ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ БЕЗПЕКОЮ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ ФАЕРВОЛУ PALO ALTO»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач(ка) вищої освіти групи БСДМ-62
ЖУРАВЕЛЬ Антон
(ПРІЗВИЩЕ, Ім'я)

Керівник: КУЗНЄЦОВ Олександр
д.т.н., професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Журавлю Антону Васильовичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія управління безпекою корпоративної мережі на основі фаєрволу Palo Alto»
керівник кваліфікаційної роботи: КУЗНЄЦОВ Олександр, д.т.н, професор,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
інформаційна система організації;
технологія управління безпекою корпоративної мережі на основі фаєрволу Palo Alto;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми захисту корпоративної мережі інформаційної системи.
2. Методи та засоби захисту корпоративної мережі організації.

3. Розроблення варіанту розгортання системи управління безпекою корпоративної мережі на основі фаерволу Palo Alto.

5. Перелік ілюстративного матеріалу:
Презентація PowerPoint

6. Дата видачі завдання 19.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Дослідження актуальності управління безпекою корпоративної мережі організації.	19.10.2023 р.	
2.	Аналіз наукової та технічної літератури за темою кваліфікаційної роботи.	22.10.2023 р.	
3.	Аналіз необхідності захисту комп'ютерної мережі організації.	27.10. 2023р.	
4.	Методи та засоби управління безпекою корпоративної мережі.	03.11.2023 р.	
5.	Розроблення варіанту розгортання системи управління безпекою корпоративної мережі на основі фаерволу Palo Alto.	15.11.2023 р.	
6.	Оформлення результатів дослідження. Проходження плагіату	26.11.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Здобувач(ка) вищої освіти _____ Андрій ЖУРАВЕЛЬ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Олександр КУЗНЄЦОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Журавель А.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія управління безпекою корпоративної мережі на основі фаерволу Palo Alto».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(*підпис*) (*Ім'я, ПРІЗВИЩЕ*)

Висновок керівника кваліфікаційної роботи

Здобувач ***ЖУРАВЕЛЬ Антон*** обрав тему роботи, метою якої було дослідити зміст технології управління безпекою корпоративної мережі. Перелік використаних джерел свідчить про вміння здобувача розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ЖУРАВЕЛЬ Антон*** показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ЖУРАВЛЯ Антона*** на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Олександр КУЗНЄЦОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) ***ЖУРАВЕЛЬ Антон*** допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Журавель Антон
на тему: «Технологія управління безпекою корпоративної мережі на основі фаерволу Palo Alto».

Актуальність:

Існує велика потреба в ефективних стратегіях та інструментах для безпечного управління Із зростанням технологічного розвитку також зростає кількість та складність кіберзагроз. Зловмисники постійно удосконалюють свої методи, і, отже, захист комп'ютерних мереж стає надзвичайно важливим для запобігання атакам, витокам даних та іншим загрозам. Захист мереж стає складнішим через зростання мобільності та віддаленої роботи. Змішана робоча модель, що включає в себе використання різних пристроїв та мереж, створює нові точки вразливості, які потребують уважного захисту. Організації все більше залежать від цифрових систем та зберігають значний обсяг критичної інформації в електронному вигляді. Це робить їх цільовими об'єктами для кіберзлочинців, і вимагає вдосконалення засобів захисту для запобігання можливим витокам чи крадіжкам даних. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено зміст проблеми управління безпекою корпоративної мережі.
2. Досліджено методи та засоби управління безпекою корпоративної мережі.
3. Запропоновано варіант технології управління безпекою корпоративної мережі на основі фаерволу Palo Alto.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У кваліфікаційній роботі доцільно було б більш детально описати різні методи та засоби управління безпекою корпоративної мережі.
2. Запропонований варіант варіант технології управління безпекою корпоративної мережі на основі фаерволу Palo Alto доцільно було б показати на прикладі конкретного підприємства.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку «**добре»**, а здобувач **ЖУРАВЕЛЬ Антон** - присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент: _____ _____
підпис *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 62 сторінки, 21 рисунок, 14 джерел.

Об'єкт дослідження – процес управління корпоративною мережею організації.

Предмет дослідження – технологія управління безпекою корпоративної мережі на основі фаерволу Palo Alto.

Мета роботи – розробити варіанти управління безпекою корпоративної мережі на основі фаерволу Palo Alto для інформаційної системи організації та рекомендації щодо застосування технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління безпекою корпоративної мережі на основі фаерволу Palo Alto.

В роботі проведено аналіз проблеми управління безпекою корпоративної мережі організації. Проаналізовано існуючі технології управління безпекою комп'ютерної мережі.

Досліджено методи та засоби управління безпекою корпоративної мережі.

Запропоновано варіант технології управління безпекою корпоративної мережі на основі фаерволу Palo Alto. Визначено призначення, основні функції та склад компонентів даної технології.

На основі проведених досліджень, в роботі розроблено варіант управління безпекою корпоративної мережі на основі фаерволу Palo Alto та рекомендації щодо забезпечення безпеки комп'ютерної мережі.

Галузь використання – кібербезпека корпоративної мережі.

КОМП'ЮТЕРНА МЕРЕЖА, КОРПОРАТИВНА МЕРЕЖА, БРАНДМАУЕР, БЕЗПЕКА, УПРАВЛІННЯ БЕЗПЕКОЮ

ABSTRACT

Text part of the master's qualification work:62 pages, 21 figures, 14 sources.

The object of research is the process of managing the organization's corporate network.

The subject of the study is the security management technology of the corporate network based on the Palo Alto firewall.

The purpose of the work is to develop security management options for the corporate network based on the Palo Alto firewall for the organization's information system and recommendations for the use of the technology.

Research methods – study of the literature on this topic, analysis of operating documentation, international standards and their comparison, modeling of the security management process of the corporate network based on the Palo Alto firewall.

The paper analyzes the problem of security management of the organization's corporate network. Existing computer network security management technologies are analyzed.

The methods and means of managing the security of the corporate network have been studied.

A variant of the corporate network security management technology based on the Palo Alto firewall is proposed. The purpose, main functions and composition of the components of this technology are defined.

On the basis of the conducted research, the paper developed an option for managing the security of the corporate network based on the Palo Alto firewall and recommendations for ensuring the security of the computer network.

The field of use is cyber security of the corporate network.

COMPUTER NETWORK, CORPORATE NETWORK, FIREWALL, SECURITY, TRAFFIC, SECURITY MANAGEMENT

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NGFW - Next Generation Firewall

HTTPS - HyperText Transfer Protocol Secure

TLS - Transport Layer Security

IoT - Internet of Things

PCI DSS - Payment Card Industry Data Security Standard

HIPAA - Health Insurance Portability and Accountability Act

NIST - National Institute of Standards and Technology

IPsec - IP Security

SSL - Secure Sockets Layer

VPN - virtual private network

DNS - Domain Name System-client

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

IPS - Intrusion Prevention System

ICMP - Internet Control Message Protocol

URL - Uniform Resource Locator

ВСТУП

Актуальність дослідження. З розвитком технологій зростає не лише кількість кіберзагроз, але й їхня складність. Захист корпоративної мережі стає надзвичайно важливим завданням для запобігання різноманітним атакам, від витоку даних до вимагань у викупі. Різноманітність та постійний розвиток технологій призводять до нових видів загроз, на які потрібно реагувати та впроваджувати нові захисні стратегії. Захист корпоративної мережі стає складнішим через поширення хмарних сервісів та збільшення кількості мобільних пристроїв, які взаємодіють з мережею. Кіберзлочинці стають більш винахідливими та використовують складні та цільовані тактики атак, такі як атаки "zero-day" та дії в тіньовому Інтернеті. Захист мережі від таких загроз вимагає постійного вдосконалення стратегій.

З огляду на зріст кількості загроз і кількість інцидентів безпеки, компанії стають більш свідомими важливості захисту корпоративної мережі. Усвідомленість допомагає виявляти недоліки і впроваджувати ефективні стратегії захисту. Технологія управління безпекою корпоративної мережі – це критичний елемент в інформаційній архітектурі будь-якої сучасної організації. Ефективне управління безпекою передбачає встановлення централізованої системи контролю, яка забезпечить єдність політик безпеки та моніторинг усіх точок в мережі. Ефективне управління доступом та використання сучасних методів ідентифікації, щоб гарантувати авторизований доступ до мережевих ресурсів.

Об'єкт дослідження – процес управління корпоративною мережею організації.

Предмет дослідження – технологія управління безпекою корпоративної мережі на основі фаерволу Palo Alto.

Мета роботи – розробити варіанти управління безпекою корпоративної мережі на основі фаерволу Palo Alto для інформаційної системи організації та рекомендації щодо застосування технології.

Наукові завдання:

- провести аналіз проблеми управління безпекою корпоративної мережі;
- проаналізувати основні загрози безпеки корпоративної мережі;
- проаналізувати методи та засоби управління безпекою корпоративної мережі;
- розробити варіант розгортання системи управління безпекою корпоративної мережі на основі фаєрволу Palo Alto та рекомендації щодо застосування даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління безпекою корпоративної мережі на основі фаерволу Palo Alto.

Практичне значення одержаних результатів полягає в розробці технології управління безпекою корпоративної мережі на основі фаерволу Palo Alto та рекомендації щодо застосування технології в організації.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

1.1. Аналіз проблеми захисту комп'ютерної мережі організації

Міжнародна організація стандартизації дає визначення безпеці комп'ютерної мережі. Це свого роду захист технології, встановленої та використовуваної для деяких систем обробки для захисту комп'ютерних даних програмного та апаратного забезпечення від знищення та витоку через деякі несподівані та злі причини. Визначення комп'ютерної безпеки включає фізичну безпеку та логічну безпеку [1]. Безпека мережі – це збереження цілісності та доступності інформації в Інтернеті. Цілісність, тобто забезпечення того, що несанкціоновані операції не можуть змінити дані. Ефективність, тобто забезпечення того, щоб несанкціоновані операції не могли знищити інформацію чи комп'ютерні ресурси. Тому, якщо говорити простіше, безпека мережевої системи включає безпеку мережі та безпеку інформації. Безпека мережі стосується безпеки фізичних ліній і з'єднань, спричинених роботою мережі та взаємозв'язком між мережами, безпекою операційної системи, безпекою управління персоналом тощо. Інформаційна безпека стосується безпеки даних, таких як конфіденційність, автентичність, доступність і контрольованість.

З широким використанням комп'ютерних технологій у різних сферах і просуванням системи автоматизації в роботі, традиційний режим роботи стає все більш викликом. Сучасне діловодство поступово розвивається в напрямку «безпаперового» та «мережевого». Особливо після комерціалізації Інтернету, Інтернет-індустрія досягла значного прогресу [2]. Інтернаціоналізація, відкритість та персоналізація інформаційної мережі не тільки забезпечують людям «обмін інформацією», але й забезпечують високу ефективність роботи та високу якість життя. Оскільки передача інформації не буде обмежена часом і простором, все

більше і більше комп’ютерів підключаються до мережі, і уряд і окремі особи поступово покладаються на мережеве середовище та мережеві ресурси. Однак проблема безпеки мережевої системи стає все більш і більш помітною і привертає все більше уваги. Витік, фальсифікація та підробка онлайн-інформації, розповсюдження вірусів і розповсюдження поганої інформації створюють дуже шкідливу загрозу для мережі. Отже, вирішення проблеми безпеки комп’ютерної мережі є невід’ємним.

Існує в основному два види проблем безпеки комп’ютера:

1) загрози інформації в системі;

2) загрози для обладнання в системі.

Існує багато факторів, які впливають на комп’ютерну систему, деякі з яких можуть бути навмисними, або мережевий зв’язок може бути ненавмисним, створеним людиною, не створеним людиною або спричиненим природним середовищем. Загалом, загрози безпеці комп’ютерних систем такі:

Крадіжка даних

Лазівки в безпеці, викликані неточною конфігурацією безпеки операторів, низьким рівнем безпеки користувачів або користувачами, які за власним бажанням позичають або діляться своїми обліковими записами з іншими, створюють загрозу безпеці мережі. Це призводить до втрати великої кількості даних. Втрата, спричинена втратою даних, невимірна. Конфіденційність і доступність можуть бути випадково порушені.

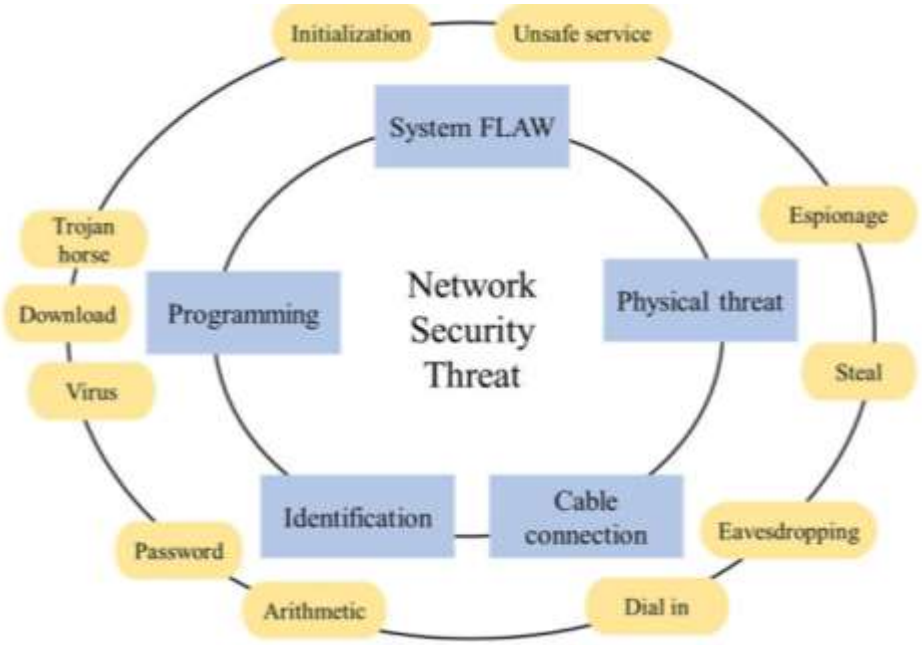

Рис.1.1. Типи загроз безпеці мережі.

Вразливості

Багато мережевих систем мають ті чи інші лазівки. Ці вразливості можуть належати системі. Крім того, він може бути сформований через недбалість керівництва. Ці вразливості можуть бути використані хакерами для здійснення різноманітних атак, включаючи виявлення пароля. Крім того, серед них поширеним методом є програмна атака. Хакери мають можливість незаконно отримати права суперкористувача комп'ютера та повністю контролювати його. Окрім роботи з файлами, він також може захоплювати зображення на робочому столі, отримувати паролі багатьох програм та виконувати деякі інші операції. На стороні клієнта та на стороні сервера є два типи цього програмного забезпечення. Коли хакери атакують, вони входитимуть за допомогою програм на стороні клієнта.

Мобільна загроза

Віруси для смартфонів становлять загрозу для корпоративних мереж і особистої інформації. З точки зору сучасної тенденції розвитку мережі, будь-який електронний продукт може бути підключений до мережі, і той факт, що мережа є всюди, свідчить про те, що атаки також є всюди. Крім того, будуть лазівки в

апаратному забезпеченні, операційній системі, обладнанні доступу до мережі та системі додатків. Використовуючи сховище мобільних пристроїв, життєвий простір і інкубаційний період шкідливого коду буде непередбачуваним.

Електромагнітні перешкоди

Високовольтні дроти, антени, що передають радіохвилі, високочастотне електронне обладнання мікрохвильової лінії тощо створюють сигнали електромагнітних перешкод. Ці сигнали електромагнітних перешкод знищують інформацію на магнітному носії комп'ютера, тим самим впливаючи на безпеку мережі.

Профілактичні заходи та прийоми формування проблем безпеки комп'ютерної мережі

Будь-яка мережева служба призведе до ризиків безпеки. проблема в тому, як мінімізувати ризик. На даний момент контрзаходи захисту безпеки мережі такі:

Створення безпечного мережевого середовища

Дуже важливо створити безпечне мережеве середовище, включаючи моніторинг користувачів, налаштування дозволів користувачів, використання контролю доступу, ідентифікації, моніторингу маршрутизаторів тощо.

Профілактика комп'ютерних вірусів.

Комп'ютерні віруси створюються штучно, використовуючи лазівки в комп'ютерному програмному забезпеченні. Завдяки швидкому розвитку комп'ютерів і появі нових вірусів швидкість передачі стає все швидшою і швидшою. Крім того, шкода стає все більш серйозною. Найпоширенішим запобіжним заходом проти комп'ютерних вірусів є встановлення антивірусного програмного забезпечення для перевірки та знищення файлів, заражених вірусом.

Існують також такі заходи для запобігання вірусу:

1) Не використовуйте програми та дані невідомого походження.

2) Не завантажуйте файли з невідомих веб-сайтів за бажанням.

3) Після завантаження файлу вилікуйте вірус перед його використанням.

4) Не легко відкривайте електронну пошту з адресою магазину невідомого походження (вкладення).

5) Часто робіть хорошу резервну копію важливих даних і так далі.

6) Слід часто встановлювати оновлення системи, щоб зменшити кількість вірусів, які використовують вразливі місця системи для атаки та знищення.

Технологія брандмауера

Брандмауер — це система, яка використовується для захисту мережевої безпеки різних хостів, користувачів або підмереж. Основною функцією брандмауера є реалізація та застосування політик безпечного доступу між різними підмережами. Брандмауер поділяє мережу користувача на різні підмережі відповідно до функції та рівня безпеки та здійснює контроль доступу через брандмауер. Інтранет є довірчою мережею. Він може отримати доступ до зовнішніх мереж, таких як Інтернет, через брандмауери. Він також може отримати доступ до мережі, яка надає послуги через брандмауер, тобто до спільної підмережі безпеки. Можна побачити, що через брандмауер ми можемо контролювати доступ між підмережами різних рівнів безпеки та запобігати зловмисному або неавторизованому доступу.

Шифрування даних

Оскільки мережеві хакери можуть вторгнутися в систему, викрасти дані або підслухати дані в мережі. Шифрування даних може зробити так, що викрадені дані не будуть просто відкриті, таким чином трохи зменшуючи втрати. На даний момент технологія шифрування є відносно розвиненою, і зазвичай використовуються два типи технологій шифрування:

1) технологія шифрування з симетричним ключем

2) технологія шифрування з відкритим ключем.

Цифровий підпис

Цифровий підпис можна використовувати для перевірки того, що повідомлення надано відправником. Крім того, коли цифровий підпис використовується для зберігання даних або програми, його можна використовувати для підтвердження цілісності даних або програми. Як і звичайні власноручні підписи, він має можливість використовуватися для перевірки достовірності інформації. 3.6. Цифровий сертифікат. У порівнянні з онлайн-ідентифікаційною

карткою, цифровий сертифікат використовує цифровий підпис для автентифікації особи в Інтернеті за допомогою авторизованої автентифікації третьої сторони, яка виконує функцію автентичності. Цифрові сертифікати безпечні, конфіденційні, захищені від підробки та ефективно захищають корпоративну інформацію.

