ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«Технології забезпечення безпеки периметру інформаційної системи на базі рішення Fortinet»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Сидоренко Є.Є.
(прізвище та ініціали)
Керівник Гайдур Г.І
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“20” грудня 2021 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Сидоренко Євгенію Євгеновичу
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Технології забезпечення безпеки периметру інформаційної системи на базі рішення Fortinet»
керівник магістерської роботи Гайдур Галина Іванівна, к.військ.н.
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від « » 2021 року №

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи
корпоративна локальна мережа;
наукова та технічна література, експлуатаційна документація, міжнародні стандарти та нормативні документи щодо використання мережевих екранів;
приклади налаштування мережевого екрану Fortigate100e.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблем кібербезпеки та способів її забезпечення
2. Технології забезпечення кібербезпеки на базі обладнання Fortinet

3. Аналіз переліку можливостей

4. Перелік графічного матеріалу

Таблиці, схеми Power Point

6. Дата видачі завдання 27.09.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	23.10.2021 р.	Вик.
2.	Аналіз проблем кібербезпеки та способів її забезпечення	06.11.2021 р.	Вик.
3.	Аналіз мережевих екранів компанії Fortinet	20.11.2021 р.	Вик.
4.	Аналіз переліку можливостей мережевого екрану Fortigate 100e та рекомендацій щодо роботи з ним	30.11.2021 р.	Вик.
5.	Висновки.	04.12.2021 р.	Вик.
6.	Оформлення результатів дослідження.	07.12.2021 р.	Вик.
7.	Підготовка доповіді до захисту.	15.12.2021 р.	Вик.

Студент Сидоренко Є.Є.

(підпис) прізвище та ініціали

Керівник магістерської роботи Гайдур Г.І.

(підпис) прізвище та ініціали

РЕЦЕНЗІЯ
ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента **Сидоренко Євгенія Євгеновича**

на тему: **«Технології забезпечення безпеки периметру інформаційної системи на базі рішення Fortinet»**

Актуальність: У магістерській роботі розглянуті можливі види атак персонального комп'ютера і локальної мережі, як з боку локальних мереж, так і з боку мережі Інтернет. Розглянуті технології забезпечення безпеки. Запропоновано способи і засоби забезпечення інформаційної безпеки за допомогою мережевих екранів, розроблені керівництва по налаштуванні і роботі апаратних і програмних засобів захисту ПК на прикладі мережевого екрану Fortigate 100e. Тому тема магістреської роботи є актуальною і своєчасною.

Позитивні сторони:

1. Зміст роботи відповідає завданню. Студент показав високий рівень знань і ступінь підготовленості її до майбутньої роботи за фахом.
2. Обґрунтовано необхідність використання мережевих екранів FortiGate в різних сферах бізнесу. Достатньо успішно виконаному аналіз представлених рішень та описано функціонал найважливіших опцій мережевих екранів.
3. Текст викладено 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. Досить поверхнево розкриті способи та засоби забезпечення інформаційної безпеки.
2. При обґрунтуванні вибору мережевого екрану доцільно було б провести порівняння з мережевими екранами інших компаній.

Вищезгадані зауваження не впливають на загальну позитивну оцінку магістерської роботи.

Висновок: робота заслуговує оцінку "відмінно", а студент – Сидоренко Євгеній Євгенович гідний присвоєння кваліфікації: 2149.2 магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Якість магістерської роботи	
Виконано на замовлення підприємст	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	*
Має практичну цінність	*
Проект-частина комплексної теми	

Підпис рецензента

_____ _____
(П.І.Б.)

_____
(посада, науковий ступінь, вчене звання)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Сидоренко Є. Є. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технології забезпечення безпеки периметру інформаційної системи на базі рішення Fortinet»

Магістерська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Сидоренко Є.Є. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Гребенніков А.Б.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Сидоренко Є.Є.*** обрав тему роботи, технології забезпечення безпеки периметру інформаційної системи на базі рішення Fortinet. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях та практиці. Під час виконання магістерської роботи Сидоренко Є.Є. 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 магістерську роботу студента Сидоренко Євгеній Євгенович на оцінку **«добре»** та присвоїти йому кваліфікацію 2149.2 магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека

Керівник магістерської роботи _____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Сидоренко Є.Є.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2021 року

РЕФЕРАТ

Текстова частина магістерської роботи: 74 сторінки, 31 рисунок, 4 таблиці, 12 джерел.

Об'єкт дослідження – є процес виявлення загроз кібернетичної безпеки в корпоративних мережах.

Предмет дослідження – є мережеві екрани FortiGate від компанії яка надає послуги по забезпеченню безпеки корпоративних мереж.

Мета роботи – розробити рекомендації щодо забезпечення інформаційної безпеки периметру при використанні технологій базі обладнання Fortigate.

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

В роботі зроблено аналіз проблеми забезпечення кібербезпеки корпоративної мережі та визначено основні загрози корпоративній мережі. Проведено аналіз характеристик систем управління інформаційною безпекою та подіями, які доцільно використовувати і корпоративних мережах різних підприємств.

На основі дослідження розроблено рекомендації щодо забезпечення інформаційної безпеки периметру на базі технологій Fortinet.

Галузь використання – кібербезпека.

КОРПОРАТИВНА ЛОКАЛЬНА МЕРЕЖА, КІБЕРБЕЗПЕКА, FORTIGATE, ЗАХИСТ ЛОКАЛЬНИХ МЕРЕЖ, АНАЛІЗ АНТИВІРУСНИХ ПРОГРАМ, МЕРЕЖЕВІ ЕКРАНИ, МЕТОДИ ТА ЗАСОБИ РОБОТИ С МЕРЕЖЕВИМИ ЕКРАНАМИ, МІЖМЕРЕЖЕВИЙ ЕКРАН, ПОПЕРЕДЖЕННЯ ЗАГРОЗ, КОНТРОЛЬ ТА МОНІТОРИНГ ТРАФІКУ, АДАПТИВНИЙ ЗАХИСТ ВІД ЗАГРОЗ.

ABSTRACT

Master’s thesis: 74 pages, 31 figures, 4 tables, 12 sources

The object of research – the process of identifying cyber security threats in corporate networks.

The subject of the research – FortiGate firewalls from a company that provides security services for corporate networks.

The aim of the research – to develop recommendations for information security of the perimeter when using technologies based on Fortigate equipment.

