DOI: https://doi.org/10.26565/2304-6201-2024-63-05

УДК 004.415.53

Мелкозьорова Ольга Михайлівна *кандидат технічних наук, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків-22, Україна, 61022; e-mail: olha.melkozerova@karazin.ua* https://orcid.org/0000-0002-1134-2925

Колованова Євгенія Павлівна *кандидат технічних наук, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків-22, Україна, 61022; e-mail: e.kolovanova@karazin.ua; https://orcid.org/0000-0002-0326-2394*

Малахов Сергій Віталійович *кандидат технічних наук, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій, Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків-22, Україна, 61022; e-mail: malakhov@karazin.ua https://orcid.org/0000-0001-8826-1616*

Огляд можливостей, налаштування та використання технологій з кібербезпеки для захисту інформаційної мережі

Кібербезпека – ключова частина критичної інфраструктури України. Особливо це стало актуальним зараз під час впливу російської агресії. Усі компанії можуть опинитися під впливом кібератак. Вартість витоку даних для великих організацій може сягнути сотень мільйонів доларів. Треба розуміти, що у компаніях працюють звичайні люди, соціальна інженерія залишається найпоширенішим видом атак. Інтернет та комп'ютери відіграють надзвичайно важливу роль не тільки, коли ці люди працюють, а також у повсякденному житті, коли відбувається спілкування поштою, у чатах або є взаємодія із банківською системою тощо. Ми живемо у світі, де загрози безпеці є всюди. Тому метою цієї роботи є необхідність ознайомлення з сучасними технологіям, які дозволяють розглянути всі можливості захисту від кіберзагроз. Комплексний захист у просторах інтернету, наприклад, забезпечують програмні та апаратні продукти компанії Check Point, які надають потужну основу для відпрацьовування захисту комп'ютерної мережі від небажаного або шкідливого захисту, для чого є можливість розгортання їх експериментальних стендів. Результатом цієї статті є рекомендації по розгортанню стендів Check Point для користувачів Windows, що є актуальною задачею для адміністраторів з кібербезпеки. Також у статті наведено огляд базової архітектури Check Point, яка складається з сервера безпеки, мережевого екрану та додатку управління, який використовується для налаштування фундаментальних політик безпеки з правилами, що керують трафіком між відповідними об'єктами. Сервер безпеки та мережевий екран мають властивості (характеристики), роботу яких можна описати моделлю взаємодії відкритих систем, тому у статті розглянуто рівні, з яких складається ця модель, а також самі вбудовані властивості цих об'єктів, такі як, наприклад, антивірус, антифішинг, антибот та інші. Ця стаття може бути актуальною для студентів старших курсів та аспірантів, які навчаються за спеціальністю з кібербезпеки.

Ключові слова: *Модель взаємодії відкритих систем, мережевий екран, Check Point, стенд, Open Server, антивірус, атака, шкідливе програмне забезпечення.*

.

Як цитувати: Мелкозьорова О. М., Колованова Є. П., Малахов С.В. Огляд можливостей, налаштування та використання технологій з кібербезпеки для захисту інформаційної мережі. *Вісник Харківського національного університету імені В. Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2024. вип. 63. С.51-59. https://doi.org/10.26565/2304-6201-2024-63-05

How to quote: O. Melkozerova, I. Kolovanova, S. Malakhov "Introduction to capabilities, configuration and using of cybersecurity technologies for information network protection", *Bulletin of V. N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 63, pp. 51-59, 2024. https://doi.org/10.26565/2304-6201-2024-63-05 [in Ukrainian]

© Мелкозьорова О.М., Колованова Є.П., Малахов С.В. 2024
This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0.

Вступ

У теперішні часи кібербезпека стала масовою частиною сучасного суспільства для організацій і ніколи не була раніше більш значущою. Так склалося, тому що люди покладаються на речі, засновані на мережі Інтернет: комп'ютерні системи, мережі та розумні пристрої під назвою Internet of Things (IoT). Через складність і широкий спектр цих пристроїв кібербезпека залишається актуальною проблемою для всіх [1].

У повсякденному житті продовжують існувати погані звички кібербезпеки (poor cybersecurity habits), які роблять користувачів та організації вразливими до атак. Відсутність багатофакторної аутентифікації (multi-factor authentication – MFA), незахищена мережа WiFi і недостатня політика паролів – все це серед цих звичок. Уразливості мобільних пристроїв продовжують залишатися питанням номер один, коли робота з дому залишається способом життя. Але все ще є надія, що цей час стане часом, коли всі організації покращать освіту з кібербезпеки і набудуть всіх навичок, необхідних для реалізації всіх необхідних процедур на свою користь [2].

Вартість витоку даних для великих організацій може сягнути сотень мільйонів доларів. Є безліч типів даних: фінансові дані, персональна ідентифікуюча інформація, бізнес-процес, пошта та спілкування, інтелектуальна власність, контракти та заявки, списки клієнтів.