1.2. Аналіз методів та засобів управління безпекою корпоративної мережі

Безпека мережі охоплює захист мереж і мережевого обладнання від атак. Однак це не обов'язково охоплює безпеку пристроїв, які використовують мережу — це також завдання безпеки кінцевої точки.

Залежно від розміру компанії та галузі процес захисту мережі відрізняється. Надійна безпека мережі виявляє аномалії, автентифікує користувачів, відокремлює пристрої та запобігає скомпрометації всієї мережі зараженими кінцевими точками.

Безпека мережі передбачає не тільки брандмауери та маршрутизатори, але й моніторинг активності, автентифікацію, шифрування та інші методи.

Хоча точні процеси захисту внутрішньої мережі відрізняються від компанії до компанії, деякі найкращі методи застосовуються майже в кожній ситуації.

Від інсайдерських загроз до зламаних облікових записів користувачів, багато проблем безпеки можна виявити шляхом моніторингу та аналізу використання мережі. Наприклад, пристрій, який раптово завантажує дані на повній швидкості 24/7, викликає занепокоєння. Це може бути викрадання даних або просто хтось поширює відеозапис. У будь-якому випадку, відстежуючи використання мережі, компанії можуть провести розслідування, поки не стане надто пізно.

Моніторинг і журналювання можна здійснювати за допомогою системи виявлення вторгнень. Залежно від мережевої інфраструктури організації це може мати форму програмного забезпечення або фізичного пристрою.

Щоб запобігти завданню значної шкоди зламаним пристроєм, обліковим записом або особою, фахівці з безпеки використовують принцип найменших привілеїв. У безпеці мережі це означає надання кожному пристрою якомога меншого доступу до інших пристроїв. Як приклад, спільні файли в мережевій

файловій системі мають бути доступні лише для тих, кому потрібен доступ для виконання своєї роботи.

Застосування принципу найменших привілеїв вимагає хорошого налаштування автентифікації. Організації, які вже перевіряють особу користувача на всіх ресурсах мережі, мають можливість легко заблокувати ці ресурси.

Шифрування запобігає перегляду чи зміні даних під час передачі через мережу. Щоб переконатися, що зловмисний або скомпрометований пристрій не зможе переглядати кожну інформацію, що передається в мережі, компаніям слід переконатися, що вони використовують шифрування під час передачі. Для веб-сайтів це відбувається у формі HTTPS, який використовує стандарт шифрування TLS для захисту даних у русі.

Багато компаній роблять помилку, не використовуючи HTTPS на сайтах внутрішньої мережі. На їхню думку, всі пристрої у внутрішній мережі є довіреними — припущення, яке руйнується, коли додається більше пристроїв. Хоча внутрішнє використання HTTPS трохи складніше, ніж зовнішнє, переваги безпеки є значними, особливо у великих мережах.

Кожна частина IT-інфраструктури, яка використовується у компанії, колись матиме вразливі місця. Якщо компаніям не вдається оновити мережеве обладнання, сервери та кінцеві точки, такі як ноутбуки та смартфони, хакери можуть отримати доступ набагато легше, ніж у повністю виправленій мережі.

Автоматизована технологія віддаленого керування — чудовий спосіб забезпечити своєчасне оновлення програмного забезпечення. Керування мобільними пристроями, поширена стратегія безпеки кінцевих точок, також має аналоги в безпеці мережі: маршрутизаторами, комутаторами та брандмауерами можна дистанційно керувати й оновлювати їх.

Практично все мережеве обладнання має можливість розділити фізичну мережу на кілька ізольованих підмереж. Ця функція безпеки може унеможливити доступ зламаного пристрою в одній підмережі до інших пристроїв або даних в інших частинах мережі.

Із розвитком продуктів Інтернету речей (IoT) у компаніях сегрегація мереж стає особливо корисною. Багато продуктів Інтернету речей надзвичайно легко зламати, тому їх слід зберігати в ділянці мережі, яка не містить критичних даних чи апаратного забезпечення.

Оскільки мережева інфраструктура зростає з новими програмами, серверами та мережевими пристроями, компаніям важко контролювати, керувати та перевіряти доступ користувачів.

Інструменти керування привілейованим доступом дозволяють компаніям контролювати привілейованих користувачів, таких як системні адміністратори, підрядники та сторонні особи, і централізувати доступ до мережевих пристроїв і серверів. Окрім підвищення безпеки шляхом увімкнення єдиного шлюзу доступу, адміністратори також можуть контролювати та записувати всі з’єднання та дії для відстеження змін, аудиту чи навчання.

З огляду на численні внутрішні та зовнішні стандарти безпеки мережі, здатність автоматизувати аудит мережі стала пріоритетом для багатьох організацій. Такі стандарти, як PCI DSS, SOX, NIS, HIPAA та ISO27001, мають індивідуальні вимоги до відповідності, які необхідно впроваджувати та контролювати, що може зайняти багато часу та напружити ресурси.

Багато інструментів аудиту мережі та контрольні списки все ще вимагають налаштування вручну, щоб забезпечити дотримання стандартів безпеки. Автоматизований моніторинг відповідності може заощадити час і спростити процедури аудиту відповідності.

Безпека мережі є важливою частиною арсеналу кібербезпеки будь-якої організації. Завдання кібербезпеки на рівні мережі полягає в тому, щоб не допустити зловмисників і зупинити атаки зі зламаних пристроїв усередині.

Незважаючи на її важливість, багато компаній не в змозі виділити належні ресурси для безпеки мережі. Проте надійна мережева безпека є свого роду страховим полісом від різноманітних дорогих і шкідливих кібератак, тому варто інвестувати в цей тип захисту.

Різноманітність стратегій — від таких простих, як своєчасне оновлення інфраструктури, до більш складних завдань, як-от реєстрація шаблонів трафіку та автоматизація перевірок відповідності — може серйозно підвищити безпеку в корпоративних мережах.

1.3. Аналіз стандартів захисту комп'ютерної мережі орагнізації

Стандарти безпеки мережі – це вказівки та найкращі практики, які допомагають організаціям захистити свої мережі від кібератак, витоку даних і несанкціонованого доступу. Вони охоплюють різні аспекти проектування мережі, конфігурації, управління та моніторингу та часто відповідають галузевим або нормативним рамкам. Розглянемо приклади безпеки мережі та використання стандартів безпеки мережі для вирішення типових проблем.

Перш ніж застосовувати стандарти мережевої безпеки, потрібно зрозуміти ризики та вразливості мережі. Це означає проведення оцінки мережевого ризику, який є процесом виявлення та оцінки потенційних загроз і впливу на мережеві активи, дані та операції. Оцінка мережевих ризиків може допомогти визначити пріоритети цілей безпеки мережі, узгодити їх із бізнес-цілями та вибрати стандарти безпеки мережі, які найбільше підходять для ситуації. Наприклад, постачальнику медичних послуг може знадобитися дотримуватися стандартів мережевої безпеки «Закон про перенесення та підзвітність медичного страхування» (HIPAA), спрямованих на захист конфіденційності та безпеки даних пацієнтів.

Після оцінки мережевих ризиків можна вибрати стандарти безпеки мережі на основі галузевих, нормативних та організаційних вимог. Доступно багато стандартів мережевої безпеки, таких як серія ISO/IEC 27000, NIST Cybersecurity Framework, CIS Controls і PCI DSS. Кожен стандарт безпеки мережі має власну сферу застосування, цілі та рекомендації щодо найкращих методів безпеки мережі. Наприклад, продавецю в Інтернеті, може знадобитися дотримуватися стандарту безпеки даних платіжних карток (PCI DSS), який є стандартом безпеки мережі, спрямованим на захист даних власників карток і платіжних операцій.

Після вибору стандартів безпеки мережі, потрібно запровадити їх у своєму мережевому середовищі. Це означає застосування засобів керування безпекою мережі та заходів, рекомендованих стандартами безпеки мережі, таких як шифрування, автентифікація, брандмауер, антивірус, резервне копіювання та аудит. Також потрібно задокументувати політику та процедури безпеки мережі та навчити мережевий персонал і користувачів, як їх дотримуватися. Наприклад, державній установі може знадобитися впровадити стандарти мережевої безпеки Федерального закону про управління інформаційною безпекою (FISMA), які вимагають створити та підтримувати програму мережевої безпеки, яка відповідає вказівкам і стандартам NIST.

Після того, як запровадили стандарти безпеки мережі, потрібно контролювати ефективність безпеки мережі та її відповідність. Це означає збір і аналіз мережевих даних і показників, таких як мережевий трафік, журнали, сповіщення, інциденти та звіти. Також потрібно проводити регулярні перевірки та перевірки мережі та за потреби оновлювати політику та процедури безпеки мережі. Наприклад, для фінансовоі установи може знадобитися стежити за дотриманням стандартів мережевої безпеки Закону Грамма-Ліча-Блілі (GLBA), які зобов’язують захищати конфіденційність і цілісність даних клієнтів і повідомляти клієнтів про будь-які дані порушення.

Після відслідковування ефективності безпеки мережі, потрібно вчитися на інцидентах безпеки мережі та покращити стан безпеки мережі. Це означає розслідування та вирішення будь-яких проблем із мережевою безпекою чи порушень, а також виявлення та впровадження основних причин і заходів для виправлення. Також потрібно поділитися уроками безпеки мережі та найкращими практиками з персоналом мережі та користувачами, а також отримати відгуки та пропозиції щодо покращення безпеки мережі. Наприклад, для навчальних закладів може знадобитися вчитися на інцидентах безпеки мережі та дотримуватися стандартів безпеки мережі Закону про сімейні права на освіту та конфіденційність (FERPA), які захищають конфіденційність і безпеку записів і даних студентів.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ PALO ALTO

2.1. Призначення, функції та можливості рішення Palo Alto Next-Generation Firewall

Next-Generation Firewall від Palo Alto Networks виявляють відомі та невідомі загрози, зокрема в зашифрованому трафіку, використовуючи дані, отримані в багатьох тисячах розгортань клієнтів. Це означає, що вони зменшують ризики та запобігають широкому спектру атак. Наприклад, вони дозволяють користувачам отримувати доступ до даних і програм на основі бізнес-вимог, а також зупиняють крадіжку облікових даних і здатність зловмисників використовувати викрадені облікові дані.

PANOS® — це програмне забезпечення, яке запускає всі брандмауери нового покоління Palo Alto Networks®. Використовуючи ключові технології, вбудовані в PANOS — AppID, ContentID, Device-ID та UserID — можна мати повну видимість і контроль над програмами, які використовуються всіма користувачами та пристроями в будь-якому місці, постійно. А оскільки вбудований ML, а також сигнатури програм і загроз автоматично перепрограмують брандмауер за допомогою найновіших інтелектуальних даних, можна бути впевненим, що весь дозволений трафік не містить відомих і невідомих загроз.

AIOps для NGFW поставляється з двома рівнями ліцензії: безкоштовно та преміум. AIOps для NGFW аналізує телеметрію пристрою та результати оцінки найкращих практик, щоб дати повне розуміння та профілактичні перевірки стану безпеки мережі. Преміальна ліцензія AIOps для NGFW також надає Хмарне керування для NGFW .

Функції безпеки

Безпечне ввімкнення додатків на основі користувачів і груп — це лише деякі з багатьох функцій, які підтримує кожен брандмауер наступного покоління Palo

Alto Networks. Гнучка мережева основа полегшує інтеграцію практично в будь-яку мережу. IPsec і SSL VPN забезпечують підключення до всього підприємства. Висока доступність із збереженням стану гарантує, що ваша мережа завжди захищена.

Видимість додатків, користувачів і вмісту

Номери портів, протоколи та IP-адреси корисні для мережевих пристроїв, але вони нічого не говорять про те, що є у мережі. Детальна інформація про програми, користувачів і вміст, що проходять через мережу, дає змогу швидко визначати будь-які ризики, які вони становлять, і швидко реагувати. Використовуючи багатий контекст, наданий міжмережевими екранами Palo Alto Networks, інструменти візуалізації, аналізу та звітування дозволяють швидко дізнатися більше про діяльність у мережі та проаналізувати інциденти з поточної чи порівняльної точки зору.

Видимість програм, веб-трафіку, загроз і шаблонів даних

Командний центр додатків (ACC) — це інтерактивне графічне резюме програм, користувачів, URL-адрес, загроз і вмісту, що охоплюють мережу. ACC забезпечує огляд того, що відбувається у мережі, і лише кількома клацаннями миші можна отримати детальне уявлення, щоб дізнатися більше, включаючи посилання на конкретну політику, яка дозволила певну поведінку, щоб можна було налаштувати її за потреби.

В ACC можна дізнатися більше про нові або незнайомі програми чи загрози, наприклад:

Опис програми або загрози.

Основні функції та поведінкові характеристики програми.

Відомості про користувачів, які використовують програму.

Детальна інформація про постраждалих від загрози.

Додаткові дані про джерело та призначення трафіку, правила безпеки та зони надають ширше уявлення про моделі використання програми, що допомагає прийняти більш обґрунтоване рішення про те, як обробляти цей трафік.

Видимість на основі користувачів і груп, а не IP-адрес

Інтеграція з широким спектром служб каталогів дозволяє системі відображати детальну інформацію про користувача (разом з його IP-адресою), доповнюючи отриману інформацію про програми та загрози. Можна додати додаткові фільтри, щоб дізнатися більше про використання програми окремими користувачами, а також про загрози, виявлені в трафіку програми. Лише за кілька хвилин ACC надає дані, необхідні для прийняття більш обґрунтованих рішень щодо політики безпеки та вжиття заходів для зменшення ризиків в організації.

Порівняльний погляд на моделі трафіку та загроз

App-Scope — це динамічне, настроюване вікно активності мережі, яке представляє порівняльну статистику на основі різних часових проміжків, програм, категорій програм, профілів загроз тощо. Стандартна функція як у веб-інтерфейсі нашого пристрою, так і в Panorama (централізоване керування), App-Scope зменшує кількість часу, який доведеться витрачати на дослідження незвичайної поведінки.

Детальний аналіз усього вашого трафіку та активності пристрою

Засіб перегляду журналів забезпечує детальне уявлення про мережеву активність. Він підсумовує весь трафік, що проходить мережею, включаючи програми, інформацію про користувачів і загрози. Засіб перегляду журналів підтримує фільтрацію на основі контексту та виразів, дозволяючи швидко й легко відстежувати, аналізувати та досліджувати інциденти безпеки. Засіб перегляду журналів використовує інтеграцію брандмауерів із сховищами користувачів, доповнюючи перегляд програм і загроз видимістю користувачів і груп. Журнали можна автоматично надсилати на сервер системного журналу, тоді як окремі результати фільтрів можна експортувати у файл CSV для автономного архівування або подальшого аналізу.

Індивідуальні звіти для всього трафіку та активності пристроїв

Використовуючи індивідуальний інтерфейс керування пристроєм брандмауера або Panorama, отримується доступ до потужних функцій звітування та журналювання, які допоможуть швидко розслідувати та аналізувати інциденти безпеки, використання програм і поведінку користувачів. Доступно понад 50 попередньо визначених звітів, які можна налаштувати, включаючи елементи, які

вибирається з інших звітів. Можна автоматизувати створення звітів за розкладом і надсилати результати електронною поштою або експортувати їх у формат PDF або Excel.

Видимість користувача:

Користувачі: невід'ємний компонент для політики активації безпечних програм. Традиційно політики безпеки застосовувалися на основі IP-адрес, але все більш динамічний характер користувачів і програм означає, що самі по собі IP-адреси стали неефективними як елемент контролю політики для безпечної роботи програм. Next-Generation Firewall інтегруються з широким спектром корпоративних каталогів і пропозицій термінальних служб, дозволяючи:

Подивитися, хто використовує програми у мережі

Встановити політику на основі користувачів

Виконувати криміналістичний аналіз і створювати звіти про дії користувачів

Видимість активності програми користувача

Видимість активності програми на рівні користувача, а не лише на рівні IP-адреси, дає змогу визначити моделі використання разом із пов'язаними бізнес-ризиками та ризиками безпеки. Дане рішення дає огляд пропускної здатності програми та споживання сеансу, пов'язаних загроз, а також джерела та призначення трафіку програми. Маючи ці знання, можна більш активно узгоджувати використання програм із вимогами організації за допомогою політик безпечного активування програм.

Керування політикою на основі користувача

Огляд використання додатків означає, що можна швидко проаналізувати роль і ризики додатків, а також те, хто їх використовує, а потім перевести цю інформацію в політику безпечного ввімкнення додатків на основі користувачів. Елементи керування політикою на основі користувача можна зібрати на основі програми, категорії та підкатегорії, до якої вона належить, її базової технології або характеристик програми. Приклади політик на основі користувачів можуть включати:

Дозвольте тільки IT-відділу використовувати такі інструменти, як SSH, telnet і FTP на стандартному порту

Дозвольте групі служби підтримки використовувати Messenger

Заблокувати використання Facebook-додатків для всіх користувачів, дозволити Facebook для всіх користувачів, але дозволити лише маркетингу використовувати Facebook-постинг

Аналіз, звітність і криміналістичний аналіз на основі користувачів

Інформація про користувача є широкою частиною набору функцій брандмауера, включаючи детальний криміналістичний аналіз і звітність. Можна легко створити фільтри журналу, клацнувши значення клітинки, яке потім можна розширити додатковими критеріями за допомогою конструктора виразів. Інформативні звіти про дії користувачів можна створювати за допомогою будь-якого з багатьох попередньо визначених звітів, або шляхом створення спеціального звіту з нуля, або шляхом зміни попередньо визначеного звіту. Будь-які звіти – попередньо визначені чи спеціальні – можна експортувати у CSV, PDF XML або надсилати електронною поштою за розкладом.

Інтеграція з будь-яким репозиторієм користувачів

Дані брандмауери можуть інтегруватися з широким списком репозиторіїв користувачів і пропозицій служб терміналів, які доповнюються API XML і явним механізмом відповіді на виклики. Точки інтеграції включають:

Служби каталогів: Microsoft Active Directory, Microsoft Exchange, OpenLDAP і eDirectory

Термінальні служби: Citrix XenAPP, Microsoft Terminal Services і XML API для нестандартних середовищ термінальних служб

Syslog Listener нативно збирає інформацію користувача з Blue Coat Proxy, Citrix Access Gateway, Aerohive AP, Cisco ASA, Juniper SA Net Connect і Juniper Infranet Controller

XML API: у випадках, коли слухач системного журналу недоступний, XML API дозволяє інтегрувати інформацію користувача у політики безпеки з інших каталогів користувачів і механізмів автентифікації.

Профілактика APT:

WildFire: захист від цілеспрямованих і невідомих загроз

Сучасні зловмисники все частіше використовують цільові та нові невідомі варіанти зловмисного програмного забезпечення, щоб пройти повз традиційні рішення безпеки. Щоб вирішити цю проблему, Palo Alto Networks розробила WildFire, яка визначає нове шкідливе програмне забезпечення за лічені хвилини. Запускаючи підозрілі файли у віртуальному середовищі та спостерігаючи за їх поведінкою, Palo Alto Networks швидко й точно визначає зловмисне програмне забезпечення, навіть якщо зразок зловмисного програмного забезпечення ніколи раніше не було виявлено.