Research methods – elaboration of literature on this topic, analysis of operational documentation, international standards and their comparison.

The paper analyzes the problem of cybersecurity of the corporate network and identifies the main threats to the corporate network. The analysis of characteristics of information security and event management systems which are expedient to use and corporate networks of various enterprises is carried out.

Based on the research, recommendations for ensuring information security of the perimeter based on Fortinet technologies have been developed.

Field of use – cybersecurity.

CORPORATE INTRANET, CYBER SECURITY, FORTIGATE, LAN SECURITY, ANALYSIS ANTIVIRUS, FIREWALL, METHODS AND TOOLS WORK WITH FIREWALLS, FIREWALLS, PREVENT THREATS, CONTROL AND TRAFFIC MONITORING, ADAPTIVE THREAT PROTECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СУІБ – Система управління інформаційною безпекою

ІБ – Інформаційна безпека

ОС – Операційна система

ПК – Персональний комп’ютер

DOS – Denial of Service

LAN – Local area network

WAN – World area network

SMTP – Simple mail transfer proocol

СКУД – Система керування управління доступом

DLP – Data leak prevention

НСД – Несанкціонований доступ

AD – Active Directory

DNS – Domain name system

NAT – Network address translation

ІСПДн – Інформаційна система персональних даних

FTP – File transfer protocol

IRC – Internet relay chat

TLS – Transport layer security

VPN – Virtual private network

NGFW – Next generation firewall

SSL – Secure sockets layer

CLI – Command line interface

HTTPS – Hypertext transfer protocol secure

UI – User interface

LDAP – Lightweight directory access protocol

Frame Relay – ретрансляція кадрів.

ATM – асинхронний спосіб передачі даних.

L2 VPN – Layer 2 VPN.

L3 VPN – Layer 3 VPN.

IP – міжмережевий протокол.

BGP – протокол граничного шлюзу.

VPLS – віртуальна приватна локальна мережа).

TCP –протокол керування передачею даних.

CER – граничний маршрутизатор клієнта.

PER – граничний маршрутизатор мережі провайдера.

MAC – фізична адеса пристрою.

LSP – тунель, шлях в MPLS.

EIGRP – протокол маршрутизації.

OSPF – протокол динамічної маршрутизації.

VRF – технологія, що дозволяє реалізовувати на базі одного фізичного маршрутизатора мати декілька віртуальних.

ВСТУП

Актуальність дослідження. Нові інформаційні технології успішно впроваджуються в усі сфери людської діяльності. Поява глобальних і локальних мереж передачі даних надало нові можливості швидкого обміну інформацією. Завдяки всесвітній мережі Інтернет за допомогою стека протоколів TCP / IP і єдиного адресного простору об'єднуються не тільки корпоративні і відомчі мережі, але і звичайні користувачі, які мають прямий доступ в Інтернет зі своїх домашніх комп'ютерів. При цьому природне бажання користувачів, мати постійний доступ до своєї персональної інформації та інформації для домашньої і службової діяльності і бути впевненими, в неможливості її неправомірного використання. Проблема забезпечення безпеки суб'єктів інформаційних відносин, захисту їх законних інтересів при використанні інформаційних систем і зберігається і оброблюваної ними інформації вимагає постійної уваги і пошуку раціональних шляхів її вирішення.

Сьогодні термін «інформація» часто використовується для позначення особливого товару, вартість якого часто перевершує вартість обчислювальної системи, в межах якої він існує. при появі загроз, пов'язаних з можливістю втрати, перекручування, розкриття конфіденційних даних і витоку певної інформації, організація або держава в цілому може втратити не тільки великі суми грошей, але і репутацію на політичному та економічному рівні.

У міру розвитку і ускладнення засобів, методів і форм автоматизації процесів обробки інформації підвищується і рівень загроз для використовуваних інформаційних технологій. Саме тому за допомогою використання сучасних способів і засобів захисту цілісності і конфіденційності інформації (антивірусних програм, між мережевих екранів, програмних і апаратних продуктів для захисту інформації від несанкціонованого доступу і вірусних атак і ін.) можна забезпечити безпеку автоматизованої системи в цілому і особистого автоматизованого робочого місця користувача.

У цій дипломній роботі розглянуті можливі види атак персонального комп'ютера і локальної мережі, як з боку локальних мереж, так і з боку мережі Інтернет. Запропоновано способи і засоби забезпечення інформаційної безпеки за допомогою мережевих екранів, розроблені керівництва по налаштуванні і роботі апаратних і програмних засобів захисту ПК на прикладі мережевого екрану FortiGate 100e.

Об'єкт дослідження – є процес виявлення загроз кібернетичної безпеки в корпоративних мережах.

Предмет дослідження – є мережеві екрани FortiGate від компанії яка надає послуги по забезпеченню безпеки корпоративних мереж.

Мета роботи – розробити рекомендації щодо забезпечення інформаційної безпеки при використанні мережевих екранів на базі обладнання Fortigate.

Наукові завдання:

- провести аналіз проблем кібербезпеки та способів її забезпечення;
- провести аналіз мережевих екранів компанії Fortinet;
- провести аналіз переліку можливостей мережевого екрану Fortigate 100e та рекомендацій щодо роботи з ним;
- розробити рекомендації по опрацьованому матеріалу.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо забезпечення інформаційної безпеки периметру за допомогую технологій на базі систем Fortinet.

1. АНАЛІЗ ПРОБЛЕМ КІБЕРБЕЗПЕКИ ТА СПОСОБІВ ЇЇ ЗАБЕЗПЕЧЕННЯ

1.1 Актуальність проблеми забезпечення інформаційної безпеки

Будь-яке фундаментальне технічне чи технологічне нововведення, надаючи можливості для вирішення одних соціальних проблем і відкриваючи широкі перспективи для розвитку особистості і суспільства, завжди викликає загострення старих або породжує нові, раніше невідомі проблеми, стає джерелом нових потенційних небезпек.

Без належної уваги до питань забезпечення безпеки наслідки переходу суспільства до нових технологій можуть бути катастрофічними для нього і його громадян. Саме так йде справа в області атомних, хімічних та інших екологічно небезпечних технологій, у сфері транспорту. Аналогічно йде справа і з інформатизацією суспільства

Бурхливий розвиток засобів обчислювальної техніки відкрило перед людством небувалі можливості по автоматизації розумової праці і призвело до створення великої кількості різного роду автоматизованих інформаційних і керуючих систем, до виникнення принципово нових, так званих, інформаційних технологій.