Однією з можливостей комплексного захисту у просторах інтернету є програмні та апаратні продукти компанії Check Point, які надають потужну основу для відпрацьовування захисту комп’ютерної мережі від небажаного або шкідливого захисту, для чого є можливість розгортання їх експериментальних стендів. Але правильне розгортання та використання їх програмного забезпечення не є тривіальною задачею, тому у цій статті є рекомендації по розгортанню стендів Check Point для користувачів Windows, що актуально для адміністраторів з кібербезпеки. Також у статті наведено огляд базової архітектури Check Point, яка складається з сервера безпеки, мережевого екрану та додатку управління, який використовується для налаштування фундаментальних політик безпеки з правилами, що керують трафіком між відповідними об’єктами. Сервер безпеки та мережевий екран мають властивості (характеристики), роботу яких можна описати моделлю взаємодії відкритих систем, тому у статті розглянуто рівні, з яких складається ця модель, а також самі вбудовані властивості цих об’єктів, такі як, наприклад, антивірус, антифішинг, антибот та інші. Ця стаття може бути актуальною для студентів старших курсів та аспірантів, які навчаються за спеціальністю з кібербезпеки.

1. Модель взаємодії відкритих систем (Open system interconnect model)

Еталонна модель взаємодії відкритих систем open system interconnection – найбільш вдала спроба стандартизації протоколів обміну даними, рік розробки моделі - 1984. Вона стала основою для розробки мережевих стандартів і гарною основою для вивчення та порівняння різних мережевих телекомунікаційних технологій. Відповідно до цієї моделі всі протоколи взаємодії поділяються на 7 рівнів, які є в таблиці 1:

1) Функція фізичного рівня – це передача потоку бітів за допомогою матеріальних переносників сигналів між двома точками по заданому каналу зв'язку. Це нижчий рівень ієрархії стека протоколів. Фізичний рівень визначає електричні та механічні характеристики підключення до фізичних ліній зв'язку. Фізичний рівень надає сервіс для наступного канального рівня або рівня ланки даних, який відповідає за передачу даних через зв'язок між двома вузлами мережі.

2) Функціями канального рівня є: упаковка інформації в кадри певної довжини, побудова перешкодостійких кодових конструкцій, формування контрольних сум. Перевірка правильності передачі кадрів після їх отримання та формування підтверджень, якщо такі передбачені в системі з повторною передачею непідтверджених даних.

3) Мережевий рівень забезпечує взаємодію між вузлом та мережею. Він формує мережеві адреси пакетів, керує потоками, маршрутизацією та підтримкою транспортних з'єднань. Одиницею кількості чи обсягу інформації протоколів мережевого рівня є пакет. Тому часто мережевий рівень називають пакетним.

4) Четвертий рівень – транспортний, призначений для трансляції потоків даних з одного порту в інший. Під портом розуміється кінець логічного каналу мережі передачі, де завершується операція транспортування. На транспортному рівні встановлюється та розриваються транспортні сполучення, формуються пакети, що належать потоку, що передається в сеансі зв'язку. Транспортний сервіс звільняє вищі рівні від рутинних завдань організації передачі.

5) Сеансовий рівень - це сукупність завдань, пов'язаних з організацією, підтримкою та закінченням сеансів логічного зв'язку між прикладними процесами, що взаємодіють по мережі.

6) Представницький рівень забезпечує перетворення даних у форму, зручну для прикладної програми. На цьому рівні операції ведуться з форматами даних та команд.

7) Сьомий рівень називається прикладним. Він пов’язаний з процесами обробки інформації, тобто прикладними процесами і забезпечують роботу прикладної програми так, ніби обмін даними відбувався не через мережу або комунікації, а автономно, всередині обчислювальної машини.

Далеко не кожна з систем телекомунікацій з комп'ютерних мереж містить у явному вигляді ознаки всіх семи рівнів, що є у моделі. Корисність цієї моделі, безперечно, у тому, що будь-який розробник нової системи віддаленої взаємодії комп'ютерної мережі або системи телекомунікації повинен чітко визначити рівень протоколів, на яких він працюватиме, що забезпечить стандартизацію та можливість подальшого розвитку розробок, навіть якщо їх виготовлятимуть інші виконавці.

Таблиця 1. Модель взаємодії відкритих систем

Рівень	Назва
1	Рівень додатків (Application)
2	Представницький (Presentation)
3	Сеансовий (Session)
4	Транспортний (Transport)
5	Мережевий(Network)
6	Канальний (Data Link)
7	Фізичний (Physical)

2. Програмне оточення для встановлення стендів Check Point

Для демонстрації та навчання можливостям технологіям використання Check Point розповсюдженими є різноманітні стенди з віртуальними машинами, які можна встановлювати на Windows з використанням візуалізаторів таких як, наприклад, VMware (Worksration) [3], VirtualBox [4] та Hyper-V [5]. Всі вони є доступними, але вбудованою середою для Windows10 є саме Hyper-V, окрім того, Hyper-V дозволяю швидко створювати віртуальні машини Windows 10 MSIX packaging environment (Windows 10 Enterprise Evaluation) без додаткових iso файлів та відносно малою потребою у пам’яті 2048 МБ. Тому для розгортання стендів Check Point у цій статті використовувався саме Hyper-V.