Як тільки файл визнається шкідливим, WildFire автоматично створює засоби захисту, які надаються всім підписникам WildFire протягом години після виявлення. Ліцензія WildFire надає IT-команді безліч криміналістів, щоб точно визначити, хто був ціллю, програму, використану для доставки, і будь-які URL-адреси, які були частиною атаки.

Аналіз пісочниці невідомих загроз

Розширені кібератаки використовують приховані, стійкі методи, щоб уникнути традиційних заходів безпеки. WildFire визначає невідоме шкідливе програмне забезпечення, експлойти нульового дня та вдосконалені стійкі загрози (APT) за допомогою динамічного аналізу в масштабованому хмарному віртуальному середовищі. Palo Alto безпосередньо спостерігають за поведінкою зловмисного програмного забезпечення та експлойтів, а потім WildFire автоматично створює та розповсюджує захист у всьому світі всього за 30 хвилин.

Інтелект на основі DNS

DNS-трафік існує майже в кожній організації, створюючи величезний океан даних, які команди безпеки часто ігнорують або не мають інструментів для належного аналізу. Знаючи про це, кібер-зловмисники все частіше зловживають DNS, щоб маскувати свою командно-контрольну (C2) діяльність, щоб доставити додаткові шкідливі програми або викрасти цінні дані. Зловмисні доменні імена, контрольовані зловмисниками, дозволяють швидко переміщати командно-

контрольні центри з точки в точку, минаючи традиційні засоби безпеки, такі як чорні списки або веб-репутація. Palo Alto Networks вирішує це:

Дозволяє пасивний моніторинг DNS, створюючи базу даних шкідливих доменів та інфраструктури в глобальній клієнтській базі. Цей інтелект використовується фільтрацією URL-адрес PAN-DB, сигнатурами команд і керування на основі DNS і WildFire для запобігання майбутнім атакам.

Дозволяє клієнтам створювати локальні DNS-протоки, перенаправляючи шкідливі запити на адресу за вибором, щоб швидко ідентифікувати та блокувати скомпрометовані хости в локальній мережі.

Звіт про поведінковий ботнет

Звіт про поведінку ботнету співвідносить аномалії трафіку та поведінку кінцевих користувачів, щоб визначити пристрої у мережі, які, ймовірно, будуть заражені ботнетом. Логіка, що підтримує звіт, відстежує невідомі або аномальні TCP і UDP, а також різні потенційно підозрілі дії, такі як повторювані шаблони завантажень, використання динамічного DNS і аномалії перегляду. Ці фактори співвідносяться, щоб створити звіт, який надає список користувачів, які ймовірно інфіковані, і поведінку, яка призвела до діагностики.

IPS:

Сьогоднішні атаки на мережу використовують комбінацію прикладних векторів і експлойтів. Брандмауери наступного покоління Palo Alto Networks забезпечують двосторонній підхід до припинення цих атак. Небажані програми блокуються через App-ID, а програми, які дозволяються, скануються на наявність вразливостей нашою системою IPS, затвердженою NSS.

Повний захист IPS, зберігаючи продуктивність

Рішення забезпечує передбачувану продуктивність IPS завдяки апаратному прискоренню, уніфікованому формату підпису та однопрохідній архітектурі програмного забезпечення. Спеціальна обробка та пам’ять для перевірки вмісту, а також мережі, безпеки та керування забезпечують апаратне прискорення, необхідне для прогнозованої продуктивності IPS.

Спеціальна обробка означає, що ключові функції не конкурують за цикли обробки з іншими функціями безпеки, що відбувається в апаратній архітектурі одного ЦП або ASIC/ЦП.

Уніфікований формат підпису усуває надлишкові процеси, загальні для кількох рішень механізму сканування (повторна збірка TCP, пошук політики, перевірка тощо).

Програмне забезпечення за один прохід означає, що трафік торкається лише один раз, незалежно від того, скільки елементів політики використовується.

Блокує широкий спектр відомих і невідомих експлойтів уразливостей

Багатий набір функцій запобігання вторгненням блокує відомі та невідомі використання вразливостей на рівні додатків і мережі від компрометації та пошкодження корпоративних інформаційних ресурсів. Експлойти вразливостей, переповнення буфера та сканування портів виявляються за допомогою перевірених механізмів виявлення та запобігання загрозам (IPS), зокрема:

Аналіз на основі декодера протоколу повністю декодує протокол, а потім інтелектуально застосовує підписи для виявлення експлойтів уразливостей.

Захист на основі аномалій протоколу виявляє використання протоколу, несумісного з RFC, наприклад використання надто довгого URI або надто довгого входу до FTP.

Зіставлення шаблонів із визначенням стану виявляє атаки на кілька пакетів, враховуючи такі елементи, як порядок надходження та послідовність.

Статистичне виявлення аномалій запобігає лавинним атакам DoS на основі швидкості.

Евристичний аналіз виявляє аномальні шаблони пакетів і трафіку, такі як сканування портів і сканування хостів.

Пасивний моніторинг DNS для глобального виявлення та створення захисту для скомпрометованих доменів та інфраструктури, а також локальний синкхолінг DNS для перенаправлення зловмисних запитів на вибрану адресу для виявлення та блокування заражених хостів.

Інші можливості захисту від атак, такі як блокування недійсних або неправильно сформованих пакетів, дефрагментація IP-адреси та повторне збирання TCP, захищають вас від методів ухилення та обфускації, які використовують зловмисники.

Спеціальні сигнатури домашнього телефону щодо вразливостей або шпигунського програмного забезпечення, які можна використовувати в профілях захисту від шпигунського програмного забезпечення або захисту від вразливостей.

Захист від DoS/DDoS атак

Брандмауери наступного покоління Palo Alto Networks захищають від атак типу «відмова в обслуговуванні» (DoS), використовуючи підхід на основі політики, який забезпечує точне виявлення. Можна розгортати політики захисту від DoS на основі комбінації елементів, включаючи тип атаки, або за обсягом (як сукупно, так і класифіковано), з варіантами відповіді, включаючи дозвіл, попередження, активацію, максимальний поріг і скидання. Охоплені конкретні типи атак DoS включають:

Захист від переповнення — захищає вас від атак затоплення на основі SYN, ICMP, UDP та інших IP-атак.

Розвідувальне виявлення — дозволяє виявляти та блокувати сканування портів і сканування IP-адрес, які часто використовуються зловмисниками, щоб знайти потенційні цілі.

Захист від пакетних атак — захищає вас від великих пакетів ICMP і фрагментованих атак ICMP.

Виявлення та дослідження провідних загроз на ринку

Система запобігання вторгненням підтримується командою досвідчених розробників сигнатур. Команда Palo Alto дуже активна в спільноті запобігання загрозам, виконуючи постійні дослідження та тісно співпрацюючи з постачальниками програмного забезпечення – як неофіційно, так і офіційно – за допомогою таких програм, як Microsoft Active Protections Program (MAPP). Як учасник MAPP, ми маємо пріоритетний доступ до щомісячних і зовнішніх оновлень системи безпеки Microsoft.

Отримавши інформацію про вразливості на ранній стадії, Palo Alto Networks може розробити та надати підписи синхронізовано, щоб забезпечити повний захист. Оновлення підписів доставляються щотижнево або в екстреному порядку. На сьогоднішній день нашій команді приписують відкриття багатьох критичних і серйозних уразливостей у програмах Microsoft і Adobe.

Фільтрація даних і блокування файлів:

Контроль рівня функцій програми, блокування файлів за типом і функції фільтрації даних наших брандмауерів нового покоління дозволяють запроваджувати ряд політик, які допомагають збалансувати дозволи на використання особистих або неробочих програм із ризиками для бізнесу та безпеки. несанкціонованої передачі файлів і даних.

Увімкнення додатків із блокуванням несхвалених або небезпечних файлів за типом

Брандмауери наступного покоління дають можливість контролювати потік широкого діапазону типів файлів, дивлячись глибоко в корисне навантаження, щоб визначити тип файлу (на відміну від перегляду лише розширення файлу), щоб визначити, чи є передача файлу дозволено вашою політикою. Можна застосувати блокування файлів за типом для кожної програми. Це дає змогу робити такі дії, як схвалювати певну програму веб-пошти, наприклад Gmail, і дозволяти вкладення, але блокувати передачу певних типів файлів.

Увімкнення або заборона використання функцій передачі файлів

Контроль на функціональному рівні над передачею файлів представляє ще один параметр політики, який допомагає збалансувати використання програми з контролем політики. Можна встановити політики, щоб дозволити використання програми миттєвих повідомлень або веб-пошти, але заборонити відповідну функцію передачі файлів.

Запобігайте втраті даних за допомогою ідентифікації вмісту на основі шаблонів

Завершуючи функції фільтрації, є можливість ідентифікувати та контролювати передачу шаблонів конфіденційних даних, таких як номери

кредитних карток, номери соціального страхування або користувацькі шаблони даних у вмісті додатків або вкладеннях.

Мобільна безпека:

Мобільні обчислення є однією з найбільш руйнівних сил в інформаційних технологіях. Це революціонізує те, як і де працюють співробітники, а також інструменти, які вони використовують для виконання своєї роботи. Мобільні пристрої — це не просто засоби доступу до існуючих додатків, наприклад корпоративної електронної пошти, а платформа для відкриття абсолютно нових способів ведення бізнесу.

Фільтрування URL:

Ідеальним доповненням до контролю додатків на основі політики, який забезпечує App-ID, є вбудована база даних фільтрації URL-адрес, яка дає повний контроль над пов’язаною веб-активністю. Усуваючи недостатню видимість і контроль як з точки зору додатка, так і з точки зору веб-сайту, App-ID і URL-фільтрування разом захищають від повного спектру юридичних, регуляторних ризиків, ризиків продуктивності та використання ресурсів.

Вбудована база даних URL-адрес максимізує продуктивність і гнучкість

Фільтрування URL-адрес увімкнено за допомогою локального пошуку, а також запитів до головної бази даних у хмарі. Локальний пошук забезпечує максимальну вбудовану продуктивність і мінімальну затримку для URL-адрес, які найчастіше відкриваються, тоді як пошук у хмарі забезпечує охоплення найновіших сайтів. Поєднання контролю додатків і фільтрації URL-адрес дає змогу впроваджувати гнучкі політики для контролю діяльності співробітників і мережі.

Керуйте веб-переглядом на основі категорії або за допомогою налаштованих білих або чорних списків.

Укажіть групову політику перегляду веб-сторінок за допомогою інтеграції репозиторію користувачів, яку забезпечує ідентифікатор користувача.

Увімкніть політики розшифровки SSL, дозволивши зашифрований доступ до певних веб-сайтів, присвячених темам, які цікавлять співробітників, як-от здоров’я,

фінанси та покупки, одночасно розшифровуючи трафік до всіх інших сайтів, таких як блоги, форуми та розважальні сайти.

Увімкніть контроль пропускної здатності для визначених категорій, створивши політики QoS для вказаних категорій URL-адрес.

Настроювана база даних URL-адрес і категорії

Щоб врахувати унікальні шаблони трафіку, кеші на пристрої зберігають URL-адреси, до яких був останній доступ. Пристрої також можуть автоматично запитувати головну базу даних у хмарі щодо інформації про категорію URL-адрес, якщо URL-адресу не знайдено на пристрої. Результати пошуку автоматично вставляються в кеш для майбутньої діяльності. Також можна створити спеціальні категорії URL-адрес.

Настроювані сповіщення для кінцевого користувача

Є кілька способів повідомити кінцевих користувачів про те, що вони намагаються відвідати веб-сторінку, яка не відповідає корпоративній політиці.

Настроювана сторінка блокування: сторінка, яка інформує користувача про те, що він порушує політику, може містити корпоративний логотип, посилання на ім’я користувача, IP-адресу, URL-адресу, до якої намагається отримати доступ, і категорію URL-адреси.

Блокування фільтрації URL-адрес і продовження: користувачі, які відкривають сторінку, яка потенційно порушує політику фільтрації URL-адрес, бачать сторінку блокування з кнопкою «Попередження та продовження».

Перевизначення фільтрації URL-адреси: вимагає від користувача правильного введення пароля, щоб обійти заблоковану сторінку та продовжити перегляд.

Гнучкий контроль над використанням Інтернету на основі політики

Щоб доповнити видимість додатків і контроль, який забезпечує ідентифікатор додатка, можна використовувати категорії URL як критерії відповідності для своїх політик. Замість створення політик, обмежених "дозволити все або заблокувати" будь-яку поведінку, URL як критерій відповідності дозволяє поведінку на основі винятків. Це підвищує гнучкість і дає більш детальні

можливості застосування політики. Приклади використання категорій URL-адрес у політиці:

Визначте та дозвольте винятки з ваших загальних політик безпеки для користувачів, які можуть належати до кількох груп у межах Active Directory (наприклад, заборонити доступ до зловмисного програмного забезпечення та хакерських сайтів для всіх користувачів, але дозволити доступ користувачам, які належать до групи безпеки).

Застосуйте політику фільтрації URL-адрес до кешованих результатів, коли кінцеві користувачі намагаються переглянути кешовані результати пошуку Google і Інтернет-архіву.

Застосуйте політику фільтрації URL-адрес до URL-адрес, які вводяться на сайтах перекладу, наприклад Google Translate, щоб обійти політики.

Застосуйте безпечний пошук, щоб запобігти появі неприйнятного вмісту в результатах пошуку користувачів. Якщо цю функцію ввімкнено, будуть дозволені лише пошукові запити Google, Yahoo або Bing із найсуворішим набором параметрів безпечного пошуку; усі інші пошуки будуть заблоковані.

Дозвольте доступ до категорії потокового медіа, але застосуйте QoS, щоб контролювати споживання пропускної здатності.

Заборонити завантаження/завантаження файлів для категорій URL-адрес, які становлять підвищений ризик (наприклад, дозволити доступ до невідомих сайтів, але заборонити завантаження/завантаження виконуваних файлів із невідомих сайтів, щоб обмежити розповсюдження шкідливих програм).

Застосуйте політики дешифрування SSL, які дозволяють зашифрований доступ до категорій фінансів і покупок, але розшифровують і перевіряють трафік для всіх інших категорій.

Мережевий захист від шкідливих програм

Розширення використання соціальних медіа, обміну повідомленнями та інших програм, не пов’язаних із роботою, створює різноманітні вектори для вірусів, шпигунського програмного забезпечення, черв’яків та інших типів шкідливого програмного забезпечення. Брандмауери наступного покоління Palo

Alto Networks дозволяють блокувати небажані програми за допомогою App-ID, а потім сканувати дозволені програми на наявність шкідливих програм.

Широкий захист від низки шкідливих програм

Наш антивірусний механізм виявляє та блокує віруси, шпигунське програмне забезпечення, завантаження шпигунського програмного забезпечення, ботнет, черв'яків і троянів. Додаткові функції, крім захисту мережі від широкого спектру загроз, включають:

Вбудований потоковий захист від шкідливих програм, вбудованих у стислі файли та веб-вміст

Аналіз ботнету на основі DNS для виявлення мереж зловмисного програмного забезпечення та веб-сайтів, що швидко розвиваються

Захист від HTML і шкідливого Javascript

Використовує дешифрування SSL у App-ID для блокування вірусів, вбудованих у трафік SSL

Потокове сканування

Антивірусна система Palo Alto Networks використовує сканування на основі потоку, щоб перевірити трафік, щойно отримано перші пакети файлу. Це усуває проблеми з продуктивністю та затримкою, пов'язані з традиційним підходом на основі проксі або файлів. Як і в IPS, для сканування на віруси використовується уніфікований формат сигнатур, що усуває надлишкові процеси, загальні для кількох рішень механізму сканування (повторна збірка TCP, пошук політики, перевірка тощо).

Постійне дослідження та оновлення шкідливих програм

Сигнатури для всіх типів зловмисного програмного забезпечення генеруються безпосередньо з мільйонів живих зразків вірусів, доставлених Palo Alto Networks провідними сторонніми дослідницькими організаціями по всьому світу. Команда Palo Alto аналізує зразки та швидко усуває дублікати та надлишки. Потім генеруються нові сигнатури для нових варіантів зловмисного програмного забезпечення (з використанням нашого єдиного формату сигнатур) і доставляються через щоденні заплановані або екстрені оновлення.

Захист мережі від загроз, які поширюються через завантаження

Нічого не підозрюючи користувачі можуть ненавмисно завантажити зловмисне програмне забезпечення, просто відвідавши свою улюблену веб-сторінку та натиснувши зображення. Цей механізм доставки зловмисного програмного забезпечення, який стає все більш популярним, відомий як «завантаження за допомогою приводу». Брандмауери нового покоління Palo Alto Networks контролюють цю загрозу, ідентифікуючи завантаження зловмисного програмного забезпечення та надсилаючи попередження вашому користувачеві, щоб переконатися, що завантаження бажане.

2.2. Архітектура Palo Alto Next-Generation Firewall

Брандмауер наступного покоління Palo Alto Networks (NGFW) відрізняється від конкурентів своєю платформою, процесом і архітектурою. Palo Alto Networks надає всі функції брандмауера наступного покоління, використовуючи єдину платформу, паралельну обробку та єдину систему керування, на відміну від інших постачальників, які використовують різні модулі або декілька систем керування, щоб пропонувати функції NGFW.