Неправомірне перекручування або фальсифікація, знищення або розголошення певної частини інформації, так само як і дезорганізація процесів її обробки і передачі в інформаційно-управляючім системах завдають серйозної матеріальної та моральної шкоди багатьом суб'єктам (державі, юридичним і фізичним особам), які беруть участь в процесах автоматизованого інформаційного взаємодії.

Життєво важливі інтереси цих суб'єктів, як правило, полягають в тому, щоб певна частина інформації, що стосується їх економічних, політичних та інших сторін діяльності, конфіденційна комерційна і персональна інформація, була б постійно легко доступна і в той же час надійно захищена від неправомірного її використання:

небажаного розголошення, фальсифікації, незаконного тиражування, блокування або знищення.

Є вагомі підстави вважати, що застосовуються в даний час більшістю організацій заходи не забезпечують необхідного рівня безпеки суб'єктів, що беруть участь в процесі інформаційної взаємодії, і не здатні в необхідній мірі протистояти різного роду впливам з метою доступу до критичної інформації та дезорганізації роботи автоматизованих систем.

На жаль, як і будь-яке інше досягнення людського генія, комп'ютер, вирішуючи одні технічні, економічні та соціальні проблеми, одночасно породжує і інші, часом не менш складні. Якщо в належній мірі не подбати про нейтралізацію супутнього прогресу негативних факторів, то ефект від впровадження новітніх досягнень науки і техніки може виявитися в цілому негативним.

1.1.1 Поняття інформаційної безпеки

Термін «інформаційна безпека» з'явився з розвитком обчислювальної техніки і ЕОМ. Нижче наведені два визначення інформаційної безпеки.

Інформаційна безпека - це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держав.

Інформаційна безпека - захищеність інформації і підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктурі.

Інформаційна безпека безпосередньо пов'язана з поняттям «захист інформації».

Захист інформації - це діяльність, спрямована на запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних дій на захищає інформацію.

Поняття інформаційної безпеки базується на трьох основних положеннях:

• конфіденційність інформації (від англ. - confidentiality) - стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на нього право;

• цілісність інформації (від англ. - integrity) - уникнути несанкціонованої модифікації інформації;

• доступність інформації (від англ. - availability) - уникнути тимчасового або постійного захування інформації від користувачів, які отримали права доступу.

Інформаційна безпека включає в себе безпеку використовуваного ПО, безпеку апаратних і технічних засобів, безпеку каналів зв'язку і багато іншого.

Забезпечення інформаційної безпеки включає перелік заходів і утворює систему забезпечення інформаційної безпеки. Суб'єкти інформаційних відносин зацікавлені в забезпеченні своєї інформаційної безпеки, а саме:

• своєчасного доступу до необхідної інформації і автоматизованим службам;

• достовірності інформації;

• конфіденційності інформації та її цілісності;

• захисту від дезінформації (нав'язування їм неправдивої інформації);

• захисту інформації від незаконного тиражування;

• можливості здійснення безперервного контролю і управління процесами обробки і передачі інформації і т.д.

Збиток суб'єктам інформаційних відносин може бути завдано не тільки з боку локальних і глобальних мереж, але і через певну інформацію з носіїв. Тому в якості об'єктів, які підлягають захисту з метою забезпечення безпеки інформаційних відносин повинні розглядатися інформація, будь-які носії, засоби зберігання і процеси її обробки (передачі).

В області захисту інформації існує великий список керівних документів. Нижче наведені деякі з міжнародних та українського зразків документів:

- ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення від 11.10.1996;
- BS 7799-1:2005 — Британський стандарт BS 7799 перша частина. BS 7799 Part 1 Code of Practice for Information Security Management (Практичні правила управління інформаційною безпекою) описує 127 механізмів контролю, необхідних

для побудови системи управління інформаційною безпекою (СУІБ) (організації, певних на основі кращих прикладів світового досвіду (best practices) в даній області . Цей документ служить практичним посібником по створенню СУІБ;

- BS 7799-2:2005 — Британський стандарт BS 7799 друга частина стандарту. BS 7799 Part 2 - Information Security management - specification for information security management systems (Специфікація системи управління інформаційною безпекою) визначає специфікацію СУІБ. Друга частина стандарту використовується в якості критеріїв при проведенні офіційної процедури сертифікації СУІБ організації;
- BS 7799-3:2006 — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт в галузі управління ризиками інформаційної безпеки;
- ISO/IEC 17799:2005 — «Інформаційні технології - Технології безпеки - Практичні правила менеджменту інформаційної безпеки». Міжнародний стандарт, який базується на BS 7799-1: 2005;
- ISO/IEC 27000 — Словник і визначення;
- ISO/IEC 27001 — «Інформаційні технології - Методи забезпечення безпеки - Системи управління інформаційною безпекою - Вимоги». Міжнародний стандарт, який базується на BS 7799-2: 2005;
- ISO/IEC 27002 — Зараз: ISO / IEC 17799: 2005. «Інформаційні технології - Технології безпеки - Практичні правила менеджменту інформаційної безпеки». Дата виходу - 2007 рік;
- ISO/IEC 27005 — Сейчас: BS 7799-3:2006 — Керівництво по менеджменту ризиків ІБ;
- German Information Security Agency. IT Baseline Protection Manual — Standard security safeguards (Керівництво по базовому рівню захисту інформаційних технологій).

1.1.2 Типи проблем в забезпеченні інформаційної безпеки

На сьогодні інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни та суспільства. Зазначене

обумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв’язку й інформатизації і, як наслідок, істотним зростанням впливу інформаційної сфери на життя нашого суспільства.

Інформаційна безпека суспільства, держави характеризується ступенем їх захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи. Загальноприйнятим є таке визначення інформаційної безпеки, як стан захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері.

Наша країна знаходиться на стадії зародження правильного управління інформаційною безпекою тому вона має наступні проблеми:

1. Відсутність дієвих механізмів забезпечення інформаційної безпеки;

2. Відсутність забезпечення підготовки якісного кадрового складу систему публічного управління у сфері забезпечення інформаційної безпеки;

3. Формування інноваційних інформаційних небезпек, які потребують термінового та ефективного вирішення;

4. Відсутність інституцій, які комплексно забезпечуватимуть систему інформаційної безпеки в публічному управлінні. Відповідно до Закону України «Про національну безпеку» до складу сектору безпеки і оборони входять: Міністерство оборони України, Збройні Сили України, Державна спеціальна служба транспорту, та ін.

