволів також важливим моментом є резервне копіювання конфігурації та підтримка актуальності резервних копій. Фаєрволи Sophos XGS мають доволі великий набір функцій, що допомагають вирішити це питання, також хмарна платформа «Sophos Central» дозволяє автоматизувати цей процес.

При управлінні фаєрволами критично важливим питанням є дублювання каналів управління, це допоможе зберегти управління пристроєм у разі внесення неправильної конфігурації. При адмініструванні пристрою через будь-який інтерфейс керування важливо приділити увагу безпеці цього самого каналу керування, нижче описані методи захисту, що варто налаштувати: автоматичне завершення сесії у разі бездіяльності (так званий тайм-аут сесії), завершує сеанс адміністрування та

деавтентифікує адміністратора, якщо той на виконує ніяких дій протягом певного проміжку часу, за замовчувнням це значення дорівнює 10 хв, за необхідності його можна зменшити чи збільшити; дозволити адміністративний доступ лише на деяких внутрішніх інтрефейсах та для визначених хостів, груп хостів чи користувачів; налаштувати «fail to ban», цей функціонал дозволяє встановити максимальну кількість невдалих спроб автентифікації з одного хоста за певний проміжок часу, після перевищення ліміту IP-адреса повинна бути заблокована на декілька хвилин, це дозволить захистити пристрій від підбору паролів; «CAPTCHA» – адміністратори, які входять до веб-консолі, а також гостьові користувачі, які заходять портал повинні вводити одноразовий пароль, який генерується у вигляді зображення, цей простий інструмент є ще одним дієвим засобом від спроби підбору паролів; встановлення політик, яким повинен відповідати пароль, його довжина, кількість спецсимволів, цифр, знаків верхнього та нижнього регістрів.

Будь-яка система захисту не є самодостатньою і має, як свої сильні так і слабкі сторони. При створенні комплексної системи захисту важливо посилювати рішення одне одним, наприклад, систему управління доступом можна посилити інтеграцією з хостовими антивірусами та інтеграцією зі стороннім рішенням NAC.

ВИСНОВКИ

В ході роботи було проведено дослідження сутності проблеми забезпечення захисту корпоративних мереж передачі даних та корпоративних інформаційних ресурсів та існуючих технологій для вирішення цієї проблеми, порівняння їх характеристик, визначення переваг та недоліків.

В першому розділі було розглянуто ряд технологій та підходів до управління доступом до інформаційної системи, ретельно розглянуто доцільність впровадження тієї чи іншої технології. Шляхом аналізу та порівняння цих технологій було визначено, що технологія SSL-VPN відрізняється від конкурентів економічністю з точки зору ресурсів, продуктивністю, криптостійкістю алгоритмів шифрування, масштабованістю, керованістю. Порівняння технологій проводилося за такими параметрами: актуальність підтримуємих криптографічних алгоритмів, простота інтеграції, можливість використання в середовищах із трансляцією мережевих адрес, пропускна здатність, можливість інтеграції з іншими рішеннями.

Проаналізувавши методи та засоби забезпечення доступу до корпоративних ресурсів було встановлено, що для підприємств малого та середнього бізнесу найкращим рішенням з точки зору економічності та керованості є реалізація подібної технології на базі міжмережевого екрану, як така, що дозволяє сконцентрувати всі

інформаційні потоки в одному місці та створити на його базі центр керування доступом.

У ході проведення дослідження було встановлено сутність завдань захисту корпоративних інформаційних ресурсів, яка полягає у: керуванні життєвим циклом політик безпеки; перевірка стану безпеки, оцінці відповідності політиці безпеки по типу користувача, типу пристрою та операційній системі; керуванні ідентифікацією і доступом; протистоянні атакам нульового дня; авторизації, автентифікації та обліку мережевих з'єднань; контролю доступу на основі профілів користувачів; профілювання: виявлення скомпрометованих пристроїв до того, як шкідливий код зможе завдати шкоди; реагуванню на інциденти: нейтралізації мережевих загроз застосуванням політик безпеки, що блокують небажаний трафік ізолюють скомпрометованих користувачів та ресурси, відновлюють працездатність сервісів; генерації звітів і аналітичних даних про спроби доступу.

У другому розділі було розглянуто фаєрволи Sophos XGS та суміжні системи захисту. У ході дослідження було визначено, що реалізація технології на базі фаєрволів Sophos XGS визначена, як одна з найперспективніших, так як вона поєднує в собі простоту налаштування й експлуатації; сучасні засоби моніторингу; можливість інтеграції з іншими рішеннями вендору «Sophos Central» та «Sophos Intercept X», що дозволяє посилити захист; в той же час, реалізація технології зберігає відкритість стандарту, що дозволяє більш тонко налаштовувати систему під специфічні задачі. Було розглянуто можливі варіанти архітектури рішення та можливості щодо адміністрування подібної системи. В ході вивчення суміжних технології було визначено, що конвергенція фаєрволів, хмарних аналітичних платформ та хостових системи значно розширює можливості технології керування доступом та покращує видимість інформаційної системи в цілому.