Умовно віртуальні машині у експериментальних стендах можна поділити на: віртуальні машини Microsoft та машини Check Point. До архітектури Check Point належить сервер безпеки (security management server), шлюз безпеки (security gateway) та Smart Console [6] (рисунок 2.1). Їх призначення описується у розділах 3 та 4 цієї статті.

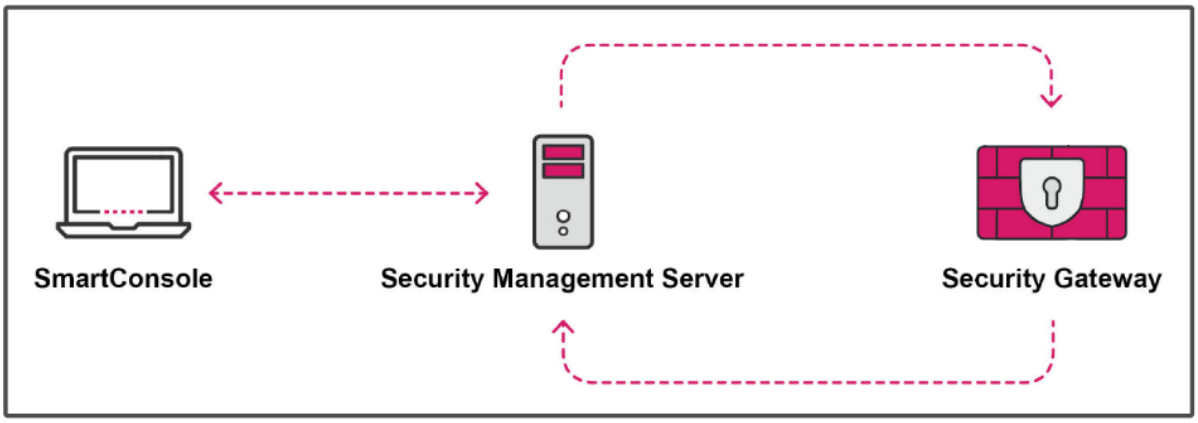

Рис.2.1 Архітектура Check Point []

Для побудови стендів на базі цієї архітектури, окрім машин Microsoft, використовується програмне забезпечення:

Check_Point_R81.20_T634.iso – операційна система Gaia, яка може працювати як сервер безпеки або мережевий екран, що налаштовується у Gaia Portal після надання доступу до Web UI;

Check_Point_SmartConsole_R81_20_jumbo_HF_B655_Win.exe – smart console, яка забезпечує графічний інтерфейс для централізованого управління у оточенні Check Point. На рисунках 2.1, 2.2 – скріншот деякий встановлених віртуальних машин, так виглядають встановлені віртуальні машини із консолі. На віртуальні машини Check Point треба встановлювати ліцензії і контракти, як це показано на рисунку 2.3. Ліцензії і контракти можна завантажити через Smart Console з умовою, що ця віртуальна машина працює і має статус під'єднаної до сервера безпеки.