Брандмауер нового покоління Palo Alto Networks головною перевагою якого є архітектура однопрохідної паралельної обробки (SP3), яка складається з двох ключових компонентів:

Програмне забезпечення Single Pass

Апаратне забезпечення паралельної обробки

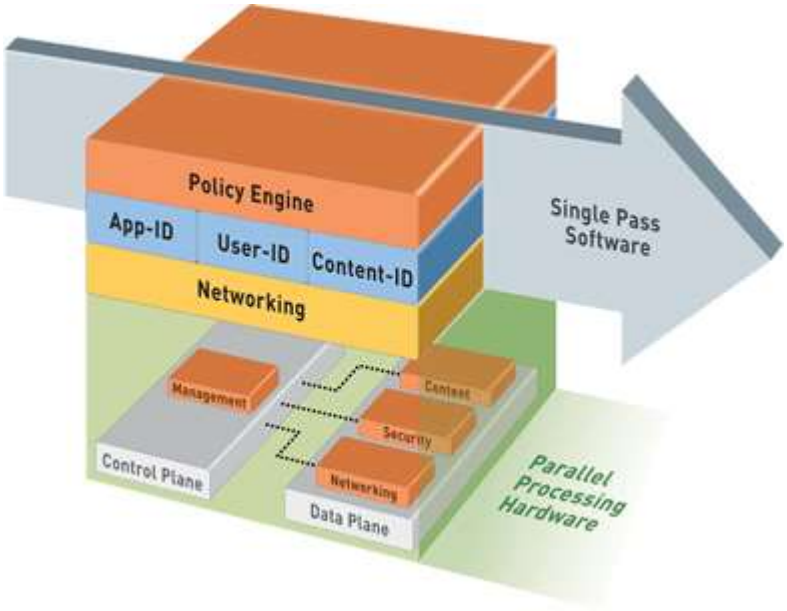

Рис.2.1. Однопрохідна архітектура паралельної обробки брандмауера Palo Alto Networks

Програмне забезпечення Single Pass

Брандмауер наступного покоління Palo Alto Networks оснащено програмним забезпеченням Single Pass, яке обробляє пакет для виконання таких функцій, як робота в мережі, ідентифікація користувача (User-ID), пошук політики, класифікація трафіку з ідентифікацією програми (App-ID), декодування, зіставлення сигнатур для виявлення загроз і вмісту, які усі виконуються один раз на пакет, як показано на рис.2.2.:

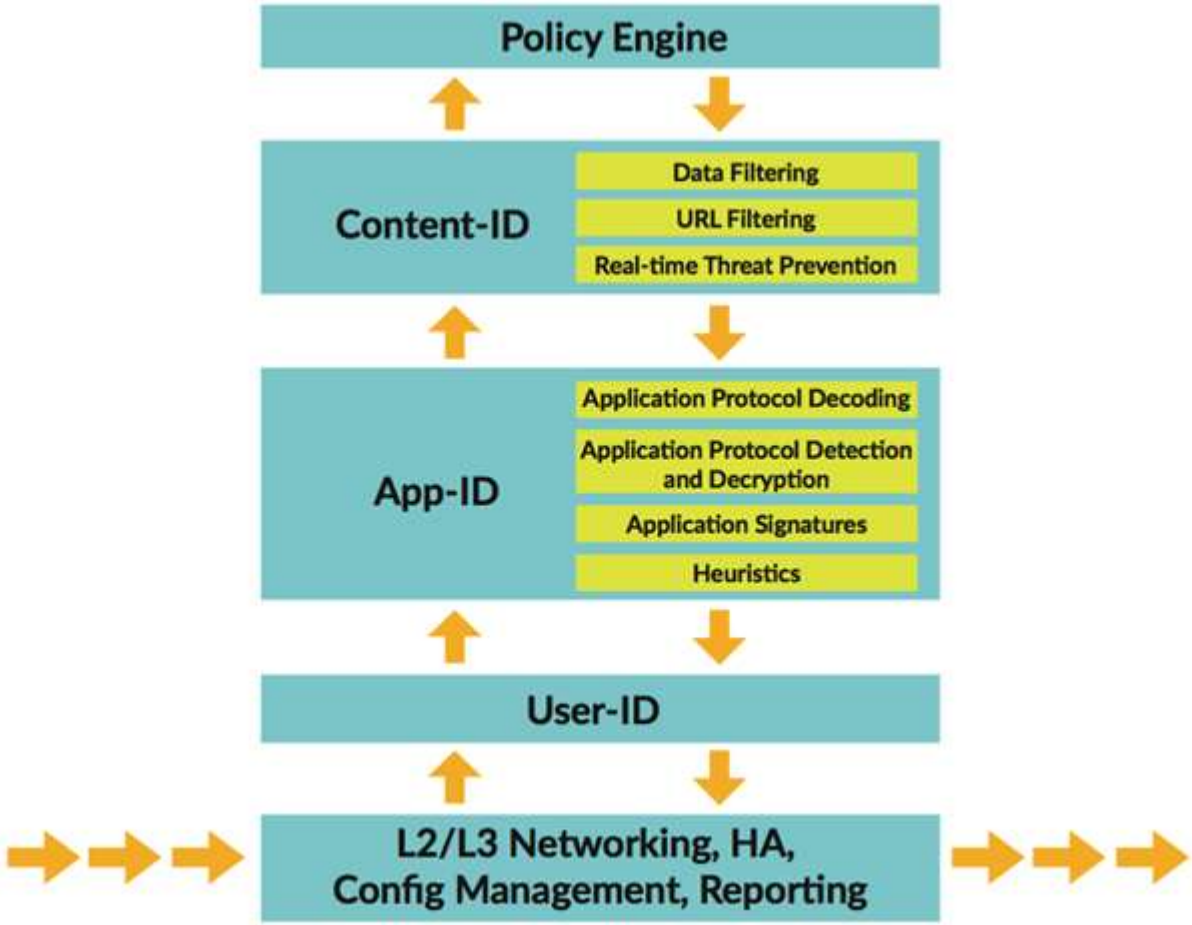

Рис.2.2. Мережевий брандмауер Palo Alto Networks – однопрохідний архітектурний потік трафіку

Така обробка пакета за один раз або за один прохід брандмауером наступного покоління Palo Alto Networks значно зменшує накладні витрати на обробку, інші брандмауери постачальників, які використовують інший тип архітектури, створюють значно вищі накладні витрати під час обробки пакетів, що проходять через брандмауер. Було помічено, що Уніфіковане управління загрозами (UTM), яке обробляє трафік за допомогою багатопрохідної архітектури, призводить до накладних витрат на процес, появи затримок і зниження пропускної здатності.

На рис.2.3. показано процес багатопрохідної архітектури, який використовується брандмауерам інших постачальників, чітко показуючи відмінності від архітектури брандмауера Palo Alto Networks і те, як створюється накладна обробка:

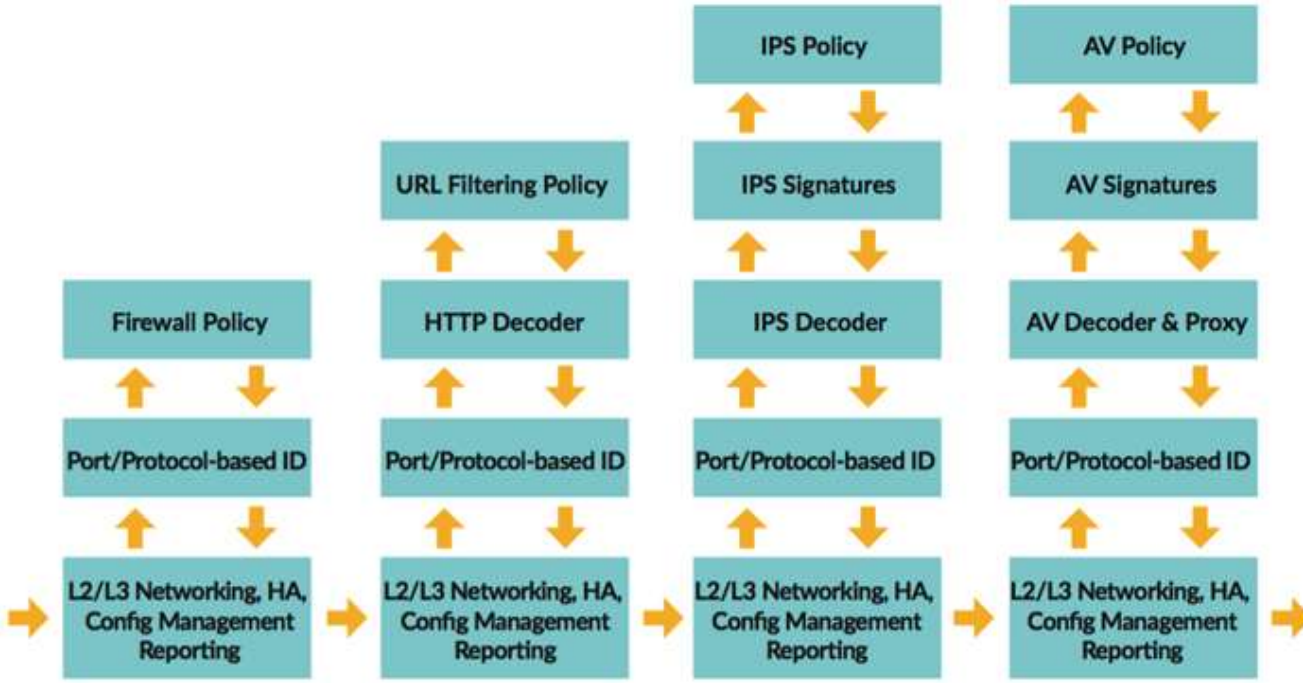

Рис. 2.3. Потік трафіку для багатопрохідної архітектури, що призводить до додаткової накладної обробки

Програмне забезпечення брандмауера наступного покоління Palo Alto Networks Single Pass сканує вміст на основі одного потоку та використовує уніфіковані шаблони відповідності сигнатур для виявлення та блокування загроз. Застосовуючи цю методологію, брандмауер наступного покоління Palo Alto Networks відмовляється від використання окремих механізмів сканування та наборів підписів, що призводить до низької затримки та високої пропускної здатності.

Апаратне забезпечення паралельної обробки

Апаратне забезпечення паралельної обробки Palo Alto Networks забезпечує паралельну обробку певних функцій на апаратному рівні, що в поєднанні зі спеціальною площиною даних і площиною керування забезпечує приголомшливі результати продуктивності. Розділивши площину даних і площину керування, Palo Alto Networks гарантує, що інтенсивне використання обох площин не вплине на загальну продуктивність платформи. У той же час це означає, що немає ніякої залежності від жодної площини, оскільки кожна має свій власний процесор і оперативну пам’ять, як показано на діаграмі нижче:

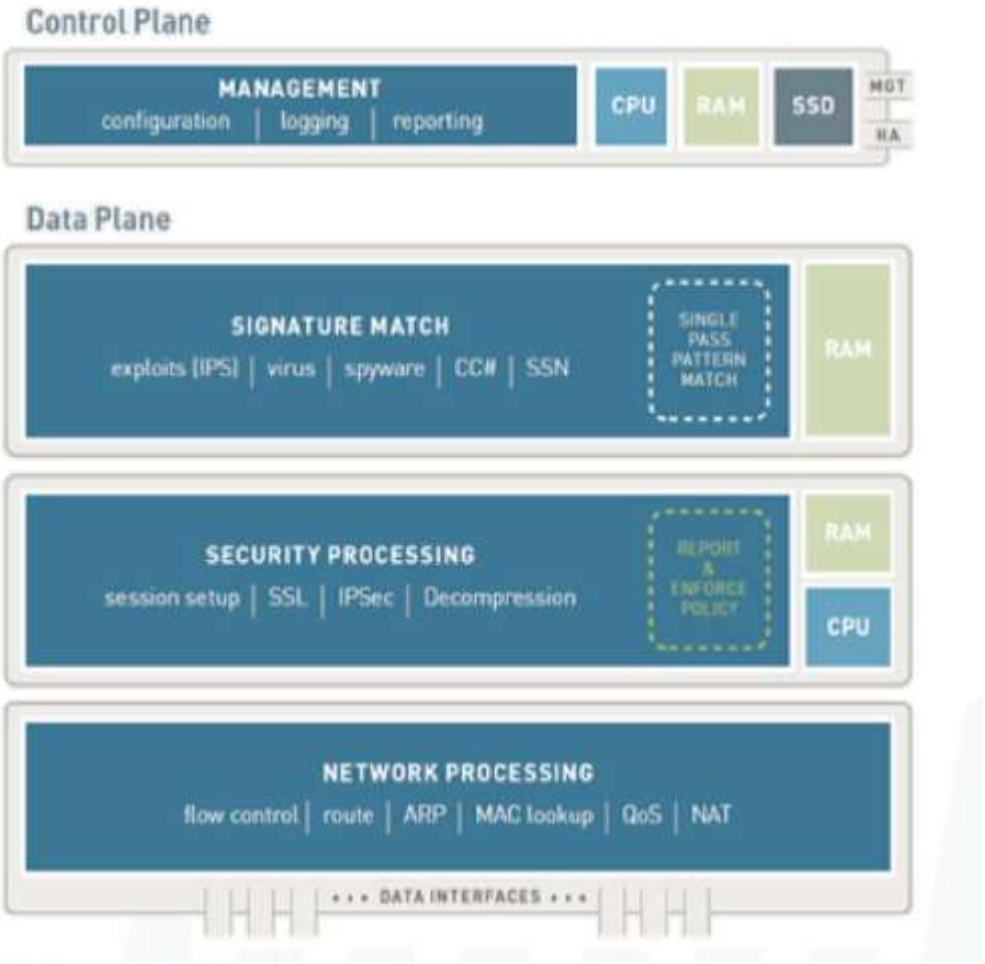

Рис.2.4. Апаратна архітектура брандмауера Palo Alto Networks – розділення площини даних і площини керування

Площина керування відповідає за такі завдання, як керування, конфігурація брандмауера наступного покоління Palo Alto Networks, а також функції журналювання та звітування.

Брандмауер наступного покоління Palo Alto Networks пропонує процесори, призначені для певних функцій, які працюють паралельно. Площина даних у моделях високого класу містить три типи процесорів (CPU), з'єднаних високошвидкісними шинами 1 Гбіт/с.

Існує три типи процесорів:

Процесор відповідності безпеки: виділений процесор, який виконує виявлення вразливостей і вірусів.

Процесор безпеки: виділений процесор, який виконує апаратне прискорення та виконує завдання безпеки, такі як розшифровка SSL, розшифровка IPsec тощо.

Мережевий процесор: Виділений процесор, який відповідає за такі функції мережі, як маршрутизація, NAT, QOS, пошук маршруту, пошук MAC-адреси та комунікації мережевого рівня.

Унікальна архітектура та дизайн Palo Alto Networks зіграли значну роль у тому, щоб виділити його серед інших конкурентів. Його єдина платформна архітектура паралельної обробки в поєднанні з єдиною системою керування створює швидкий і високотехнологічний брандмауер наступного покоління, який не залишиться позаду найближчим часом.

2.3. Переваги рішення Palo Alto Next-Generation Firewall

Стрімкий розвиток IT змінив вигляд мережевого периметра. Дані всюди, користувачі мають доступ до них з будь-якого місця та з усіх видів пристроїв. Водночас IT-відділи використовують хмарні технології, аналітику та автоматизацію, щоб пришвидшити доставку нових додатків і стимулювати розвиток бізнесу. Ці фундаментальні зміни створили ландшафт загроз, який розкриває слабкі місця в застарілих технологіях безпеки, таких як безпека мережі на основі портів, або різні інструменти та технології, які не інтегровані на початковому етапі. Ці інструменти не були розроблені для автоматизації та вимагають від аналітиків вручну об’єднати статистичні дані з багатьох від’єднаних джерел, перш ніж діяти.

Брандмауер Palo Alto дозволяє перевіряти весь трафік, включаючи всі програми, загрози та вміст, і прив’язувати цей трафік до користувача, незалежно від місця розташування чи типу пристрою.

Next-Generation Firewall дозволяє організаціям:

Безпечно дозволяти користувачам, контенту та програмам, у тому числі програмам програмного забезпечення як послуги (SaaS), класифікуючи весь трафік незалежно від порту.

Зменшити ризик атаки за допомогою позитивної моделі примусового виконання — дозволяючи всі потрібні програми та блокуючи все інше.

Застосовувати політики безпеки, щоб блокувати відомі експлойти вразливостей, віруси, програми-вимагачі, шпигунські програми, бот-мережі та інше невідоме зловмисне програмне забезпечення, наприклад розширені постійні загрози (APT).

Захистітити центри обробки даних, включаючи віртуалізовані центри обробки даних, шляхом сегментації даних і додатків, а також застосування Zero Trust.

Застосувати стабільний захист у локальному та хмарному середовищах, а також у філіях.

Скористатися безпечними мобільними обчисленнями, розширивши захист користувачів і пристроїв незалежно від їх розташування.

Отримати централізовану видимість і оптимізувати мережеву безпеку, роблячи величезні обсяги даних активними, щоб мати можливість запобігати кібератакам.

Ключові можливості Next-Generation Firewall

Zero Trust

Звичайні моделі безпеки ґрунтуються на застарілому припущенні, що можна довіряти всьому в мережі організації. Ці моделі призначені для захисту периметра. Водночас загрози, які проникають у мережу, залишаються непоміченими та можуть скомпрометувати конфіденційні та цінні бізнес-дані. У цифровому світі довіра – це не що інше, як вразливість.

Нульова довіра це стратегія кібербезпеки, яка усуває поняття довіри. У світі нульової довіри немає довірених пристроїв, систем або людей. Організації визначають дані, активи, програми та послуги, які є найбільш критичними для бізнесу, визначається, хто або що має мати доступ на основі їхніх конкретних посадових функцій, і забезпечується застосування моделі найменш привілейованого доступу за допомогою сегментації мережі, детальної політики безпеки рівня 7 , контроль доступу користувачів і запобігання загрозам.

Next-Generation Firewall безпосередньо відповідають принципу Zero Trust, зокрема забезпечують безпечний доступ для всіх користувачів незалежно від місця розташування, перевіряють увесь трафік, застосовують політики для контролю доступу з найменшими привілейами, а також виявляють і запобігають розширеним загрозам. Це значно скорочує шляхи доступу зловмисників до критично важливих активів, незалежно від того, перебувають вони в організації чи за її межами.

Ідентифікація користувачів і захист ідентичності користувачів

Технології ідентифікації користувача дає змогу брандмауерам наступного покоління ідентифікувати користувачів у будь-якому місці, незалежно від типу їх пристрою чи операційної системи. Видимість активності додатків — на основі користувачів і груп, а не IP-адрес — безпечно вмикає додатки, узгоджуючи використання з бізнес-вимогами. Можна визначити політики доступу до програми на основі користувачів або груп користувачів. Наприклад, дозволити лише IT-адміністраторам використовувати такі інструменти, як Secure Shell, Telnet і File Transfer Protocol. Політика стежить за користувачами незалежно від того, куди вони йдуть — у штаб-квартирі, філії чи вдома — і на будь-яких пристроях, які вони можуть використовувати. Крім того, можна використовувати спеціальні або попередньо визначені параметри звітності для створення інформативних звітів про дії користувачів.

Однак проблема ідентифікації користувача виходить за межі політики та звітності, що базуються на користувачах. Не менш важливим є захист особистих даних користувача. Згідно з даними Forrester Research, щонайменше 80% порушень даних пов’язані з скомпрометованими привілейованими обліковими даними. Зловмисники використовують викрадені облікові дані, щоб отримати доступ до мереж організацій, де вони знаходять цінні програми та дані, які вони можуть викрасти. Щоб запобігти атакам на основі облікових даних, брандмауери дають змогу:

Блокувати доступ до відомих фішингових сайтів через URL фільтрація, використання останніх глобальних даних про загрози, які оновлюються кожні п’ять хвилин, щоб захистити користувачів від спроб викрадення їхніх облікових даних.

Заборонити користувачам надсилати корпоративні облікові дані до невідомі сайти, захищаючи їх від цілеспрямованих атак, які використовують нові невідомі фішингові сайти, щоб залишитися непоміченими.

Дозволяє застосувати багатофакторну автентифікацію (MFA) для будь-якої програми, яка вважається конфіденційною, включно зі застарілими програмами, які важко піддаються MFA. Це захистить, якщо зловмисник уже володіє вкраденими обліковими даними. Можна використовувати цю можливість із вибраним постачальником ідентифікаційної інформації, включаючи Ping Identity, Okta, RSA та Duo Security.