1.1.3 Шкідливі програми

Сьогодні, мабуть, годі й шукати користувача Інтернет, який не стикався б з вірусами, які надходять в його ОС з глобальної мережі. При відвідуванні ненадійних сайтів або скачуванні будь-якої інформації існує велика ймовірність завести у себе в комп'ютері декілька різноманітних вірусів, що згодом призведе до непередбачуваної поведінки апаратних і технічних засобів ПК або локальної мережі в цілому.

Комп'ютерний вірус — комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу.

Прийнято розділяти віруси:

• по ураженню об'єктів (файлові віруси, завантажувальні віруси, скріптові віруси, мережеві черв'яки);

• по уражається ОС і платформ (DOS, Microsoft Windows, Unix, GNU / Linux, Java та ін.);

• за технологіями, що використовуються вірусом (поліморфні віруси, стелс віруси);

• за мовою, на якій написано вірус.

Процес впровадження вірусом своєї копії в програму (системну область диска і т.д.) називається зараженням, а програма або інший об'єкт, підданий зараженню вірусом (вірус) - зараженим.

Коли заражена програма починає свою роботу, то спочатку управління отримує вірус, що знаходиться всередині неї. Вірус знаходить і «заражає» інші програми або інші об'єкти, а також може виконати будь-які ненавмисні дії. Потім вірус передає управління тій програмі, в якій він знаходиться, і вона працює так само, як зазвичай. Тим самим зовні робота зараженої програми виглядає так само, як і незараженной. Однак при кожному запуску зараженої програми в ОС користувача розмножується все більше і більше віруссодержащего програм, що призводить до збоїв в роботі комп'ютера.

Мережеві черв'яки - Worm

Мережними хробаками прийнято називати шкідливі програми, основна мета яких полягає в найбільшому поширенні на різноманітні мережеві пристрої. Існує різновид мережевих черв'яків, які носять назву безфайлових або пакетних. Вони

поширюються в вигляді мережевих пакетів, проникають безпосередньо в пам'ять комп'ютера і там активізують свій код. Подібні мережеві черв'яки користуються уразливими в програмному забезпеченні ОС.

Небезпечні типи файлів:

ins, js, msc, msi, pif, reg, scf, scr, vbs, asx, bas, bat, cmd, com, crt, exe, inf.

Як працює мережевий черв'як.

1. Мережевий черв'як потрапляє на комп'ютер. Для цього він використовує різні комп'ютерні та мобільні мережі: електронну пошту, IRC-і файлообмінні (P2P, від peer-to-peer, - рівний до рівного, однорангова, децентралізована або пірінгова мережу) мережі, LAN, мережі обміну даними між мобільними пристроями і т.д. Більшість мережевих черв'яків маскуються у вигляді файлів: вкладення в електронний лист, посилання на заражений файл на якому-небудь веб-або FTP-ресурсі в ICQ- і IRC-повідомленнях і т.д;

2. Створюється і запускається копія хробака;

3. Копія хробака прагне перейти в наступний пристрій: комп'ютери в Інтернет, локальної мережі і т.д.

Віруси-блокувальники — Winlock

Такі програми блокують користувачеві доступ до операційної системи. При завантаженні комп’ютеру з’являється вікно, в якому користувача звинувачують у скачуванні неліцензійного контенту або порушенні авторських прав. І під загрозою повного видалення всіх даних з комп’ютера вимагають відіслати смс на номер телефону або поповнити його рахунок. Звісно що після переказу грошей на рахунок зловмисника, банер нікуди не пропадає.

Віруси-шпигуни — Spyware

Шпигуни збирають інформацію про поведінку і дії користувача. Здебільшого їх цікавить інформація — адреси, паролі, дані кредитних карт.

Зомбі — Zombie

Віруси зомбі дозволяють зловмисникові керувати комп’ютером користувача. Комп’ютери — зомбі можуть бути об’єднані в мережу (бот-нет) і використовуватися

для масової атаки на сайти або розсилання спаму. Користувач може навіть не здогадуватися, що його комп’ютер зомбований і використовується зловмисником.

Рекламні віруси — Adware

Програми-реклами, без відома користувачів вбудовуються в різне програмне забезпечення з метою демонстрації рекламних оголошень. Як правило, програми-реклами вбудовані в програмне забезпечення, що поширюється безкоштовно. Реклама розташовується в робочому інтерфейсі. Найчастіше такі- програми також збирають і переправляють своєму розробникові персональну інформацію про користувача.

Троянські програми

Троянська програма - це шкідлива програма, яка використовується зловмисником для збору інформації, її руйнування або модифікації, порушення працездатності комп'ютера або використання його ресурсів в несприятливих цілях.

Троянська програма не здатна поширюватися саморозмноженням, як віруси, вона запускається користувачем вручну або автоматично - програмою або частиною ОС, що виконується на комп'ютері-жертві.

Для цього файл програми називають службовим ім'ям, що маскує його під будь-яку іншу програму, файл іншого типу або просто дають привабливе для запуску назва, іконку і т.п. При запуску вона завантажує приховані програми, команди і скрипти за згодою або без згоди і відома користувача. Троянська програма може в тій чи іншій мірі імітувати завдання або файл даних, під які вона маскується. Троянська програма може бути модулем вірусу, і отримавши можливість, самораспространяющемуся свої копії.

Метою троянської програми може бути закачування і викачування файлів.

1.1.4 Атаки та контратаки

Атаки на мережу призводять до відмови в обслуговуванні користувачам мережевого ресурсу. Мережевий ресурс може бути виведений з ладу різними шкідливими програмами або перевантажений в тому випадку, коли зловмисник посилає на атакується комп'ютер величезна кількість запитів. Така проблема носить назву - атака типу «відмова в обслуговуванні »або DoS-атака (Denial of Service). Принцип дії DoS-атак показаний на рис. 1.1.