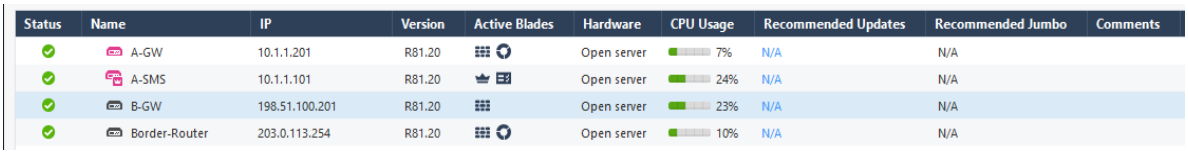

Рис.2.2 Створені віртуальні машини у Smart Console

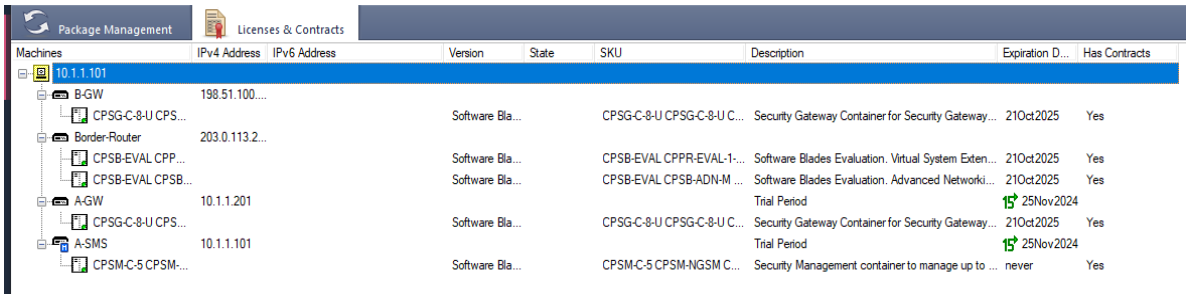

Рис.2.3 Створені віртуальні машини у Smart Console із ліцензіями та контрактами

До машин Microsoft відносяться машині Windows 10 та Windows Server 2019, 17763.3650.221105-1748.rs5_release_svc_refresh_SERVER_EVAL_x64FRE_en-us.iso файл сервера можна завантажити за посиланням [7]. Для завантаження html документу використовується інструмент Internet information services manager. На рисунку 2.4 можна побачити ip адресу 192.198.12.101, доступ через порт 80. На рисунку 2.5 видно файл html, який є у папці. Доступ до сайту можна отримати за посиланням http://192.168.12.101, як це видно на рисунку 2.6. Документ html було завантажено з сайту partner map Check Point [8].

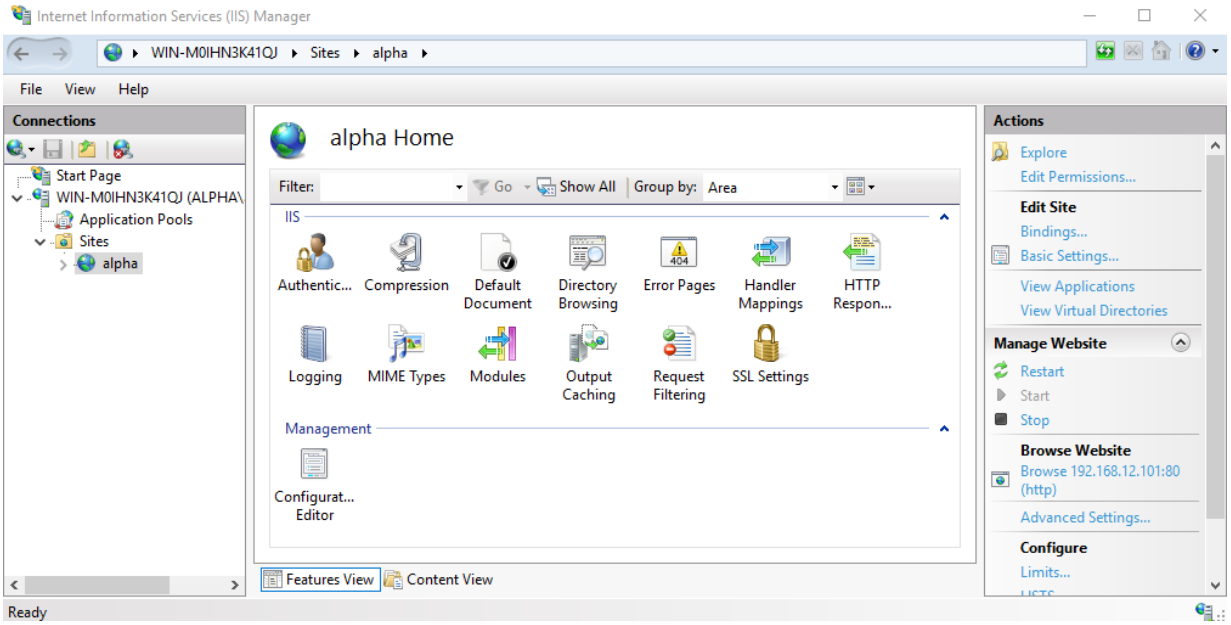

Рис.2.4 Інструмент Internet information services manager, можна побачити ip адресу 192.198.12.101

3. Сервер безпеки Security Management Server Check Point

Security Management Server – це сервер, який керує об'єктами у смарт консолі, встановлюється шляхом запуску операційної системи Gaia та подальшим налаштуванням First Time Configuration Wizard через Gaia Portal. Після відповідних налаштувань можна перевірити статус запуску сервера, на рисунок 3.1 – сервер ще не запущений, на рисунку 3.2 – сервер запущений. Доки не буде статусу started, смарт консоль запускатися не буде.