Автоматизуйте відповіді, які адаптують і слідують поведінці користувачів за допомогою динамічних груп користувачів (DUG). Незалежно від того, чи скомпрометовано облікові дані користувача чи потрібно надати тимчасовий доступ користувачам, DUG дають змогу використовувати дані про поведінку користувачів ізCortex XDR™, аналітику поведінки користувачів і об’єктів (UEBA) і системи керування інформацією та подіями безпеки (SIEM) для автоматичного застосування політик безпеки в реальному часі.

Безпечне ввімкнення програм

.Технологія App-ID в брандмауерах наступного покоління точно визначає програми в усьому трафіку, що проходить через мережу, включаючи програми, замасковані під авторизований трафік, які використовують динамічні порти або намагаються сховатися під завісою шифрування. App-ID дозволяє розуміти та контролювати програми та їхні функції, такі як потокове відео чи чат, завантаження чи завантаження, спільний доступ до екрана чи віддалене керування пристроєм тощо.

Характеристики програми SaaS дозволяють зрозуміти використання програми. Наприклад, можна визначити, які програми SaaS, доступ до яких здійснюється з організації, не мають необхідних сертифікатів або мають історію порушень даних. Можна дозволити доступ до санкціонованих корпоративних облікових записів у програмах SaaS, наприклад Microsoft 365™, одночасно

заблокувавши доступ до несанкціонованих облікових записів, зокрема особистих/споживацьких облікових записів.

За допомогою оптимізатора політики можна посилити безпеку, усунувши небезпечні прогалини в політиці, створені застарілими політиками брандмауера. Оптимізатор політики допомагає команді безпеки легко замінити усталені правила інтуїтивно зрозумілими політиками на основі програм. Оскільки правила на основі App ID легко створювати, розуміти та змінювати в міру розвитку потреб бізнесу, вони зводять до мінімуму помилки конфігурації. Ці політики посилюють безпеку та потребують значно менше часу для керування.

Організації покладаються на численні джерела аналізу загроз, щоб забезпечити найширшу видимість невідомих загроз, але їм важко агрегувати, співвідносити, перевіряти та ділитися цією інформацією, щоб забезпечити захист у своїй мережі. WildFire виявляє невідомі загрози за допомогою даних глобальної спільноти та автоматично їх блокує; AutoFocus - це служба розвідки, яка надає інформацію про контекст, агрегацію та атрибуцію, щоб служби безпеки могли швидше реагувати; а Cortex XDR виявляє внутрішні загрози та координує цю інформацію з WildFire.

Крім того, WildFire підтримує брандмауери наступного покоління з оцінкою трафіку шляхом аналізу невідомих загроз і застосування високоточного автоматизованого захисту в мережевих, мобільних і хмарних середовищах.

Наприклад, якщо брандмауер наступного покоління або кінцева точка клієнта в Сінгапурі стикається з підозрілим файлом, цей файл надсилається в WildFire для розширеного аналізу. Результати аналізу, включаючи вердикти та захисти, потім автоматично надсилаються клієнту в Сінгапурі, а також усім іншим клієнтам WildFire у всьому світі.

Управління мережевою безпекою

Контроль доступу Panorama на основі ролей (RBAC) у поєднанні з попередніми та пост-правилами дозволяє збалансувати централізований нагляд із необхідністю редагування локальної політики та гнучкості конфігурації пристрою. Центр керування додатками (ACC) і можливості керування журналами створюють

єдине скло для ефективної видимості на кількох пристроях, незалежно від того, де вони розгорнуті. Додаткова підтримка інструментів на основі стандартів, таких як простий протокол керування мережею (SNMP) і API на основі REST, дозволяє легко інтегрувати інструменти керування сторонніх виробників.

Нативно інтегрована SD-WAN

Оскільки все більше підприємств впроваджують цифрову трансформацію та переміщують додатки в хмару, IT-командам постає завдання швидко, надійно та безпечно підключати корпоративних і віддалених користувачів до критично важливих бізнес-ресурсів.

Незважаючи на те, що технологія програмно визначеної глобальної мережі (SD-WAN) обіцяє збільшити пропускну здатність і покращити взаємодію з користувачем, організації повинні бути обережними, щоб не поставити під загрозу безпеку, продуктивність або простоту. Брандмауери нового покоління Palo Alto Net-works дозволяють IT-командам легко адаптувати наскрізну архітектуру SD-WAN із вбудованою безпекою світового рівня та підключенням. Використовуючи Prisma Access як центр SD-WAN, ви можете мінімізувати затримку та забезпечити надійність для оптимізації продуктивності всієї вашої мережі, забезпечуючи виняткову взаємодію з користувачами у своїх відділеннях.

Palo Alto Networks підтримує кілька варіантів розгортання SD-WAN, у тому числі розгортання на основі сітки, концентратора та розгортання в хмарі.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ БЕЗПЕКОЮ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ PALOALTO NEXT-GENERATION FIREWALL

3.1. Розроблення варіанту розгортання системи захисту управління безпекою корпоративної мережі на основі PaloAlto

Розгортання брандмауера PaloAlto в Google Cloud

Брандмауер PaloAlto Networks VM-Series є віртуалізованою формою брандмауера наступного покоління PaloAlto Networks. Він призначений для використання у віртуалізованому або хмарному середовищі, де він може захищати трафік схід-захід і північ-південь.

На рис. 3.1. показано компоненти, необхідні для захисту мережевого трафіку за допомогою брандмауера серії VM.

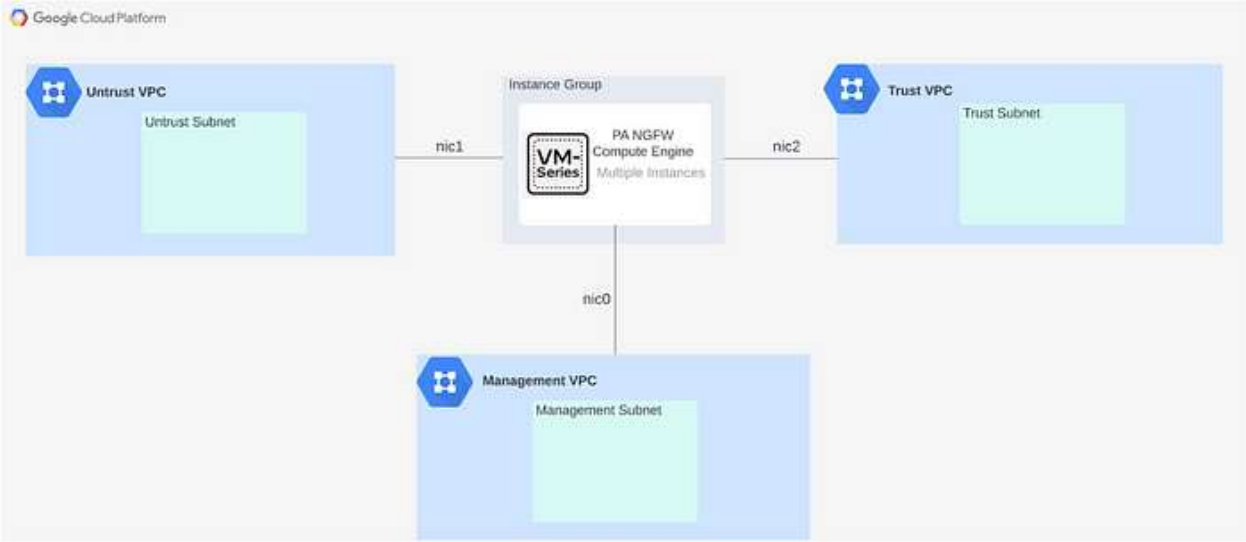

Рис.3.1. Основні компоненти брандмауера

Компоненти:

Довіра/внутрішня мережа

Довірчий інтерфейс VM-Series підключено до приватної мережі VPC. Щоб забезпечити високу доступність, рекомендовано встановити довірчий інтерфейс як серверну частину внутрішнього балансувальника навантаження TCP/UDP.

Приватна мережа VPC має маршрут за замовчуванням, який вказує або на інтерфейс довіреної мережі, або на внутрішній балансувальник навантаження TCP/UDP як наступний стрибок. Зазвичай приватна мережа VPC використовується як:

Спільна мережа VPC, яка делегує свої підмережі проектам обслуговування організації.

Центральна мережа VPC, яка забезпечує транзитивну маршрутизацію та перевірку для кількох мереж VPC.

Недовіра/Зовнішня мережа

Ненадійний інтерфейс VPC служить інтернет-шлюзом для ресурсів, розгорнутих у приватній мережі. Щоб увімкнути вихідне підключення до Інтернету з приватної мережі VPC, приєднайте зовнішню IP-адресу до ненадійного інтерфейсу або скористайтеся хмарним NAT для загальнодоступної мережі VPC. Для вхідного інтернет-з'єднання з ресурсами приватної мережі можна досягти розподілу трафіку та високої доступності, налаштувавши інтерфейси, щоб вони слугували сервером зовнішнього балансувальника навантаження.

Мережа управління

Інтерфейс керування є основним мережевим інтерфейсом екземпляра Compute. IP-адреса інтерфейсу керування надає доступ до інтерфейсу користувача VM-Series і консолі терміналу.

Наразі Palo Alto Networks підтримує два типи ліцензій:

Принесіть власну ліцензію (BYOL)

PAYGO (оплата по ходу)

Він також підтримує такі дві моделі ліцензування:

Кредити брандмауера нового покоління програмного забезпечення:

Доступно для брандмауерів серії VM, які працюють у всіх версіях PAN-OS. Брандмауери серії VM під керуванням PAN-OS версій 10.0.4 і пізніших пропонують розширені функції та більшу гнучкість.

Виправлені конфігурації моделі серії VM:

Топологія:

Брандмауери Palo Alto Networks можна розгортати на Google Cloud Platform різними способами, як-от керування декількома VPC за допомогою розгортання кількох мережевих інтерфейсів або однорангової моделі VPC.

Модель розгортання кількох мережевих інтерфейсів

Віртуальна машина з декількома мережевими інтерфейсами дозволяє Palo Alto Networks забезпечувати ту саму безпеку корпоративного рівня, яка використовується в корпоративних центрах обробки даних. Можна перевіряти не лише трафік, що надходить до GCP, але й трафік зі сходу на захід між проектами GCP і VPC.

Щоб захистити кілька мереж, можна додати додаткові інтерфейси площини даних серії VM безпосередньо до мереж VPC. Щоб спрямовувати трафік до інтерфейсу NGFW серії VM або до внутрішнього балансувальника навантаження, потрібно використовувати спеціальний маршрут для кожної підключеної мережі, однак потрібно пам’ятати, що існує обмеження у вісім мережевих інтерфейсів на екземпляр віртуальної машини (прилад серії VM). І не можна додавати або видаляти мережеві інтерфейси після його розгортання.

У наведеному нижче прикладі показано шаблони трафіку, які проходять через брандмауери серії VM у цій конфігурації:

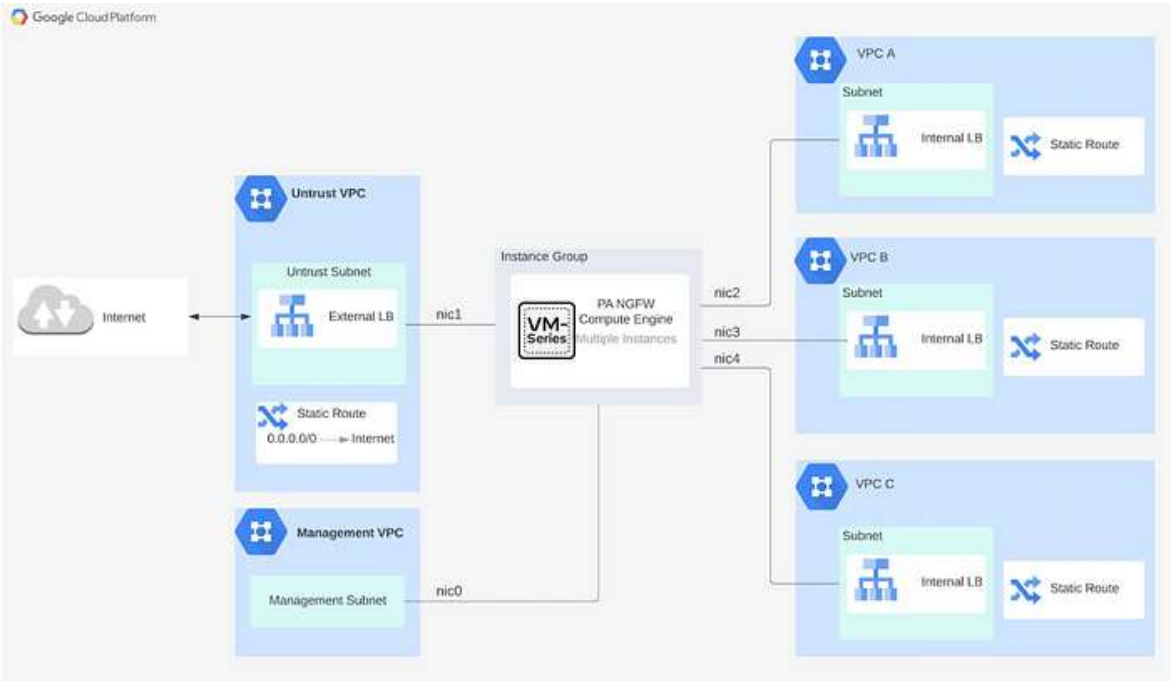

Рис.3.2. Шаблони трафіку

Як показано в цій архітектурі, якщо вхідний запит надсилається до програми, розміщеної у VPC C. Зовнішній балансувальник навантаження розподіляє запит до інтерфейсу недовіри PaloAlto, а потім пристрій VM-Series перевіряє та пересилає запит через NIC4 у VPC C і до цільової програми.

З іншого боку, якщо ресурс у VPC A робить запит до ресурсу у VPC B. Таблиця маршрутизації VPC A направляє запит до внутрішнього балансувальника навантаження у VPC A. Балансувальник навантаження розподіляє запит до NIC2 на віртуальній машині. VM-Series перевіряє та пересилає запит через NIC3 до ресурсу у VPC B. VPC B направляє свій зворотний трафік до свого внутрішнього балансувальника навантаження TCP/UDP за допомогою таблиці маршрутів VPC B.

Потім таблиця маршрутів VPC B спрямовує трафік, який спрямовується до Інтернету, на IP-адресу внутрішнього балансувальника навантаження TCP/UDP VPC B. Балансувальник навантаження розподіляє трафік до NIC3 на брандмауерах серії VM. VM-Series перевіряє та пересилає трафік через свій ненадійний інтерфейс (NIC1) до Інтернету.

Модель Hub-and-Spoke з мережевим пірингом VPC

Піринг VPC допомагає побудувати топологію концентратора та стріли для захисту багатьох мереж VPC, де можна додавати та видаляти спільні мережі VPC залежно від потреби, оскільки піринг мережі забезпечує велику гнучкість.

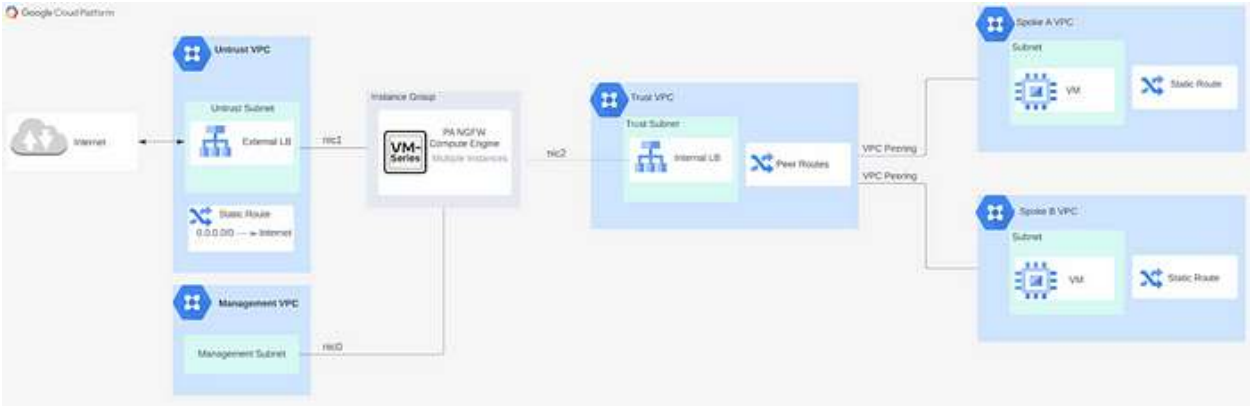

Рис.3.3. Приклад розгортання брандмауера

На рис.3.3. брандмауери серії VM розгорнуті в групі екземплярів, щоб допомогти захистити трафік для різних спільних мереж VPC. Мережа

концентратора містить довірчі інтерфейси серії VM. Довірчі інтерфейси є серверною частиною внутрішнього балансувальника навантаження TCP/UDP. Сполучені мережі є партнерами VPC мережі-концентратора. Кожна спілка має спеціальний маршрут за замовчуванням, який спрямовує трафік на IP-адресу внутрішнього балансувальника навантаження TCP/UDP.

Трафік з Інтернету до програм у сполучених мережах розподіляється зовнішнім балансувальником навантаження TCP/UDP на інтерфейси серії VM (NIC0). VM-Series перевіряє трафік і пересилає допустимий трафік через свій довірчий інтерфейс (NIC2) до програми в розповсюдженій мережі.

Трафік із спільних мереж, спрямований до Інтернету, направляється до внутрішнього балансувальника навантаження TCP/UDP у концентраторі VPC. VM-Series перевіряє трафік і пересилає допустимий трафік через свій ненадійний інтерфейс (NIC0) в Інтернет.

Трафік між сполучними мережами направляється до внутрішнього балансувальника навантаження TCP/UDP у VPC-концентраторі. VM-Series перевіряє та пересилає трафік через інтерфейс довіри (NIC2) у мережу-концентратор, яка направляє допустимий трафік до кінцевої мережі.

Можна об’єднати кілька моделей мережевого інтерфейсу та моделі однорангового мережевого зв’язку VPC, щоб допомогти масштабувати безпеку для багатьох мереж VPC, під’єднавши додаткові інтерфейси серії VM до додаткових концентраторних мереж VPC. Для цього під’єднайте кожен інтерфейс і мережу до кількох спільних мереж через мережевий піринг VPC.

Є багато переваг використання архітектури VPC зі зв’язками-концентраторами з міжмережевими екранами Пало-Альто, як-от централізоване керування політиками безпеки, підвищення безпеки завдяки сегментації та зниження витрат завдяки консолідації ресурсів.

З іншого боку, у також можуть виникнути деякі проблеми, як-от складність архітектури або зниження продуктивності через збільшення мережевого трафіку, якщо його не спланувати належним чином.

Щоб розпочати розгортання, створіть три виділені мережі VPC (довіру, недовіру та керування) у GCP у рамках централізованого проекту, який можна назвати проектом-концентратором для керування трафіком і пристроєм.

Перейдіть до конкретного проекту концентратора, де вже створено 3 відповідні VPC для розгортання брандмауера.