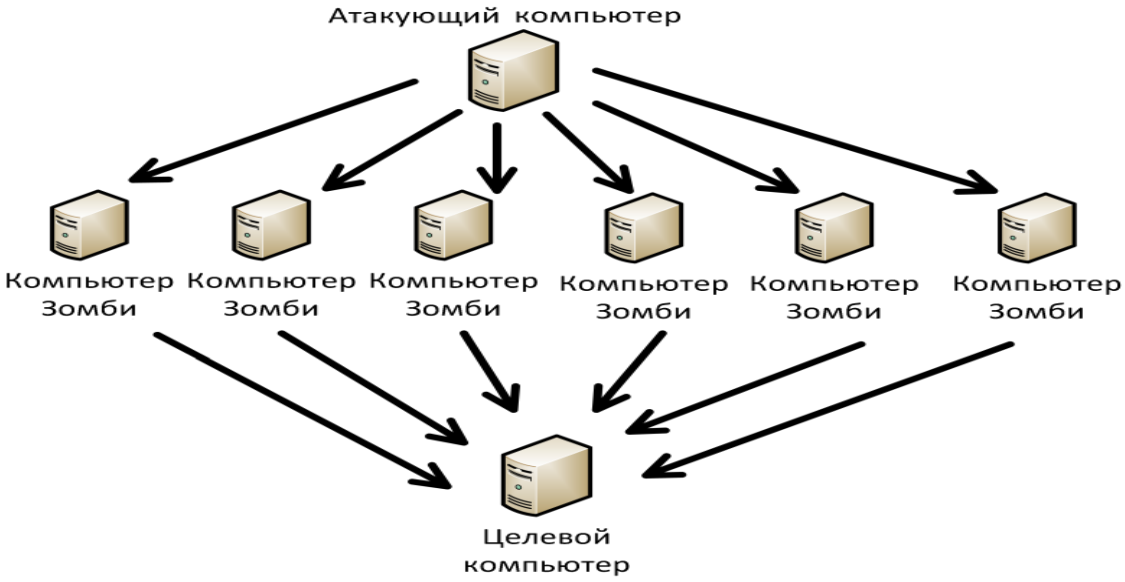


Рис. 1.1. Прінцип дії DoS-атак

Контрдії складаються в прийнятті превентивних заходів. Наприклад, система відмовляє атакуючому зловмисникові в доступі до сервісу за допомогою перевірки адрес вхідних пакетів даних і відкидання пакетів з підозрілими адресами.

1.1.5 Спам та фішинг

Спамом (від англ. - «spam») називається масова розсилка повідомлень рекламного характеру без згоди одержувачів. Термін спам з'явився в 1993 році. Спам в залежності від цілей і завдань відправника (спамера) може містити комерційну інформацію або іншу інформацію.

Зазвичай спамери використовують наступну схему: встановлюється SMTP-з'єднання з хостом, на якому дозволена пересилання пошти на будь-які хости (open mail relay - відкритий релей). На нього посилається лист з безліччю адресатів і, як правило, з підробленим адресою відправника. Хост, який опинився «жертвою», пересилає отримане повідомлення всім адресатам. В результаті, витрати на розсилку спаму лягають на одержувачів і хост, що пересилає пошту.

Інтернет-провайдери негативно ставляться до спаму, оскільки він створює досить істотне навантаження на їх системи і незручності їх користувачам. Багато провайдерів відключають прийом пошти з відкритих реле, помічених в передачі спаму. Система електронної пошти побудована таким чином, що розсилка відразу на величезну кількість адрес одного і того ж повідомлення коштує стільки ж, скільки і посилка одного-єдиного листа. Одержувач ж оплачує той час, який він витрачає на отримання цього непотрібного листа. Подібні розсилки масового характеру здатні помітно завантажити поштові сервери, через що можуть виникати затримки в отриманні важливої кореспонденції.

Фішинг (від англ. Phishing, від fishing - риболовля, видобування і password - пароль) - це вид інтернет-шахрайства, мета якого - отримати ідентифікаційні дані користувачів. Сюди відносяться крадіжки паролів, номерів кредитних карт, банківських рахунків та іншої конфіденційної інформації.

Фішинг являє собою прийшли на пошту підроблені повідомлення від банків, провайдерів, платіжних систем та інших організацій про те, що з якоїсь причини одержувачу терміново потрібно передати/оновити особисті дані.

Атаки фішерів стають все більш продуманими, застосовуються методи соціальної інженерії. Але в будь-якому випадку клієнта намагаються налякати,

придумати критичну причину для того, щоб він видав свою особисту інформацію. Як правило, повідомлення містять загрози, наприклад, заблокувати рахунок в разі невиконання одержувачем вимог, викладених в повідомленні. Часто в якості причини, по якій користувач нібито повинен видати конфіденційну інформацію, фішери називають необхідність поліпшити антифішинговий системи («якщо хочете убезпечити себе від фішингу, пройдіть по цьому посиланню і введіть свій логін і пароль»).

Для боротьби з такого роду атаками, перш за все не варто відповідати на листи сумнівного характеру, використовувати спеціальні програми-фільтри, які здійснюють перевірку пошти на утримання спаму і видалення таких листів прямо на поштовому сервері.

1.2 Засоби забезпечення інформаційної безпеки

Існує три фундаментальних способу забезпечення інформаційної безпеки. Організація інформаційної безпеки може проводитися за допомогою застосування організаційних, апаратних (технічних) або програмних засобів захисту інформації. Найбільша ефективність буде отримана в разі застосування комплексного захисту вище перелічених варіантів. Вище вказані способи можуть бути реалізовані різноманітними засобами.

Для захисту периметра інформаційної системи шляхом застосування організаційних засобів створюються:

• системи охоронної та пожежної сигналізації;

• системи цифрового відео спостереження;

• системи контролю та управління доступом (СКУД) і ін.

Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами та заходами:

• використанням екранованого кабелю і прокладкою проводів і кабелів в екранованих конструкціях;

• установкою на лініях зв'язку високочастотних фільтрів;

• побудовою екранованих приміщень («капсул»);

• використанням екранованого обладнання;

• установкою активних систем зашумлення;

• створенням контрольованих зон та ін.

До апаратних засобів захисту відносяться різні електронні, електронно-механічні, електронно-оптичні пристрої.

До теперішнього часу найбільшого поширення набули такі апаратні засоби:

• спеціальні регістри для зберігання реквізитів захисту: паролів, ідентифікують кодів, грифів або рівнів секретності;

• пристрої вимірювання індивідуальних характеристик людини (голоси, відбитків) з метою його ідентифікації;

• схеми переривання передачі інформації в лінії зв'язку з метою періодичної перевірки адреси видачі даних;

• використання мережевих єкранів;

• пристрої для шифрування інформації (криптографічні методи) і ін.