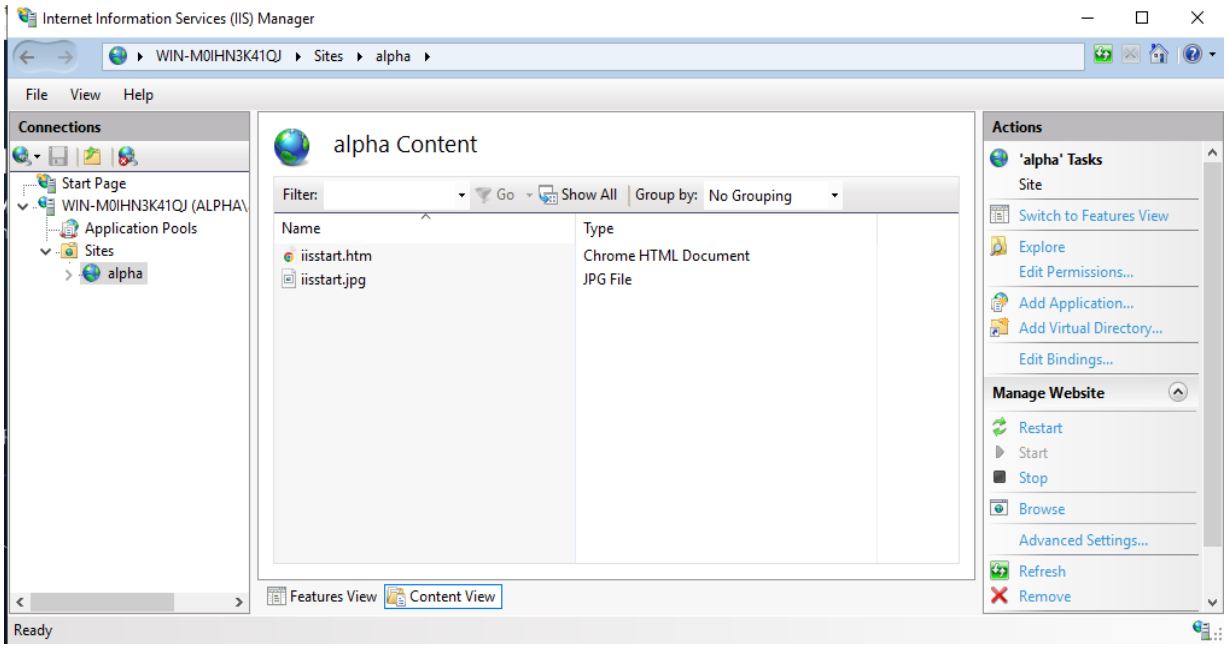

Рис.2.5 Інструмент Internet information services manager, можна побачити html документ

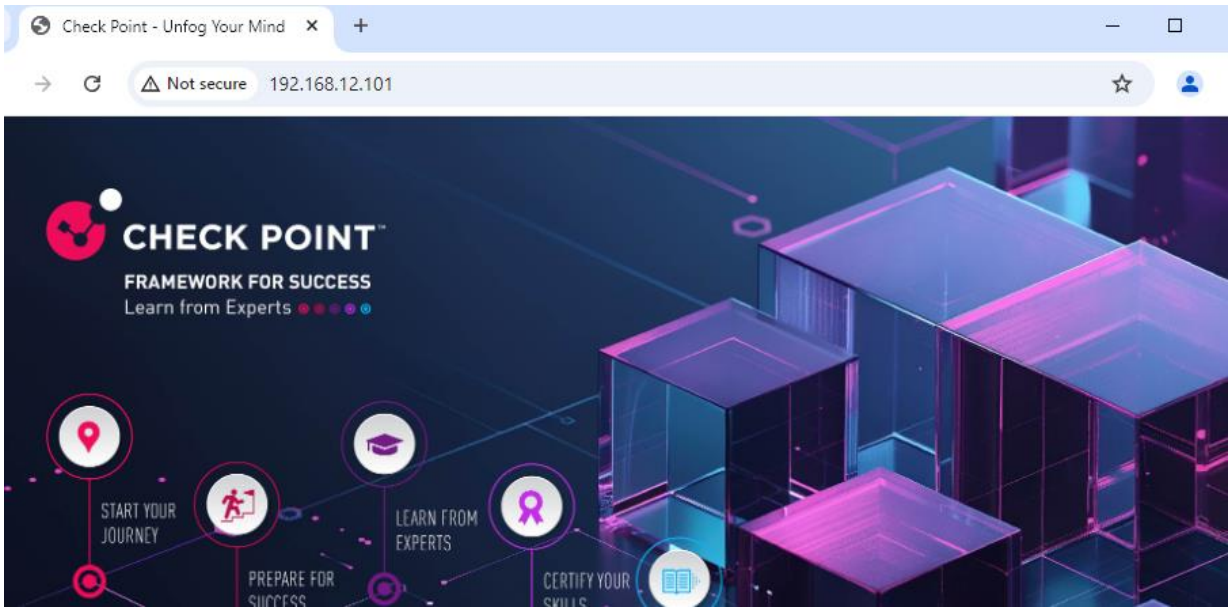

Рис.2.6 Відображення сайту у браузері, доступ http://192.168.12.101 (документ html було завантажено з сайту [8]

```
A-SMS> api status

API Settings:
---------------------
Accessibility:                    Require local
Automatic Start:                  Unknown

Processes:

Name      State     PID       More Information
-------------------------------------------------
API       Stopped   6769
CPM       Starting  6769      Check Point Security Management Server is during initialization
FWM       Started   6449
APACHE    Started   5593
```