Перейдіть до рішень Marketplace і знайдіть брандмауер PaloAlto. Отримаєте два варіанти: BYOL і Bundle1.

Пакет в основному використовується для моделі «Pay-As-You-Go».

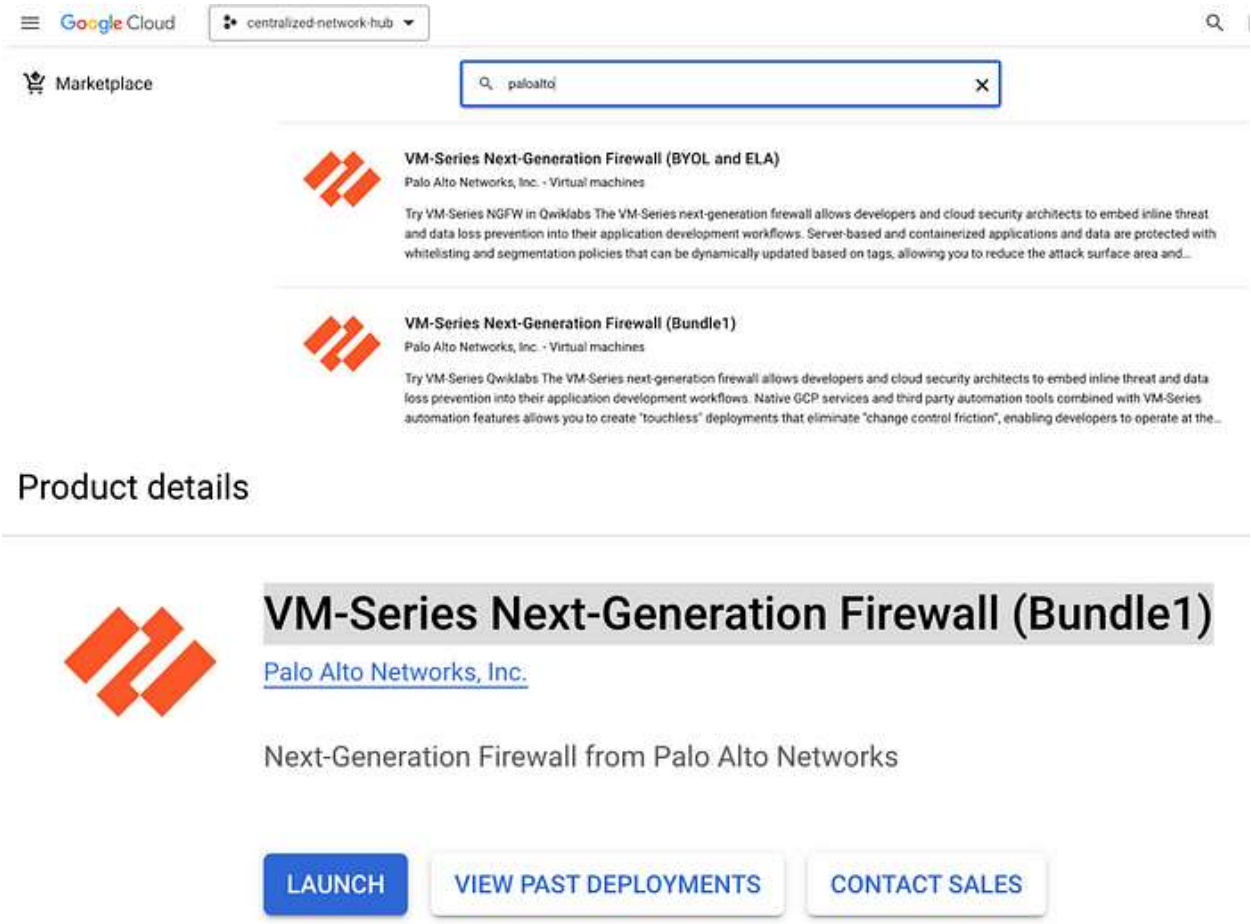

Рис.3.4. Конфігурація розгортання

Потрібно надати тут необхідну інформацію, як-от ім’я розгортання (ім’я віртуальної машини PaloAlto), версію, конкретну зону, тип комп’ютера на бажану ємність і, найголовніше, ключ SSH, який можемо створити за допомогою утиліти keygen і призначити тут для підключення та налаштування пристрою через термінал.

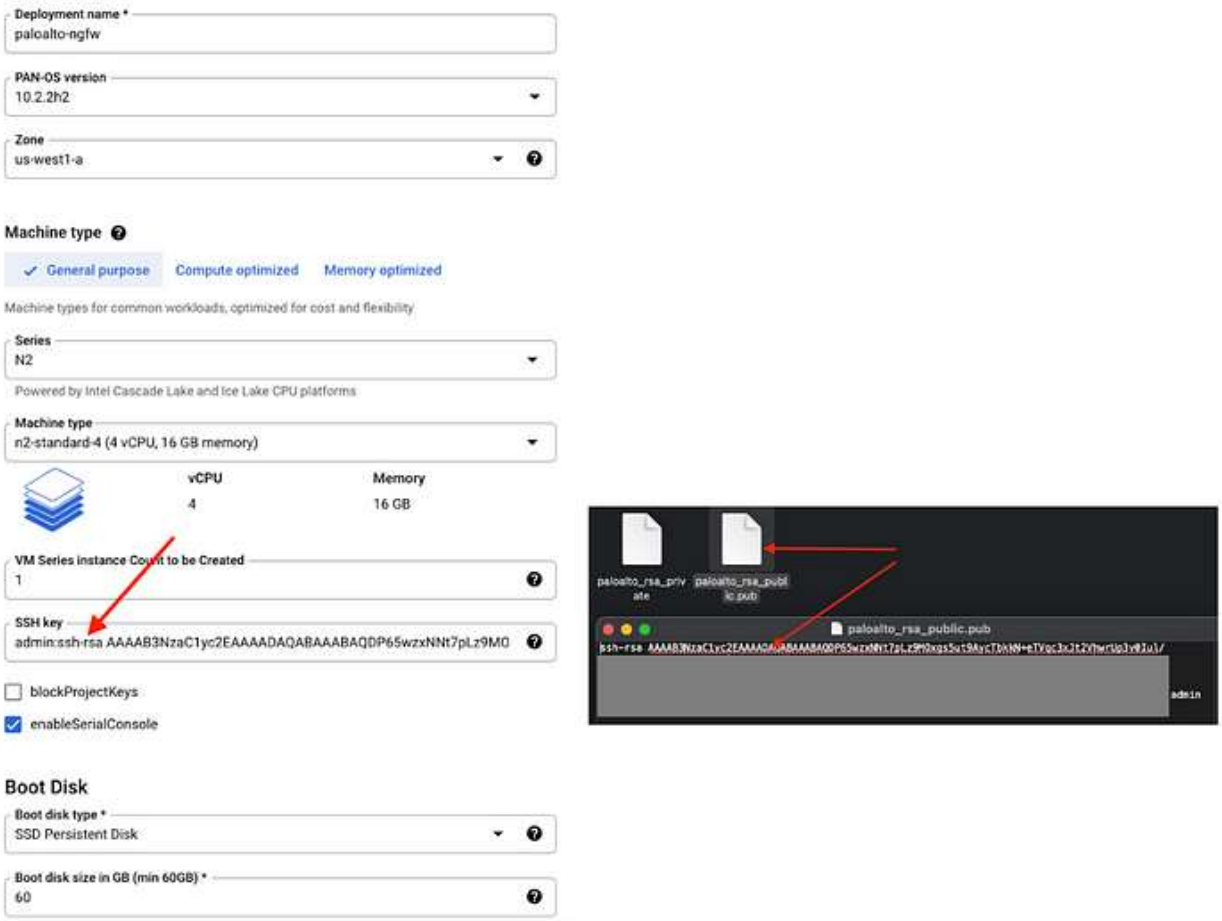

Рис.3.5. Основні налаштування для розгортання

Призначте відкритий ключ під час розгортання брандмауера, і тоді можемо використовувати закритий ключ для підключення програмного пристрою через термінал.

Налаштуйте мережеві інтерфейси відповідно до вимог, у цьому розгортанні/архітектурі використовуватимемо три інтерфейси (керування, ненадійний/зовнішній, довірчий/внутрішній) відповідно до мережевої архітектури концентратора та стріли.

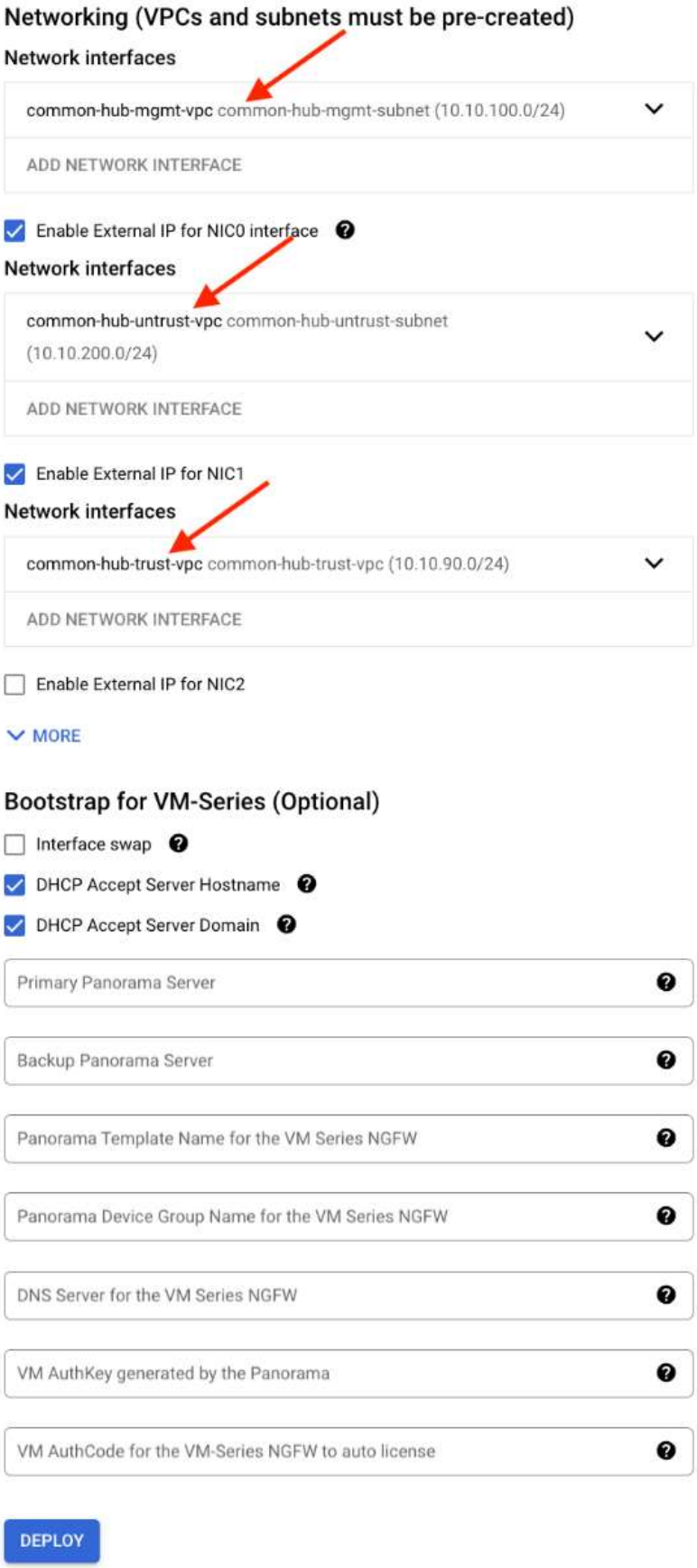

Рис.3.5. Конфігурація брандмауера

Тепер розгортання завершено та готове до подальшого налаштування.

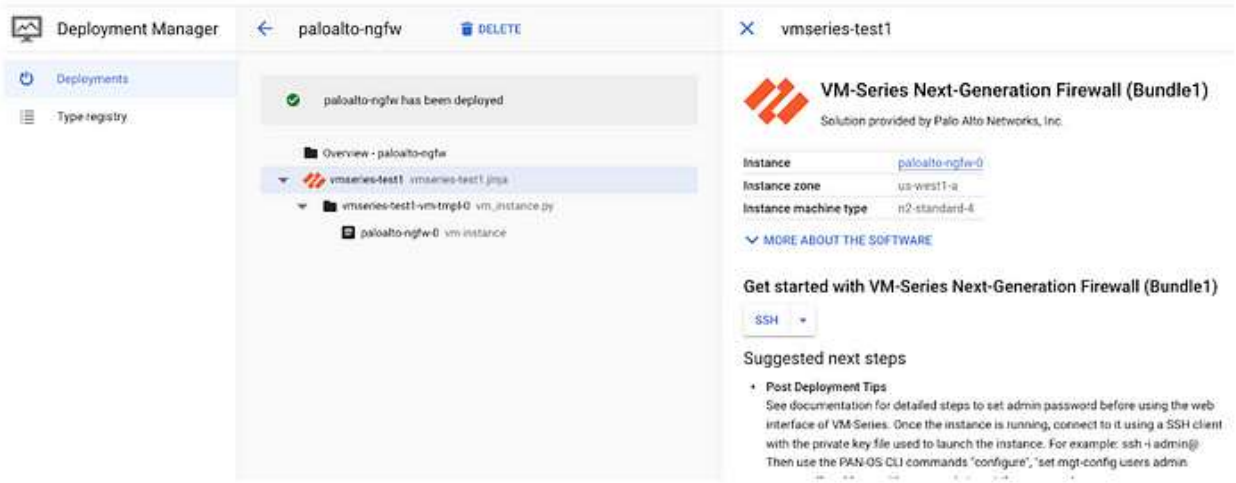

Рис.3.6. Завершення розгортання

Як перший крок зарезервуємо IP-адреси (як внутрішні, так і зовнішні), щоб виправити їх, щоб вони не змінювалися після перезавантаження пристрою. Також можете зарезервувати їх перед розгортанням і відповідно призначити назад.

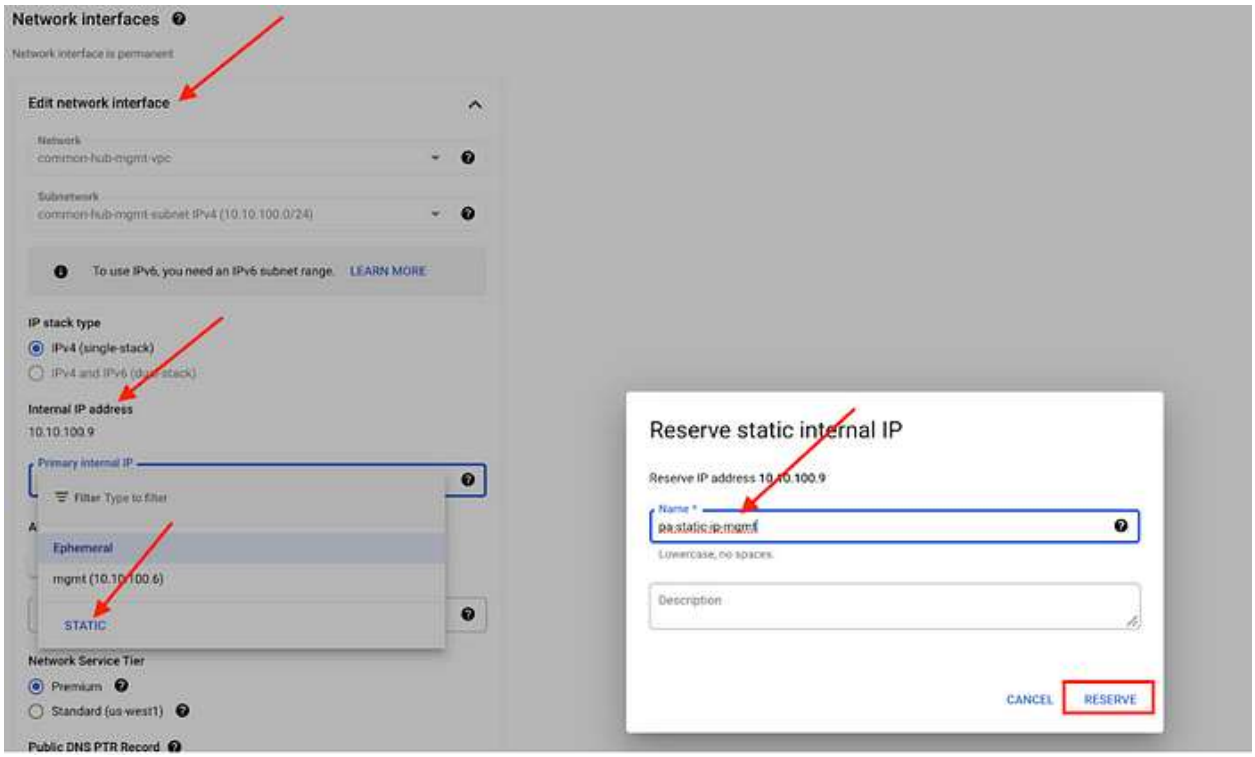

Рис.3.7. Конфігурація IP-адрес

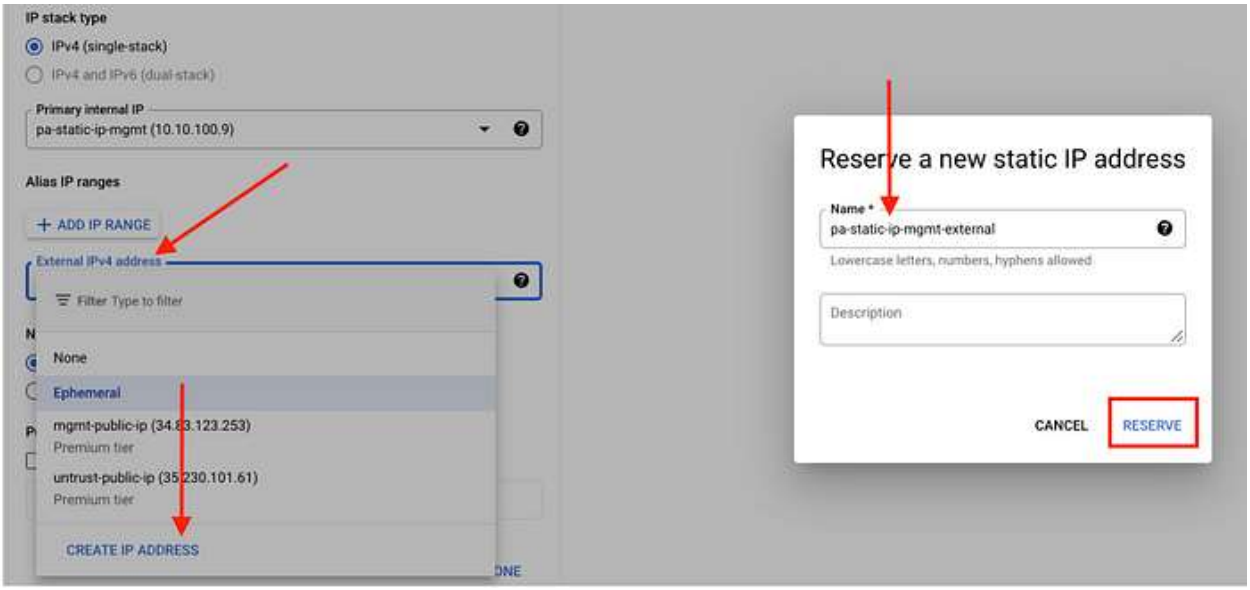

Рис.3.8. Конфігурація IP-адрес

Тепер PaloAlto NGFW готовий до подальшого налаштування, дозволяє використовувати SSH із IP-адресою керування (зовнішнім) після закритого ключа.