У третьому розділі було наведено варіант топології інформаційної системи підприємства та методи надання доступу до неї на базі Sophos XGS. Розроблено рекомендації щодо застосування технології управління доступом до мережі.

Використання запропонованого варіанту технології дозволить створити просту, керовану та прозору з точки зору клієнтів систему, що в той же час забезпечує повну видимість, контроль, максимальну захищеність та інтеграцію з іншими рішеннями.

ПЕРЕЛІК ПОСИЛАНЬ

1. A History and Survey of Network Firewalls / Ingham K., Forrest S. 2004. P. 4–30.

2. Compuquip. What is a Firewall? The Different Firewall Types & Architectures [Електронний ресурс] – Режим доступу: https://www.compuquip.com/blog/types-firewall-architectures

3. Javatpoint. Types of Firewall [Електронний ресурс] – Режим доступу: https://www.javatpoint.com/types-of-firewall

4. Parallels. What Are the Basic Types of Firewalls? [Електронний ресурс] – Режим доступу: https://www.parallels.com/blogs/ras/types-of-firewalls/

5. Juniper. Stateful Firewalls [Електронний ресурс] – Режим доступу: https://www.juniper.net/documentation/us/en/software/junos/interfaces-adaptive-services/topics/topic-map/stateful-firewalls.html

6. Purplesec. Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2022 [Електронний ресурс] – Режим доступу: https://purplesec.us/resources/cyber-security-statistics/

7. Cisco. What Is Network Access Control? [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

8. Genias. Understanding Network Access Control [Електронний ресурс] – Режим доступу: https://docs.genians.com/release/en/intro.html

9. Aruba Networks. What Is AAA? [Електронний ресурс] – Режим доступу: https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/802.1X%20Authentication/About_AAA.htm

10. Sophos. Sophos firewall solution brief [Електронний ресурс] – Режим доступу: https://assets.sophos.com/X24WTUEQ/at/jsnq2t4n27xzvr53khxc8m/sophos-firewall-solution-brief.pdf

11. Sophos. Sophos XGS tech specs [Електронний ресурс] – Режим доступу: https://www.sophos.com/en-us/products/next-gen-firewall/tech-specs#Overview

12. Sophos. Introducing Sophos Firewall and the New XGS Series Appliances [Електронний ресурс] – Режим доступу: https://partnernews.sophos.com/en-us/2021/04/products/introducing-sophos-firewall-and-the-new-xgs-series-appliances/

13. Techbast. Sophos Deployment Mode [Електронний ресурс] – Режим доступу: https://techbast.com/2016/07/sophos-deployment-mode.html

14. Sophos. Administrator help [Електронний ресурс] – Режим доступу: https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/GettingStarted/index.html

15. Linkmeup. Где сохранить пакет [Електронний ресурс] – Режим доступу: https://linkmeup.ru/blog/929/

16. Ixbt. IPSec — протокол защиты сетевого трафика на IP-уровне [Електронний ресурс] – Режим доступу: https://www.ixbt.com/comm/ipsecure.shtml