Рис.3.1 Перевірка статусу стану сервера безпеки: сервер ще не працює

```
A-SMS> api status

API Settings:
---------------------
Accessibility:                    Require local
Automatic Start:                  Enabled

Processes:

Name      State     PID       More Information
-------------------------------------------------
API       Started   6769
CPM       Started   6769      Check Point Security Management Server is running and ready
FWM       Started   6449
APACHE    Started   5593

Port Details:
-------------------
JETTY Internal Port:              50337
JETTY Documentation Internal Port: 60428
APACHE Gaia Port:                 443

Profile:
-------------------
Machine profile:                  Small Medium env resources profile
CPM heap size:                    1280m

                        Apache port retrieved from: httpd-ssl.conf


-----------------------------------------
Overall API Status: Started
-----------------------------------------

API readiness test SUCCESSFUL. The server is up and ready to receive connections

Notes:
------------
To collect troubleshooting data, please run 'api status -s <comment>'
```

Рис.3.2 Перевірка статусу стану сервера безпеки: сервер працює, можна запускати Smart Console

На рисунку 3.3 наведено основні характеристики сервера безпеки Check Point, нижче стисло наведено їх опис:

- Network policy management забезпечує комплексне, централізоване управління шлюзами безпеки через смарт консоль.

- Встановлений на комп'ютер клієнт Harmony Endpoint забезпечує захист віддалених користувачів від всіх загроз, підключається через Endpoint policy server за допомогою властивості Endpoint policy management.

- User Directory дозволяє застосовувати LDAP сервери (lightweight directory access protocol) для отримання ідентифікації та інформації про мережу користувачів, знизити рівень, пов'язаний з ручним налаштуванням та синхронізацією надлишкової інформації.

- Provisioning забезпечує централізоване адміністрування та забезпечення пристроїв Check Point.

- Compliance забезпечує інтегровану та повністю автоматизовану безпеку та моніторинг сумісності.

- Smart Event Server інтегрується з архітектурою серверу безпеки та комунікує з Log Server для читання та аналізу логування.

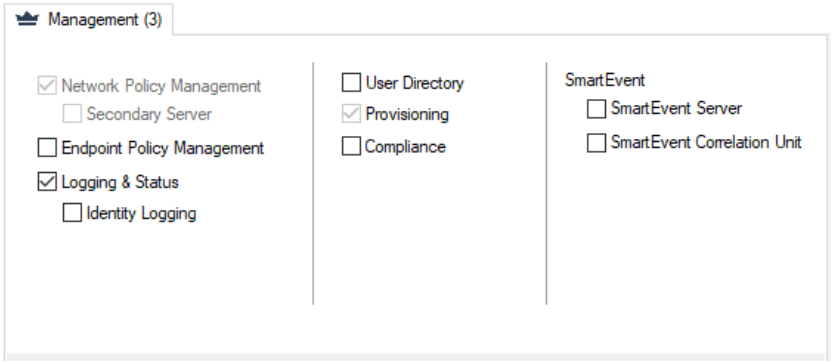

Рис.3.3 Скріншот основних властивостей сервера безпеки Check Point

4. Шлюз безпеки Security gateway Check Point

Мережеві екрани (security gateway, firewall) – перша лінія захисту проти кібератак, досліджує (забороняє або дозволяє) вхідний та вихідний трафік відповідно до визначених політик безпеки, щоб захистити мережу від небажаного або шкідливого трафіку. Політики безпеки складаються із правил, які встановлюються на відповідний мережевий екран. Адміністратор може створити правила, щоб дозволити відповідний тип трафіку.

Мережеві екрани можуть бути представлені апаратним забезпеченням, програмним забезпеченням та комбінацією обох. У вільному доступі є реалізація у вигляді програмного забезпечення Open Server.

Деякі стандартні технології, які використовуються для цієї мети: packet filtering, stateful inspection, application layer firewall.

Властивості захисту мережі для мережевих екранів на прикладі Check Point можна поділити на дві категорій:

- захист мережі (network security) (рисунок 4.1);
- захист від загроз (thread prevention) (рисунок 4.2).

Серед налаштувань для захисту від загроз можна виділити наступні:

- Sandbox. Захист від невідомих та передових атак шляхом запуску підозрілих файлів та використання технік штучного інтелекту.
- Sand Blast thread emulation захищає від багато-рівневих атак на ранній стадії.
- Sand Blast thread extraction знижує рівень загроз від Microsoft Office та PDF документів шляхом видалення контенту, такого як макросів, вставлених об’єктів, та зовнішніх посилань. Працівник отримує документ, який містить відомі безпечні елементи.
- Thread Cloud – це глобальний хмарний інтелект, який використовує всесвітню мережу сенсорів загрози Check Point.
- Anti-Virus виконує пре інфекційне виявлення та блокування шкідливого програмного забезпечення та постійно оновлюється ThreadCloud.
- Zero phishing запобігає невідомим (zero-day) та відомим атакам на веб-сайтах у реальному часі з використанням алгоритмів машинного навчання та патентованим інспекційним технологіям.
- Sanitization забезпечує захист від невідомих атак, шляхом обробки файлів перед тим, як вони будуть передані до користувача.
- Command and control (C&C) визначає інфіковані і компрометовані пристрої у мережі, блокує атаки за запобігає пошкодженню шляхом блокування шкідливого програмного забезпечення.
- Anti-Bot захищає від руйнувань шляхом блокування ботів комунікацій C&C.
- Intrusion prevention system (IPS protection) забезпечує передовий захист від атак та захищає усі інформаційні системи: сервери, індустріальні системи та Інтернет речей (IoT).