Програмно-технічні засоби і способи забезпечення інформаційної безпеки є основою системи захисту інформації. Це сукупність алгоритмів, програм і протоколів, що забезпечують шифрування, контроль за НСД, захист від шкідливих програм і багато іншого.

Ось деякі з таких засобів захисту інформації:

• Засоби захисту від несанкціонованого доступу;

• Системи виявлення й запобігання вторгнень;

• Системи запобігання витоків конфіденційної інформації (DLP-системи);

• Аналізатори протоколів;

• Антивірусні програми;

• Міжмережеві екрани (брандмауери);

• Криптографічні засоби:

• Шифрування;

• Цифровий підпис.

• Системи резервного копіювання та ін.

Застосування зазначених способів і засобів повинні забезпечити користувачеві впевненість в тому, що:

• сторонні особи не отримували доступ до його даних;

• дані відправлені саме тим, від чийого імені отримані;

• прийняті дані не були змінені шляхом від відправника до одержувача;

• відсутній доступ до ресурсу без відповідних повноважень (НСД) і ін.

У дипломній роботі акцент зроблений на розгляд апратно-технічніх засобів захисту інформації, оскільки їх функціональна роль в забезпеченні інформаційної безпеки носить фундаментальний характер та стоїть в базі работи з мережевим обладнання та безпекою мережі загалом.

1.2.1 Антивірусні программи

Це програма для виявлення комп'ютерних вірусів, небажаних (вважаються шкідливими) програм і відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики - запобігання зараженню (модифікації) файлів або ОС шкідливим кодом.

Класифікація антивірусів за принципом їх дії:

• Сканери - принцип їх роботи полягає в пошуку в файлах, пам'яті і завантажувальних секторах унікального програмного коду вірусу - вірусних масок. Вірусні маски (опису) містяться в антивірусній базі даних, і якщо сканер зустрічає програмний код, що співпадає з одним з цих описів, то він видає повідомлення про виявлення відповідного вірусу;

• Ревізори - запам'ятовують стан комп'ютера, стежать за змінами файлової системи і сповіщають про важливі або підозрілих змінах користувачеві;

• Монітори - є різновидом сканерів, які постійно перебувають в пам'яті комп'ютера і здійснюють автоматичну перевірку всіх використовуваних файлів в масштабі реального часу. Сучасні монітори здійснюють перевірку в момент відкриття і закриття програми;

• Вакцини (іммунізатори) - поділяються на два види: іммунізатори, повідомляють про зараження, і іммунізатори, блокуючі зараження яким-небудь типом вірусу;

Класифікація антивірусів по їх функціональному призначенню:

• Антишпіон (antispyware) - антивірусна програма, призначена для виявлення і видалення шпигунського ПЗ (spyware) з комп'ютера користувача;

• Онлайн-сканер - антивірусний засіб для виявлення і видалення вірусів з файлової системи персонального комп'ютера, підключеного до мережі Інтернет. Їх основною перевагою є відсутність необхідності інсталяції програми. Недоліком є те, що сканер тільки виявляє віруси, які вже проникли в систему і не здатний захистити комп'ютер від майбутнього зараження;

• Мережевий екран (firewall) - це програма, яка забезпечує безпечну роботу комп'ютера в мережі, яка дозволяє блокувати небажаний мережевий трафік, а також забезпечує невидимість комп'ютера в мережі, з метою запобігання хакерських атак;

• Комплексний захист - програмні пакети, які надають в собі всі перераховані вище засоби захисту комп'ютера плюс додаткові функціональні компоненти. Можуть містити антивірус, мережевий екран, антишпигун, захист від фішингу, антиспам, засіб резервного копіювання даних.

Як антивірусна програма знаходить вірус в системі:

За кожним існуючим вірусом закріплений унікальний для нього шматок коду, так звана сигнатура. Цей шматок коду зберігається в базі антивіруса, і якщо такий шматок коду знайдений у файлі, то такий файл визначається як відповідний вірус. Після знаходження підозрілого файлу, в залежності від налаштувань встановленого на ПК антивіруса, користувач або отримує повідомлення на право вибору «долі» даного файлу, або антивірусна програма сама вирішує це за нього. Однак для того, щоб в базі сигнатур антивірусної програми з'явився прописаний унікальний код вірусу, цей вірус повинен потрапити на аналіз вірусним аналітикам фірми розробника антивірусного забезпечення. Це досить довгий шлях, тому що щодня з'являються тисячі нових різновидів вірусів, а програма-антивірус повинна якісно захищати ПО. Для вирішення такої проблеми регулярно з'являються оновлення для

антивірусів, а також певні антивірусні програми наділені такою властивістю як евристичний аналіз.

Евристичний аналіз працює по іншому, ніж вище викладені бази сигнатур. Він аналізує вміст файлу і шукає в ньому не сигнатуру, а послідовності операцій, типові для вірусів. Тому антивірусна програма має можливість виявлення вірусів, які ще не потрапили на дослідження вірусним аналітикам. Чим більш досконалий алгоритм евристичного аналізу використовує антивірус, тим він надійніший.

1.2.2 Мережеві екрани, загальний огляд та порівняння мережевих екранів

Створення захищеної системи - завдання комплексне. Один із заходів забезпечення безпеки - використання міжмережевих екранів (вони ж брандмауери і файрволи). Як усі ми знаємо, брандмауери бувають програмними і апаратними. Можливості і перших, і других - не безмежні.

Фаєрволи (міжмережеві екрани) - наріжний камінь будівлі IT-безпеки, як для корпоративних бізнес-додатків, так і додатків, націлених на автоматизацію виробництва. Але наскільки вони безпечні? Фаєрволи з нами вже 25 років, але, незважаючи на цей довгий термін, їх обмеження все ще не цілком відомі широкому загалу, зацікавленої в питаннях забезпечення IT-безпеки (виняток - фахівці рівня експерта, як провідні легальну діяльність, так і ті, хто займаються протизаконною діяльністю).