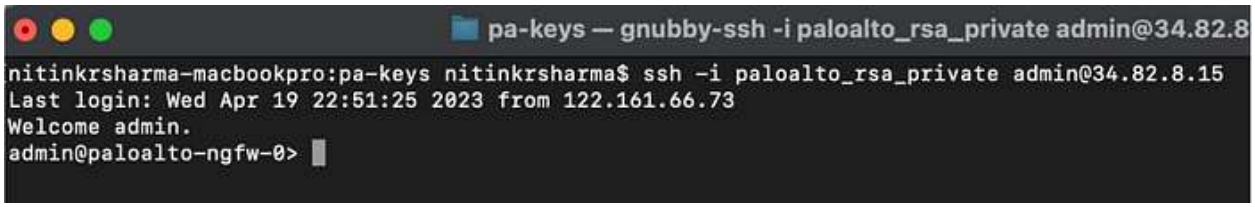

Рис.3.9. Консоль управління

Перейдіть у режим налаштування та встановіть пароль для доступу адміністратора.

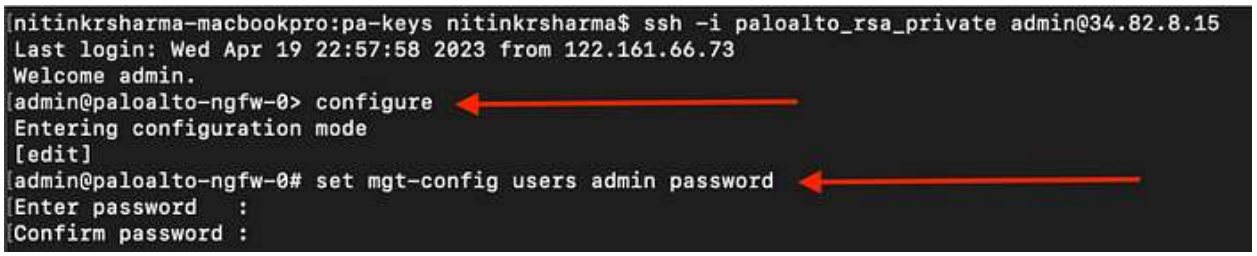

Рис.3.10. Налаштування параметрів адміністратора

Тепер можна отримати доступ до пристрою через графічний інтерфейс із IP-адресою керування (зовнішньою) після користувача адміністратора та пароля, які встановлювалися раніше.

Переконайтеся, що правила брандмауера GCP оновлено, щоб дозволити трафік керування на портах 443 і 80 всередині керування VPC.

Після підключення до пристрою через GUI нам потрібно налаштувати інтерфейси всередині брандмауера PaloAlto.

Перейдіть до «Мережі», а потім до «Інтерфейсів», де можна побачити кілька інтерфейсів, які мають стандартну конфігурацію.

Виберіть перший інтерфейс «interface 1/1», який зробили «untrust/outside» для взаємодії із зовнішнім трафіком.

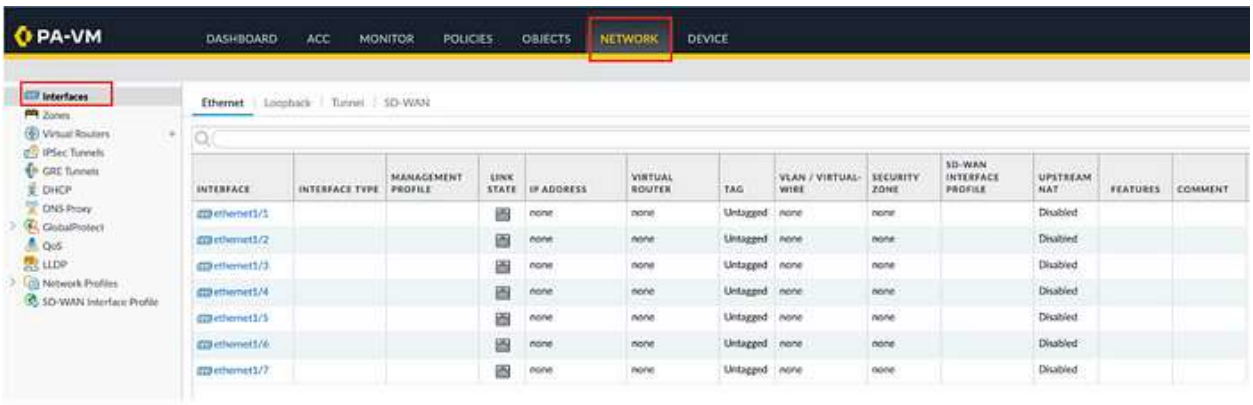

Рис.3.11. Налаштування інтерфейсів

Оновіть ім’я на вкладці «Коментар», виберіть «Рівень 3» для «Типу інтерфейсу», а потім оновіть IP-адреси (приватні та зовнішні) у розділі IPv4, який ми виділили на рівні віртуальної машини для ненадійного інтерфейсу.

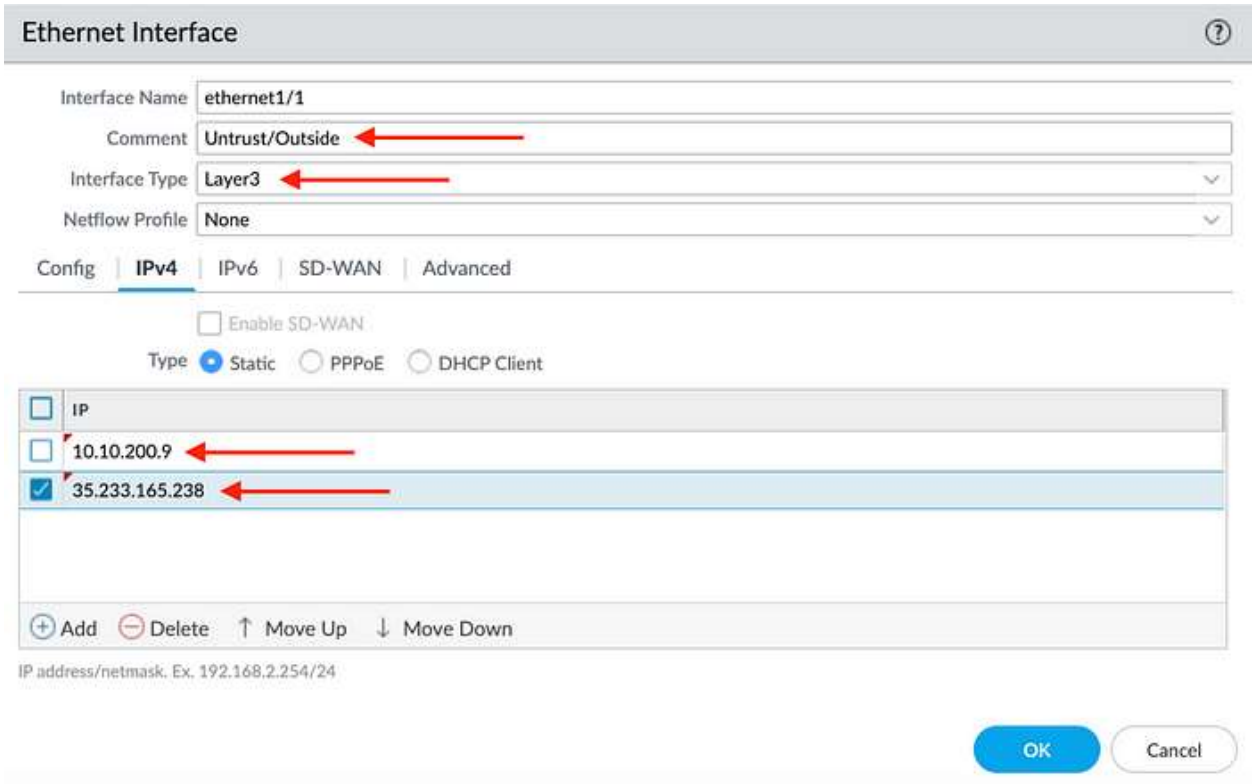

Рис.3.12. Налаштування Ethernet інтерфейсу

.

Оновіть/налаштуйте «Профіль керування». він використовуватиметься для обробки трафіку за різними протоколами для ненадійних мереж, таких як HTTP, HTTPS, PING.

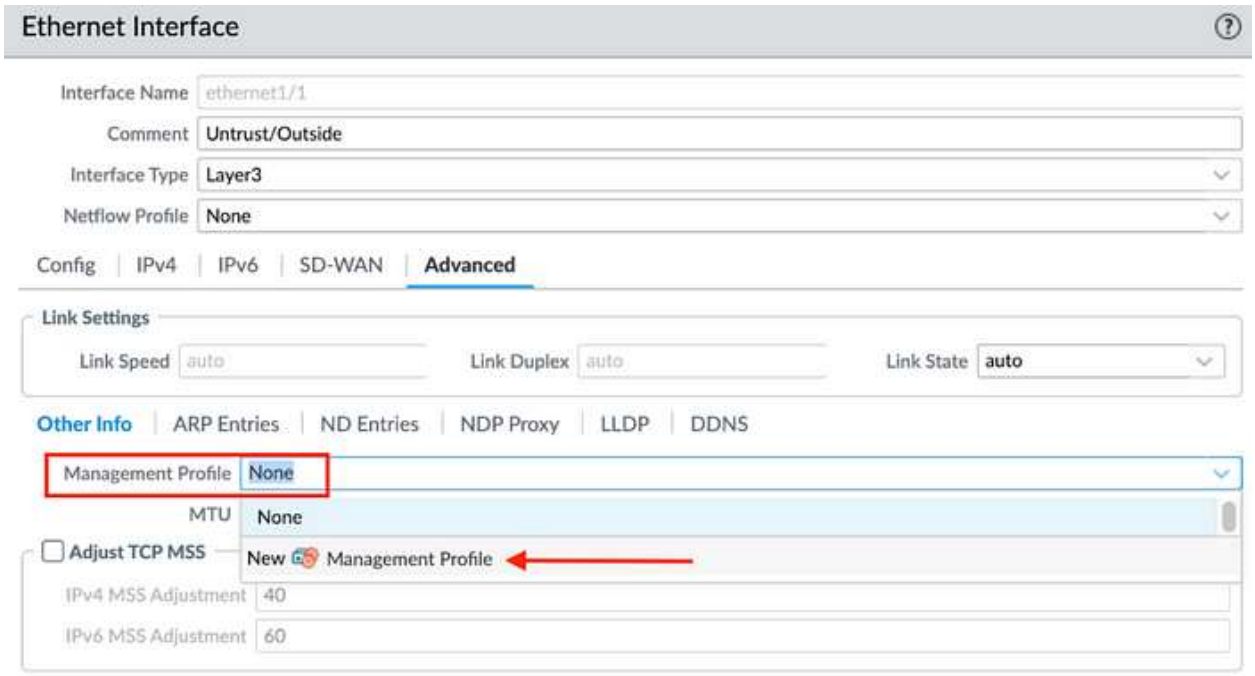

Рис.3.13. Профілі керування

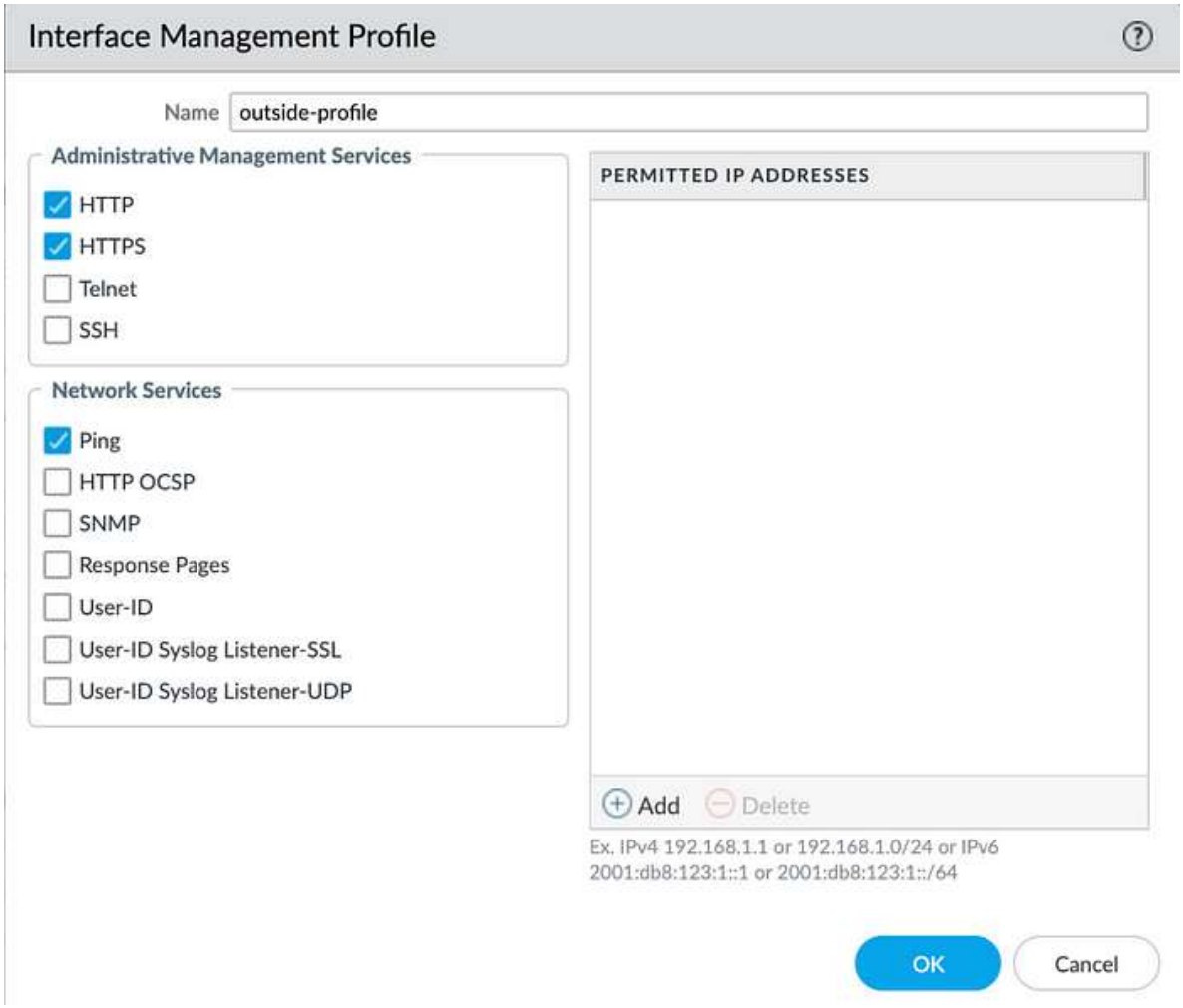

Рис.3.14. Конфігурація профілів керування

Налаштуйте ethernet1/2 для мережі Trust так само, як і Untrust, однак в даному випадку надамо лише приватну IP-адресу, оскільки це буде внутрішній трафік із протоколом PING.

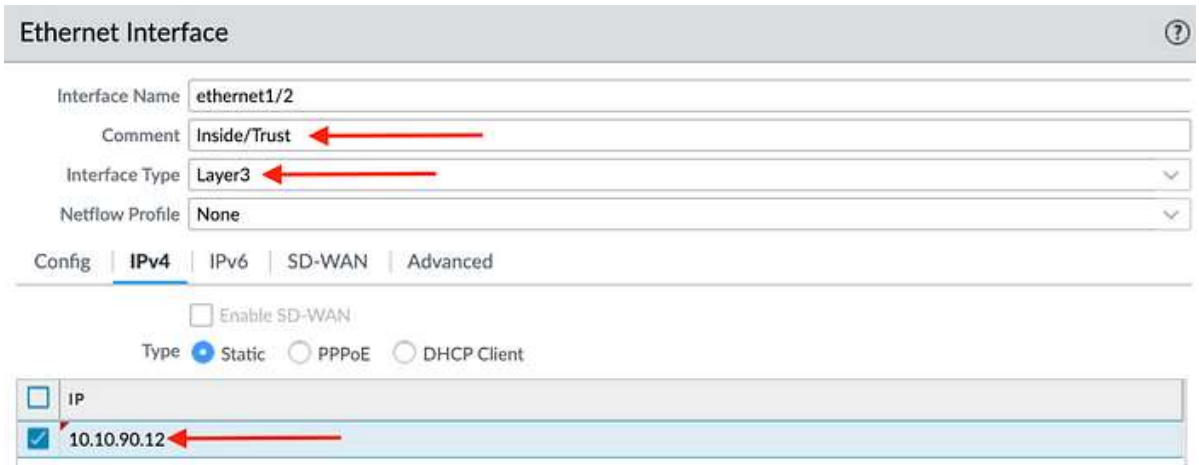

Рис.3.15. Конфігурація мережі

Далі налаштуємо «Профіль керування інтерфейсом». Він використовуватиметься лише для обробки трафіку керування пристроєм.