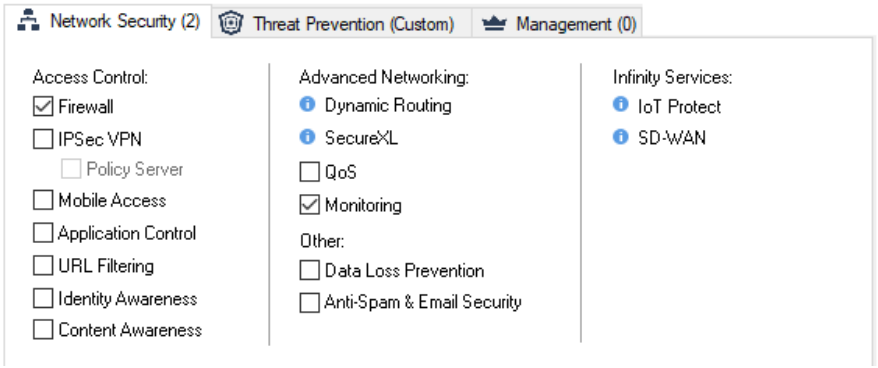

Рис.4.2 Можливість налаштування об'єкту Gateway консолі для захисту мережі

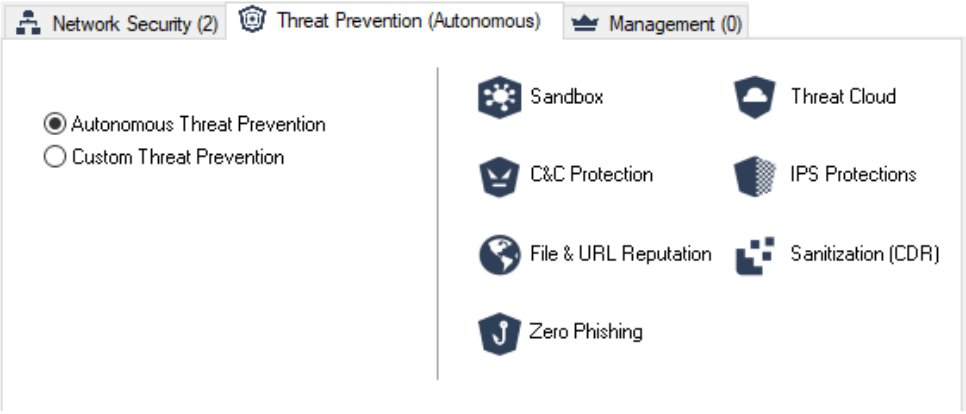

Рис.4.3 Можливість налаштування об'єкту Gateway консолі для захисту від загроз

Висновки

Кібербезпека завжди була і буде важливим об'єктом дослідження та удосконалення, оскільки пройшла велику відстань самовдосконалення та змін, але не можна стверджувати, що досягла своєї мети, коли всі люди можуть себе почувати захищеними від кібератак. Мета цієї роботи – це збір програмної бази для експериментальних стендів, які можуть бути у нагоді для дослідження можливостей захисту від кібератак. Така освітня база дозволила б підвищити рівень знань з кібербезпеки, тому що соціальна інженерія залишається поширеним видом атак. У роботі наведено перелік програмного забезпечення та рекомендації по його розгортанню з акцентом на збереженні ресурсів комп'ютерів. Апаратне забезпечення коштує багато грошей, тому вихід – це використання віртуальних машини. Віртуальні машини займають багато місця на жорсткому диску та вимагають багато оперативної пам'яті. При розгортанні таких стендів потрібна оптимізація використаних ресурсів. У якості прикладу експериментального стенду використано програмне забезпечення Check Point (машини на операційний системі Gaia) та Microsoft, а саме Windows 10 та Windows Server 2019. Наведено перелік властивостей віртуальних машин Check Point.

Існує безліч програмних інструментів, таких як, наприклад, сканери вразливостей, антивірусні програми тощо. Задача систематизації таких програм, пошуку кращих рішень – це задачі для подальших досліджень. Окрім того, експериментальний стенд, який розгортався для написання цієї статті, складався в восьми віртуальних машин. З використанням потужного комп'ютера вони були створені та запущені. При відсутності таких можливостей на звичайному ноутбуці можна запустити до 4 машин. Є ймовірність що кількість віртуальних машин треба буде збільшувати. Все це говорить про необхідність використання хмарних сервісів, таких, як, наприклад, Azure, що також є важливою та актуальною подальшою задачею.