Програмні і апаратні файрволи

Насамперед потрібно поговорити, що є програмним, а що - апаратним рішенням. Всі ми звикли, що якщо купується якась «залізяка», то це рішення називається апаратним, а якщо коробочка з програмним забезпеченням, це ознака програмного рішення. На наш погляд, різниця між апаратним та програмним рішенням досить умовна. Що являє собою залізна коробочка? По суті, це той же комп'ютер, нехай з іншою архітектурою, нехай з трохи обмеженими можливостями (до нього не можна підключити клавіатуру і монітор, він «заточений» під виконання однієї функції), на який встановлено ПО. ПО - це якийсь варіант UNIX-системи з

«веб-мордою». Функції апаратного брандмауера залежать від використовуваного фільтра пакетів (знову-таки - це ПЗ) і самої «веб-морди». Всі апаратні брандмауери можна «перепрошити», тобто по суті, просто замінити ПЗ. Та й зі справжньою прошивкою (яка в старі-добрі часи виконувалася за допомогою програматора) процес оновлення «прошивки» на сучасних пристроях має мало що спільного. Просто на «флешку» всередині «залізяки» записується нове ПЗ. Програмний брандмауер - це ПЗ, яке встановлюється на вже наявний самий звичайний комп'ютер, але у випадку з апаратним брандмауером - без ПО ніяк, а у випадку з програмним - без «заліза» ніяк. Саме тому грань між даними типами міжмережевих екранів вельми умовна.

Найбільша різниця між програмним і апаратним брандмауером навіть аж ніяк не функціональність. Ніхто не заважає вибрати апаратний брандмауер з потрібними функціями. Різниця в способі використання. Як правило, програмний брандмауер встановлюється на кожен ПК мережі (на кожен сервер і на кожну робочу станцію), а апаратний брандмауер забезпечує захист не окремої ПК, а всієї мережі відразу. Звичайно, ніхто не завадить вам встановити апаратний брандмауер для кожного ПК, але все впирається в гроші. З огляду на вартість «залізяк», навряд чи вам захочеться захищати кожен ПК апаратний брандмауер.

Переваги апаратних брандмауерів

У «залізних» міжмережевих екранів спостерігаються такі переваги:

Відносна простота розгортання і використання. Підключив, включив, поставив параметри через веб-інтерфейс і забув про його існування. Втім, сучасні програмні міжмережеві екрани підтримують розгортання через ActiveDirectory, на яке теж не піде багато часу. Але, по-перше, не всі брандмауери підтримують ActiveDirectory, і, по-друге, не завжди на підприємстві використовується Windows.

Розміри і енергоспоживання. Як правило, апаратні брандмауери мають більш скромні розміри і менше енергоспоживання. Не завжди, правда, енергоспоживання грає роль, а ось розміри важливі. Одна справа невелика компактна коробочка, інше - величезний «системник».

Продуктивність. Зазвичай продуктивність у апаратного рішення вище. Хоча б тому, що апаратний міжмережевий екран займається тільки своєю безпосередньою функцією - фільтрацією пакетів. На ньому не запущені будь-які сторонні процеси і служби, як це часто буває у випадку з програмними брандмауерами. Ось уявіть, що ви організували програмний шлюз (з функціями брандмауера і NAT) на базі сервера з Windows Server. Навряд чи ви будете виділяти цілий сервер тільки під брандмауер і NAT. Це нераціонально. Швидше за все, на ньому будуть запущені і інші служби - той же AD, DNS і т.д. Вже мовчу про СУБД і поштові служби.

Надійність. Вважається, що апаратні рішення більш надійні (саме через те, що на них рідко коли виконуються сторонні служби). Але ніхто вам не заважає виділити окремий системник (нехай навіть не найсучасніший), встановити на нього ту ж FreeBSD (одна з найнадійніших в світі операційних систем) і налаштувати правила брандмауера. Думаю, надійність такого рішення буде не нижче, ніж у випадку з апаратним файрволом. Але таке завдання вимагає підвищеної кваліфікації адміністратора, саме тому раніше було відзначено, що апаратні рішення більш прості у використанні.

Переваги програмних міжмережевих екранів

До переваг програмних рішень відносяться:

Вартість. Ціна програмного брандмауера зазвичай нижче «залізяки». За ціну середнього апаратного рішення можна захистити всю мережу програмним брандмауером.

Можливість захисту мережі зсередини. Не завжди загрози походять ззовні. Усередині локальної мережі є безліч загроз. Атаки можуть виходити з внутрішніх комп'ютерів. Ініціювати атаку може будь-який користувач LAN, наприклад, незадоволений компанією. Як вже зазначалося, можна, звичайно, використовувати окремий апаратний маршрутизатор для захисту кожного окремого вузла, але на практиці нам таких рішень не зустрічалися. Аж надто вони нераціональні.

Можливість розмежування сегментів локальної мережі без виділення підмереж. У більшості випадків до локальної мережі підключаються комп'ютери різних відділів, наприклад, бухгалтерії, фінансового відділу, IT-відділу і т.д. Не

завжди ці комп'ютери повинні взаємодіяти між собою. Як виконати розмежування ІСПДн? Перше рішення полягає в створенні декількох підмереж (наприклад, 192.168.1.0, 192.168.2.0 і т.д.) і налаштування належним чином маршрутизації між цими підмережми. Не можна сказати, що рішення дуже складне, але все ж складніше, ніж використання програмного файрвола. Та й не завжди можна виділити підмережі з тих чи інших причин. Друге рішення полягає у використанні брандмауера, призначеного саме для захисту ІСПДн (не у всіх програмних міжмережевих екранах легко розмежувати ІСПДн). У цьому випадку навіть в найбільшій мережі ви виконаєте розмежування ІСПДн за лічені хвилини, і вам не доведеться возитися з налаштуванням маршрутизації.

Можливість розгортання на існуючих серверах. Немає сенсу купувати ще одну «залізяку», якщо є достатній комп'ютерний парк. Досить на одному з серверів розгорнути міжмережевий екран і налаштувати NAT і машрутізацію. Зазвичай обидві ці операції виконуються за допомогою графічного інтерфейсу брандмауера і реалізуються за допомогою декількох клацань мишею в потрібних місцях.

Розширений функціонал. Як правило, функціонал програмних міжмережевих екранів ширше, ніж у їх апаратних побратимів. Так, деякі міжмережеві екрани надають функції балансування навантаження, IDS / IPS і тому подібні корисні речі, що дозволяють підвищити загальну безпеку системи обробки даних. Так, такі функції є не у всіх програмних брандмауерів, але ніщо і ніхто не заважає вам вибрати міжмережевий екран, відповідний вашим потребам. Звичайно, такі функції є і у деяких апаратних комплексів. Наприклад, StoneGate IPS - надає функціонал системи запобігання вторгнень, але вартість таких рішень не завжди сподобається керівництву підприємства. Також є і апаратні балансувальник навантаження, але вони коштують ще дорожче, ніж апаратні IPS.