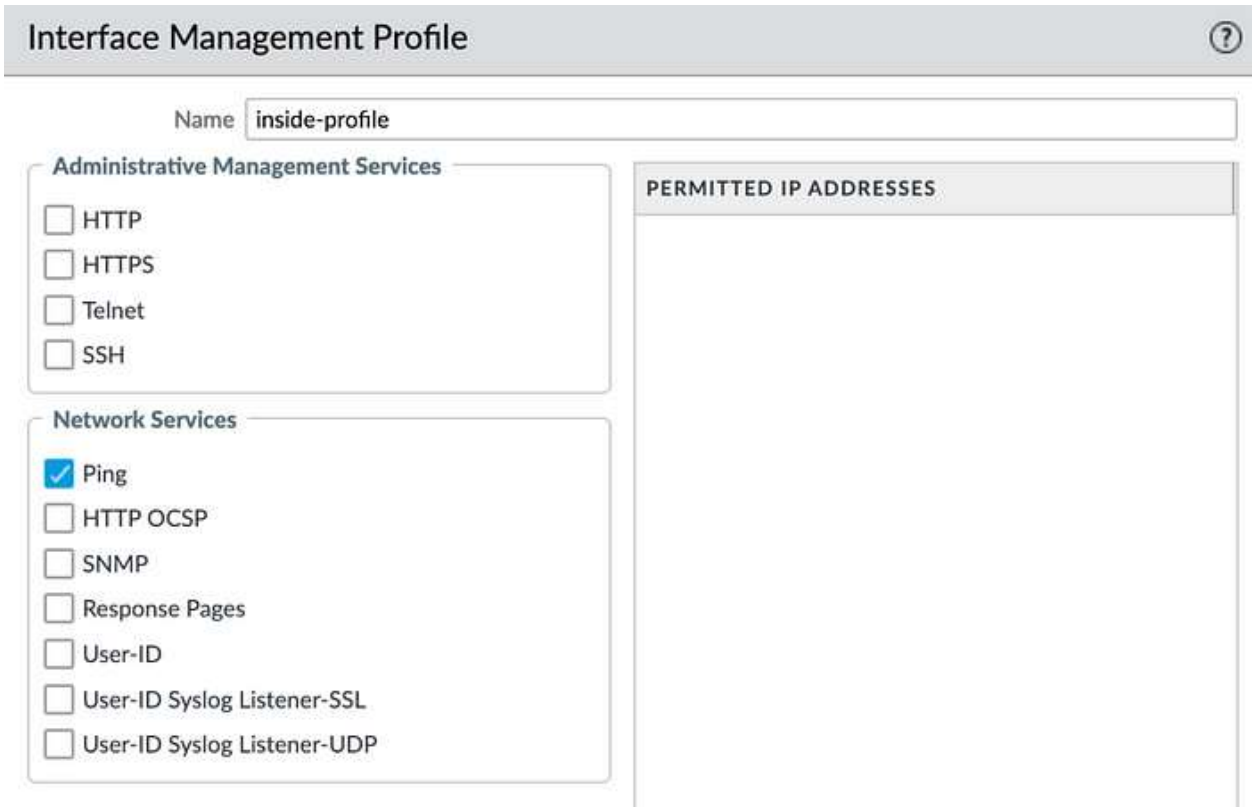

Рис.3.16. Налаштування профілю керування інтерфейсів

Після оновлення інтерфейсів це виглядатиме так.

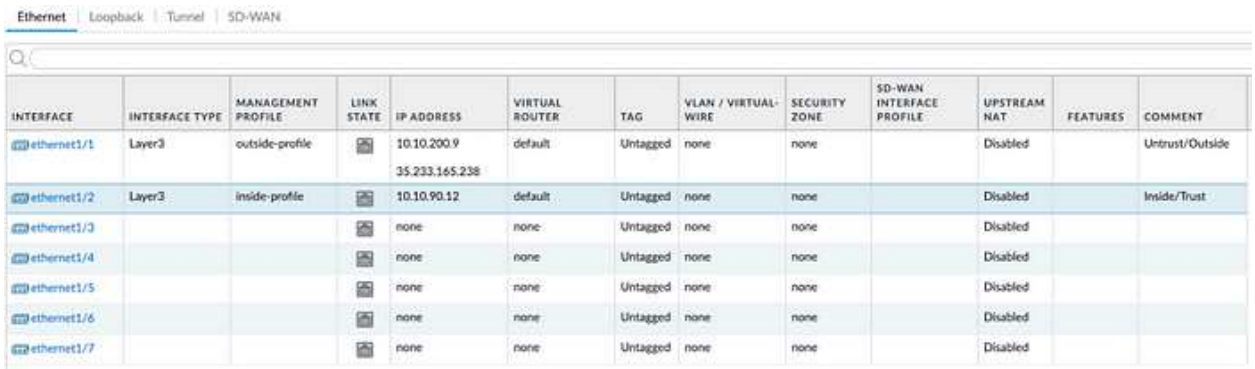

Рис.3.17. Оновлені інтерфейси

Весь цей процес завершує розгортання серії PaloAlto VM на GCP для захисту та керування трафіком різними способами.

3.2. Технологія управління безпекою корпоративної мережі на основі рішення від Palo Alto Networks

Брандмауери нового покоління Palo Alto Networks забезпечують детальний контроль над трафіком, дозволеним для доступу до мережі. До основних функцій і переваг належать:

Застосування політики на основі програми (App-ID)

—Контроль доступу відповідно до типу програми набагато ефективніший, якщо ідентифікація програми ґрунтується не лише на протоколі та номері порту. Служба App-ID може блокувати програми з високим ризиком, а також поведінку з високим ризиком, наприклад обмін файлами, а трафік, зашифрований за допомогою протоколу Secure Sockets Layer (SSL), можна розшифровувати та перевіряти.

Ідентифікація користувача (User-ID™)

— Функція ідентифікатора користувача дозволяє адміністраторам налаштовувати та застосовувати політики брандмауера на основі користувачів і груп користувачів замість або на додаток до мережевих зон і адрес. Брандмауер може спілкуватися з багатьма серверами каталогів, такими як Microsoft Active Directory, eDirectory, SunOne, OpenLDAP та більшістю інших серверів каталогів на основі LDAP, щоб надавати брандмауеру інформацію про користувачів і групи. Потім можна використовувати цю інформацію для активації безпечної програми, яку можна визначити для кожного користувача чи групи. Наприклад, адміністратор може дозволити одній організації використовувати веб-програму, але не дозволити іншим організаціям у компанії використовувати ту саму програму. Також можна налаштувати детальне керування певними компонентами програми на основі користувачів і груп.

Запобігання загрозам

— Служби запобігання загрозам, які захищають мережу від вірусів, хробаків, шпигунського програмного забезпечення та іншого шкідливого трафіку, можуть відрізнятися залежно від програми та джерела.

Фільтрування URL-адрес

— Вихідні з’єднання можна відфільтрувати, щоб запобігти доступу до невідповідних веб-сайтів.

Видимість дорожнього руху

— Розширені звіти, журнали та механізми сповіщень забезпечують детальну видимість трафіку мережевих програм і подій безпеки. Центр керування програмами (ACC) у веб-інтерфейсі визначає програми з найбільшим трафіком і найвищим ризиком для безпеки.

Універсальність і швидкість роботи в мережі

— Брандмауер Palo Alto Networks може доповнити або замінити існуючий брандмауер і може бути прозоро встановлений у будь-якій мережі або налаштований для підтримки комутованого або маршрутизованого середовища. Багатогігабітні швидкості та однопрохідна архітектура надають ці послуги з незначним впливом на затримку мережі.

GlobalProtect

— Програмне забезпечення GlobalProtect™ забезпечує безпеку для клієнтських систем, таких як ноутбуки, які використовуються в організації, дозволяючи простий і безпечний вхід з будь-якої точки світу.

Безвідмовна робота

—Підтримка високої доступності (HA) забезпечує автоматичне перемикання після збоїв у разі збою будь-якого апаратного чи програмного забезпечення.

Аналіз шкідливих програм і звітування

— Хмарна служба аналізу WildFire™ забезпечує детальний аналіз і звітування про зловмисне програмне забезпечення, яке проходить через брандмауер. Інтеграція зі службою аналізу загроз AutoFocus™ дозволяє оцінити ризик, пов’язаний з мережевим трафіком на рівні організації, галузі та глобальному рівні.

Брандмауер серії VM

— Брандмауер серії VM надає віртуальний екземпляр PAN-OS® для використання у віртуалізованому середовищі центру обробки даних і ідеально

підходить для приватних, загальнодоступних і гібридних хмарних обчислювальних середовищ.

Менеджмент і Panorama

— Можна керувати кожним брандмауером через інтуїтивно зрозумілий веб-інтерфейс або через інтерфейс командного рядка (CLI), або централізовано керувати всіма брандмауерам через централізовану систему керування Panorama™, яка має веб-інтерфейс, дуже схожий на веб-інтерфейс palo alto брандмауерів.

3.3. Рекомендації щодо управління безпекою корпоративної мережі орагнізації

Процес захисту мережі починається задовго до розгортання мережі. Це передбачає аналіз операційної системи, яка лежить в основі брандмауера, щоб переконатися, що в ній немає вразливостей. Дотримуючись надійних інструкцій від визнаних органів, таких як організації, що встановлюють стандарти, і постачальники, які виробляють програмне або апаратне забезпечення брандмауера, можна гарантувати, що правила брандмауера налаштовано точно й ретельно. Не забувайте про веб-сервери, які часто є основними цілями для кібератак і потребують ретельного налаштування брандмауера, щоб захистити їх від потенційних загроз. Система, яка не є надійною з самого початку, може бути найслабшою ланкою в захищеній системі.

Конфігурація брандмауера, з іншого боку, є динамічним і постійним завданням. Ефективність брандмауера визначається не лише властивими йому функціями, а й тим, як його налаштовано. Погана конфігурація може ненавмисно створити лазівки для кіберзловмисників, пропускаючи потенційно зловмисний мережевий трафік. Команди безпеки повинні проводити регулярні перевірки конфігурації брандмауера, вносячи необхідні коригування на основі мінливого середовища загроз.

Розгортання брандмауера не є універсальною пропозицією. Стратегія розгортання має базуватися на унікальній інфраструктурі та вимогах організації.

Переконайтеся, що міжмережевий екран правильно взаємодіє з мережами рівня 2 і рівня 3 є життєво важливим для створення адаптивної системи безпеки. Зони, отримані від цих з'єднань, можуть допомогти спростити та налаштувати програми політики брандмауера.

Перехід до розширених конфігурацій брандмауера має бути методичним. Різка зміна може призвести до неочікуваних збоїв, потенційно порушуючи доступ користувачів до Інтернету та погіршуючи взаємодію з ними. Стратегія поетапного розгортання може зменшити ці ризики.

Застарілі протоколи, такі як telnet або незахищені конфігурації SNMP, можуть бути потенційними шлюзами для зламу. Необхідно постійно оцінювати та оновлювати протоколи.

Окрім технічних конфігурацій, пильне спостереження за загрозами має вирішальне значення. Втручання людини відіграє тут ключову роль. Будьте в курсі нових загроз, уразливостей, характерних для моделей брандмауерів, і рекомендованих постачальником виправлень може захистити мережу від потенційних викликів безпеці.

Брандмауери відіграють ключову роль у регулюванні того, хто і що взаємодіє з мережею. Загальний принцип надійної безпеки полягає в забороні всього трафіку за замовчуванням, дозволяючи лише відомі та надійні об'єкти. Класифікуючи трафік — із зовнішніх джерел, внутрішніх відділів чи конкретних бізнес-підрозділів — встановлюється організований, систематичний потік.

Моніторинг не закінчується класифікацією. Потрібна постійна пильність, щоб виявити аномалії в схемах доступу або потоку трафіку. Будь-яке відхилення від норми може вказувати на потенційні загрози або порушення, що робить моніторинг у реальному часі та можливості швидкого реагування безцінними.

У міру розвитку організацій змінюється характер і кількість осіб, яким потрібен доступ до критично важливих систем, таких як брандмауери. Регулярні перевірки списку контролю доступу гарантують, що лише необхідний персонал має доступ, мінімізуючи потенційну внутрішню вразливість. Обмеження доступу

також означає, що в разі порушень контролюється кількість потенційних внутрішніх джерел, що сприяє швидкому вирішенню.

Однак засоби контролю доступу — це не лише обмеження. Вони також забезпечують користувачам доступ до необхідних ресурсів, забезпечуючи безперебійну роботу. Зі зміною ролей потреби в доступі можуть змінюватися. Швидка адаптація елементів керування гарантує, що операції не будуть перешкоджати, а безпека залишиться непорушною.

Комплексні механізми журналювання забезпечують детальне відстеження всього вихідного та вхідного трафіку, пропонуючи безцінне розуміння закономірностей, включаючи аномалії в IP-адресах джерела та IP-адресах призначення, потенційні вразливості та навіть внутрішні загрози. Ця документація також може інформувати майбутні політичні рішення.

Журнали є значущими, лише якщо з ними вжити заходів. Попередження про аномалії в реальному часі забезпечують швидке реагування. Регулярні перевірки журналів можуть виявити потенційні загрози до того, як вони виявляться порушенням безпеки. Сповіщення в режимі реального часу в поєднанні з періодичними перевірками забезпечують надійний механізм безпеки брандмауера, що швидко реагує.

Резервне копіювання є основою надійної безпеки. Вони забезпечують швидке відновлення конфігурацій, політик та інших критичних даних, зберігаючи безпеку та цілісність внутрішньої мережі.

Вкрай важливо встановити докладні протоколи відновлення. Ці процедури мають бути задокументовані, доступні та регулярно перевірятися. Проводячи тестове відновлення, організація може переконатися в цілісності резервних копій, гарантуючи, що вони є не просто заповнювачами, а функціональними інструментами в кризових ситуаціях.

Поступливість — це палиця з двома кінцями. Хоча він встановлює мінімальні стандарти безпеки, яких має дотримуватися організація, покладатися лише на показники відповідності може бути короткозорим. Регулярне узгодження

конфігурацій і політик брандмауера з чинними правилами гарантує, що організація відповідає необхідним стандартам і готова до перевірок.

Відповідність не є статичною. Зі зміною кіберзагроз змінюються і нормативні акти. Інтеграція допоміжних механізмів безпеки, інформування про нормативні зміни та регулярне коригування параметрів брандмауера гарантує, що організація залишається сумісною та безпечною.

Регулярна перевірка брандмауерів на сценарії ретельного тестування, як-от аналіз шляху, гарантує, що вони працюють належним чином. Такі проактивні заходи допомагають виявити потенційні слабкі місця, пропонуючи розуміння областей, які можна покращити.

Ще одним безцінним інструментом є періодичне тестування на проникнення. Імітуючи реальні сценарії кібератак, організації можуть оцінити надійність захисту свого брандмауера, гарантуючи, що вони добре підготовлені до справжніх загроз.

Аудити служать як перевіркою, так і балансом. Регулярні перевірки гарантують, що програмне забезпечення, вбудоване програмне забезпечення та функції журналу залишаються актуальними та в оптимальному робочому стані. Це підвищує ефективність брандмауера та готує організацію до зовнішніх перевірок.

Структурований підхід до внесення змін до політики, отриманий за результатами цих перевірок, гарантує, що зміни покращують безпеку, а не ставлять під загрозу. Будь-яке коригування має бути методичним, його наслідки повинні бути ретельно врахованими, щоб безпека залишалася безкомпромісною.

ВИСНОВКИ

Здійснене дослідження технології управління безпекою корпоративної мережі виявило важливий внесок у сферу кібербезпеки для підприємств. Застосування сучасних технологій управління безпекою стає визначальним аспектом забезпечення надійності, конфіденційності та доступності корпоративних мереж у умовах постійно зростаючого ризику кіберзагроз.

Дослідження підтверджує, що використання технологій управління безпекою дозволяє ефективно виявляти та протидіяти різноманітним кіберзагрозам, що загрожують корпоративній мережі.

У рамках даної дипломної роботи було проведено докладне дослідження технології управління безпекою корпоративної мережі на основі файерволу Palo Alto. Основною метою було вивчення можливостей цього рішення щодо забезпечення ефективного контролю і захисту мережевого середовища організацій. Встановлено, що файервол Palo Alto пропонує інтегровану систему безпеки, яка охоплює різноманітні аспекти захисту мережі, включаючи виявлення загроз, аналіз трафіку та керування доступом.

Виокремлено ефективність системи виявлення загроз, що базується на аналізі поведінки мережі і використанні інтелектуальних алгоритмів для вчасного розпізнавання атак. Palo Alto володіє потужним механізмом глибокого аналізу трафіку, що дозволяє ідентифікувати навіть складні кіберзагрози та миттєво реагувати на них.

Встановлено, що файервол Palo Alto надає ефективні засоби керування доступом, що дозволяють точно налаштовувати права доступу для різних користувачів та ресурсів мережі. Зазначено, що автоматизація процесів управління безпекою, а також використання інтелектуальних алгоритмів, дозволяє забезпечувати швидке реагування на нові загрози та зменшувати ризик людського фактору. Виокремлено важливість централізованої системи управління, яка

спрощує процеси моніторингу, конфігурації та аналізу безпеки мережі для адміністраторів.

Зазначено гнучкість та можливість масштабування рішення, що дозволяє впроваджувати його в різних мережевих середовищах, від невеликих підприємств до великих корпоративних інфраструктур.

Отже, технології управління безпекою корпоративної мережі рекомендується активно впроваджувати сучасні рішення в області кібербезпеки. Важливо враховувати індивідуальні потреби та особливості кожного підприємства при впровадженні та конфігурації технологій управління безпекою.

ПЕРЕЛІК ПОСИЛАНЬ

1. IOPscience. Research on Computer Network Security

2. Problems and Countermeasures .URL: https://iopscience.iop.org/article/10.1088/1742-6596/1992/3/032069/pdf (дата звернення: 23.10.2023).

3. Network Security Best Practices - Restorepoint. Multi-Vendor Network Configuration and Compliance Management. URL: https://www.restorepoint.com/topics/network-security-best-practices (дата звернення: 24.12.2023).

4. Next-Generation Firewall. Palo Alto Networks | TechDocs Home. URL: https://docs.paloaltonetworks.com/ngfw (дата звернення: 24.12.2023).

5. Next-Generation Firewall. Palo Alto Networks NGFW AIOps | TechDocs Home. URL https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/ngfw/ngfw-aiops.pdf

6. PaloGuard - Enterprise Security Platforms. Palo Alto Networks Products & Solutions | PaloGuard.com. URL: https://www.paloguard.com/Features-Security.asp (дата звернення: 24.12.2023).

7. The Benefits of Palo Alto Networks Firewall Single Pass Parallel Processing (SP3) and Hardware Architecture. Cisco Networking, VPN Security, Routing, Catalyst-Nexus Switching, Virtualization Hyper-V, Network Monitoring, Windows Server, CallManager, Free Cisco Lab, Linux Tutorials, Protocol Analysis, CCNA, CCNP, CCIE. URL: https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-single-pass-parallel-processing-hardware-architecture.html (дата звернення: 24.12.2023).

8. ZADEA. How Palo Alto Networks Next-Generation Firewalls Secure Your Business URL: https://www.zadea.it/pdf/paloalto-firewall-features-overview.pdf (дата звернення: 24.12.2023).

9. Sharma N. K. PaloAlto Firewall Deployment on Google Cloud. Medium. URL: https://medium.com/@nitinkrsharma/paloalto-firewall-deployment-on-google-cloud-bb114c833bd0 (дата звернення: 24.12.2023).

10. Onboard Devices and Deployments. Palo Alto Networks | TechDocs Home. URL: https://docs.paloaltonetworks.com/ngfw/administration/onboard-devices-and-deployments (дата звернення: 24.12.2023).

11. Cloud Management of NGFW Administration | TechDocs Home. URL: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/ngfw/ngfw-administration.pdf (дата звернення: 24.12.2023).

12. PAN-OS® Networking Administrator's Guide | TechDocs Home. URL: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-1/pan-os-networking-admin/pan-os-networking-admin.pdf (дата звернення: 24.12.2023).

Configure Interfaces. Palo Alto Networks | TechDocs Home. URL: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/configure-interfaces (дата звернення: 24.12.2023).

13. Features and Benefits. Palo Alto Networks | TechDocs Home. URL: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/web-interface-basics/features-and-benefits (date of access: 24.12.2023).

14. Key Firewall Best Practices. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/firewall-best-practices (date of access: 24.12.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)