СПИСОК ЛІТЕРАТУРИ

1. Range Force: веб-сайт. URL: https://www.rangeforce.com/ (дата звернення: 27.10.2024).
2. Вступ до кібербезпеки : методичні вказівки щодо виконання практичних робіт. / О. М. Мелкозьорова та ін. Харків : ХНУ імені В. Н. Каразіна, 2024. 36 с.
3. Wmvare: веб-сайт. URL: https://www.vmware.com/ (дата звернення: 25.11.2024).

4. VirtualBox: веб-сайт. URL: https://www.virtualbox.org/ (дата звернення: 25.11.2024).
5. Introduction to hyper-v on Windows: веб-сайт. URL: https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/ (дата звернення: 25.11.2024).
6. Dreyer P, Frey M., Joaquim M. Check point certified security administrator : Student and lab manual. Tel Aviv Israel, 2023. 906 p. URL: https://read.kortext.com/reader/pdf/2342938/2
7. Microsoft evaluation center: веб-сайт. URL: https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019/ (дата звернення: 29.11.2024).
8. Partner map Check Point: веб-сайт. URL: https://sc1.checkpoint.com/uc/htmls/PartnerHome.html (дата звернення: 29.11.2024).

REFERENCES

1. Range Force. [Online]. Available: https://www.rangeforce.com/. Accessed on: October 27, 2024.
2. О. М. Мелкозьорова, С. В. Малахов, О. П. Нарєжній, Є. П. Колованова та І. М. Гальцева**,** Вступ до кібербезпеки: методичні вказівки щодо виконання практичних робіт. Харків, Україна: ХНУ імені В. Н. Каразіна, 2024. [in Ukrainian]
3. Wmvare. [Online]. Available: https://www.vmware.com/. Accessed on: November 25, 2024.
4. VirtualBox. [Online]. Available: https://www.vmware.com/. Accessed on: November 25, 2024.
5. Introduction to hyper-v on Windows. [Online]. https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/. Accessed on: November 25, 2024.
6. P. Dreyer, M. Frey M. ta M. Joaquim, Check point certified security administrator : Student and lab manual. Tel Aviv, Israel, 2023. 906 p. [in English]
7. Microsoft evaluation center. [Online]. https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019/. Accessed on: November 29, 2024.
8. Partner home Check Point. [Online]. https://sc1.checkpoint.com/uc/htmls/PartnerHome.html. Accessed on: November 29, 2024.

Melkozerova Olha *PhD,Associate Professor of Cybersecurity of information systems, networks and technologies Department V. N. Karasin Kharkiv National University, Svobody Sq 4, 61022, Kharkiv, Ukraine;*

Kolovanova Ievgenia *PhD,Associate Professor of Cybersecurity of information systems, networks and technologies Department V. N. Karasin Kharkiv National University, Svobody Sq 4, 61022, Kharkiv, Ukraine;*

Malakhov Serhii *PhD,Associate Professor of Cybersecurity of information systems, networks and technologies Department V. N. Karasin Kharkiv National University, Svobody Sq 4, 61022, Kharkiv, Ukraine.*

Introduction to capabilities, configuration and using of cybersecurity technologies for information network protection

Cybersecurity is a key part of Ukraine's critical infrastructure. This has become especially relevant now during the impact of Russian aggression. All companies can be affected by cyberattacks. The cost of data leakage for large organizations can reach hundreds of millions of dollars. It is necessary to understand that ordinary people work in companies, social engineering remains the most common type of attack. The Internet and computers play an extremely important role not only when these people work, but also in everyday life, when communicating by mail, in chats or interacting with the banking system, etc. We live in a world where security threats are everywhere. Therefore, the purpose of this work is the need to familiarize yourself with modern technologies that allow you to consider all the possibilities of protection against cyberthreats. Comprehensive protection in the Internet, for example, is provided by software and hardware products of the Check Point company, which provide a powerful basis for practicing the protection of a computer network from unwanted or malicious protection, for which there is a possibility of deploying their experimental stands. The result of this article is recommendations for deploying Check Point stands for Windows users, which is a relevant task for cybersecurity administrators. The article also provides an overview of the basic architecture of Check Point, which consists of a security server, a firewall, and a management application, which is used to configure fundamental security policies with rules that govern traffic between the corresponding objects. The security server and the firewall have properties (characteristics) whose work can be described by the model of open systems interaction, so the article considers the layers that make up this model, as well as the built-in properties of these objects themselves, such as, for example, antivirus, anti-phishing, anti-bot, and others. This article may be useful for students and philosophy students studying in the specialty of cybersecurity.

Keywords: *Open Systems interconnection Model, firewall, Check Point, stand, Open Server, antivirus, attack, malware.*

Надійшла у першій редакції 19.09.2024, в останній - 20.10.2024.
The first version has been received on 19.09.2024, the final version – on 20.10.2024.