17. Opennet. VPN и IPSec на пальцах [Електронний ресурс] – Режим доступу: http://www.opennet.ru/docs/RUS/vpn_ipsec/

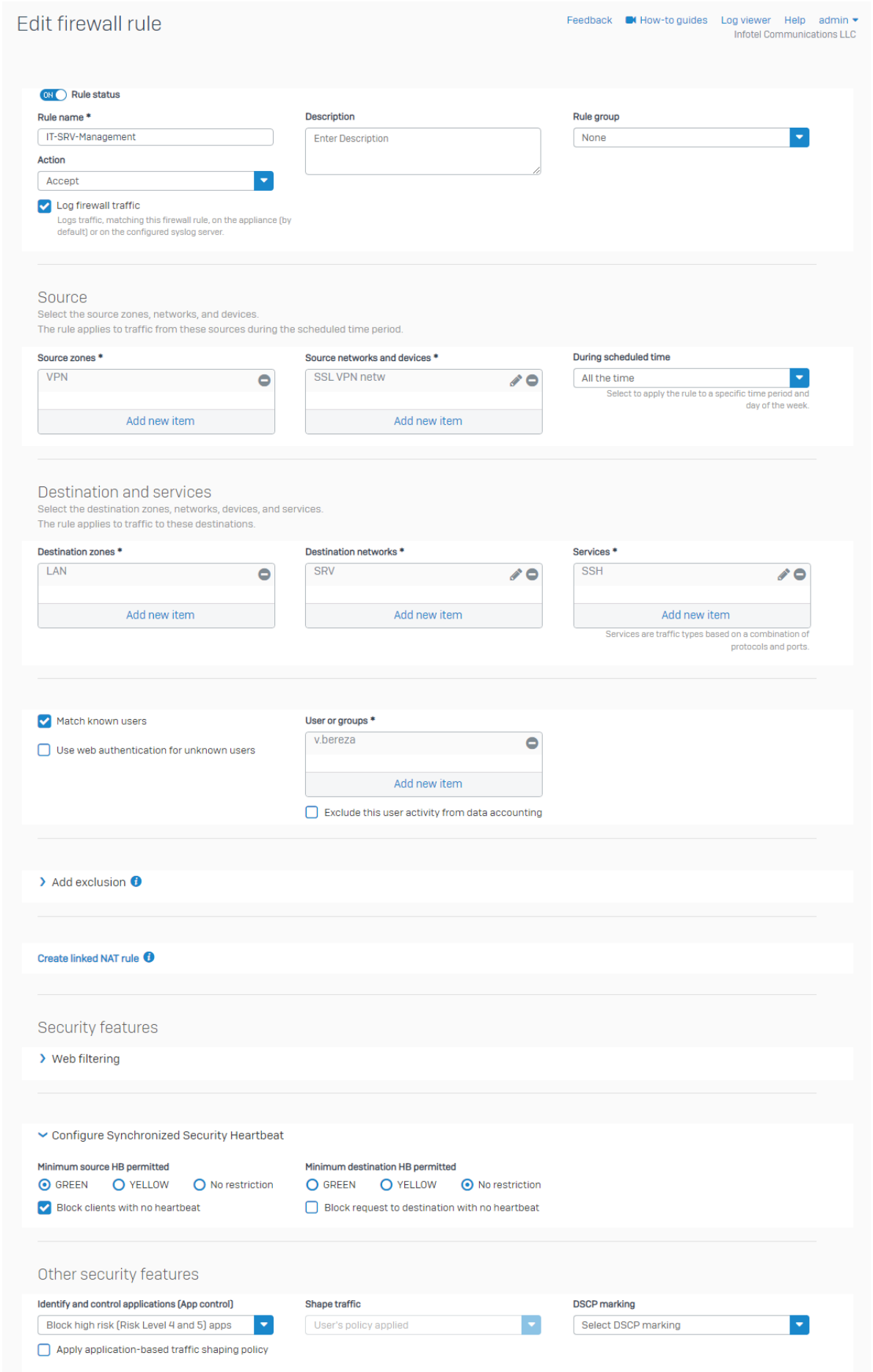
18. Fortinet. What is an SSL VPN? [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/ssl-vpn

19. Sophos. Sophos Firewall: Configure SSL VPN remote access [Електронний ресурс] – Режим доступу: https://support.sophos.com/support/s/article/KB-000035542?language=en_US

20. Sophos. Sophos Central [Електронний ресурс] – Режим доступу: https://www.sophos.com/en-us/products/sophos-central

21. Sophos. The World’s Best Endpoint Protection [Електронний ресурс] – Режим доступу: https://www.sophos.com/en-us/products/endpoint-antivirus

ДОДАТОК А


Edit firewall rule
Feedback
How-to guides
Log viewer
Help
admin
Infotel Communications LLC
ON
Rule status
Rule name *
IT-SRV-Management
Description
Enter Description
Rule group
None
Action
Accept
Log firewall traffic
Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.
Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.
Source zones *
VPN
Add new item
Source networks and devices *
SSL VPN netw
Add new item
During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.
Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.
Destination zones *
LAN
Add new item
Destination networks *
SRV
Add new item
Services *
SSH
Add new item
Services are traffic types based on a combination of protocols and ports.
Match known users
Use web authentication for unknown users
User or groups *
v.bereza
Add new item
Exclude this user activity from data accounting
Add exclusion
Create linked NAT rule
Security features
Web filtering
Configure Synchronized Security Heartbeat
Minimum source HB permitted
GREEN
YELLOW
No restriction
Block clients with no heartbeat
Minimum destination HB permitted
GREEN
YELLOW
No restriction
Block request to destination with no heartbeat
Other security features
Identify and control applications (App control)
Block high risk (Risk Level 4 and 5) apps
Apply application-based traffic shaping policy
Shape traffic
User's policy applied
DSCP marking
Select DSCP marking

(Презентація)