Про недоліки писати не будемо - вони слідують з переваг. Переваги одного виду брандмауерів зазвичай є недоліками іншого виду. Наприклад, до недоліків апаратних рішень можна віднести вартість і неможливість захисту локальної мережі зсередини, а до недоліків програмних - складність розгортання і використання (хоча, як було відзначено, все відносно).

Правда, є один недолік апаратних міжмережевих екранів, про який варто згадати. Як правило, у всіх апаратних міжмережевих екранів є кнопка скидання, натиснувши яку можна повернути параметри за замовчуванням. Для натискання цієї кнопки не потрібно володіти якоюсь особливою кваліфікацією. А ось, щоб змінити параметри програмного брандмауера, потрібно, як мінімум, отримати права адміністратора. Натиснувши одну кнопку, незадоволений співробітник може негативно вплинути на безпечність всього підприємства (або залишити підприємство без доступу до Інтернету, що навіть краще тому як витік інформації може коштувати на багато дорожче ніж 1-2 години відсутності доступу до інтернету, також необхідно розуміти що Fortinet надає змогу залишити доступ до інтернету та відключити лише робочу станцію співробітника). Тому при використанні апаратних рішень потрібно більш відповідально підійти до питань фізичної безпеки самих пристроїв.

Захист інформаційної системи повинна бути комплексною - це і програмні, і апаратні брандмауери, і антивіруси, і відказо стійке налаштування самої системи. Що ж стосується нашого протистояння між програмними і апаратними брандмауерами, то перші ефективно використовувати для захисту кожного вузла мережі, а останні - для захисту всієї мережі в цілому. Апаратний брандмауер не може забезпечити захист кожної окремої робочої станції, безсилий при атаках всередині мережі, а також не може виконати розмежування ІСПДн, які слід виконувати в контексті захисту персональних даних.

1.2.3 Порівняння Fortinet та Palo Alto

Fortinet та Palo Alto є одними зі світових компаній на ринку мережевої безпеки. На даний момент NGFW є ключовим рішенням на ринку ІБ, без якого ми не можемо уявити повноцінний захист компаній будь-якого розміру. Такі світові компанії як Ubisoft, CD Project, Nether Realms та інші великі компанії з розробки світових ігор обирають рішення безпеки на базі Fortinet та Palo Alto. За допомогою ціх рішень компанії мають змогу вирішувати проблеми з безпекою та побудуванням безпечних

каналів зв’язку між своїми філіалами та іншими компаніями, які беруть участь в розробці найдорожчих ігор на планеті, та в усій індустрії загалом.

Загалом Fortinet та Palo Alto мають збіжний функціонал у своїх можливостях. Palo Alto Networks був одним із перших постачальників апаратних брандмауерів, представлених на ринку FWaaS. Він представив DLP для Prisma Access. Palo alto надає змогу використовувати рішення IPS на рівні TLS та розшифровувати весь трафік що надходить до клієнтів навіть при роботі з сервісами Google, за допомгою зміни TLS сертифікату на рівні NGFW.

Обидва постачальники чудові. Fortinet отримав рейтинг ефективності безпеки 99,3% NSS Labs в опублікованих результатах тестування, а Palo Alto отримав оцінку 98,7%. Однако багато мережевих адміністраторів відзначають що керування та налаштування засобів безпеки набагато легше відтворюється на базі систем Fortinet.

Обидві системи мають рішення які відсутні на звичайних роутерах, а саме вбудований VPN сервер, що надає змогу автоматично відтворювати та оновлювати маршрути що отримуються в реальному часі. Forti SSL та Global Protect мають глибоку систему контролю користувачів та гнучкі інтеграції з іншими системами, а саме 2FA сервісами наприклад як PrivicyIdea що генерує тимчасові коди авторизації, та дає змогу інсталяції приватного серверу в мережі компанії. Також що найбільш важливо є глубокі інтеграції з системами антивірусів таких як ESET. Глубока інтеграція з системами Windows та Active Directory надає змогу мережевому адміністратору не займатися створенням облікових записів на самому NGFW, а отримувати облікові записи по LDAP. Що не менш важливо ми маємо змогу створити правила доступу до критичних ресурсів та надавати мережевий доступ при отриманні користувачем відповідної групи в Active Directory. За допомогою такого рішення ми маємо подвійний контроль доступу у різних системах.

Обидві системи мають контроль доступу за допомогою HIP profile, таким чином ми можемо захистити доступ до корпоративної мережі при підключенні через системи віддаленого доступу а саме за допомогою вендорних VPN клієнтів. Для того щоб отримати доступ до корпоративної мережі, ми можемо налаштувати HIP matching, при якому VPN клієнт буде перевіряти наявність перевіреного сертифікату

компанії, налаштованого антивірусу компанії, встановленого DLP та інших профайлів безпеки що потребує безпека компанії при відповідній сертифікації. Таким чином кліенти що будуть перевіряти можливості підключення з особистих персональних компьютерів будуть отримувати блокування в корпоративній системі, або інші блокування що передбачені відділом кібербезпеки.

Рішення дуже тісно схожі, відтворення різних систем захисту можливе у першого та другого постачальника систем захисту. Нажаль одне дуже важливе питання це є ціна цих рішень, зазвичай рішення на Palo Alto набагато дорожче. Це унеможливлює введення рішення проблем в компанії.

2. ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НА БАЗІ ОБЛАДНАННЯ FORTINET

2.1 Знайомство з компанією Fortinet, аналіз переліку обладнання компанії

Fortinet - американська транснаціональна корпорація. Її головний офіс розташований у місті Саннівейл (Каліфорнія). Компанія спеціалізується на розробці і просуванні програмного забезпечення, рішень і сервісів в області інформаційної безпеки: міжмережевих екранів, антивірусних програм, систем запобігання вторгнень і забезпечення безпеки кінцевих точок і інших продуктів. За обсягом виручки компанія займає четверте місце серед всіх компаній, що спеціалізуються в області мережевої безпеки.

Компанія Fortinet була заснована в 2000 році братами Кеном і Майклом Кси.

Першим продуктом Fortinet став пристрій FortiGate 3000, випущене в жовтні 2002 року, пропускна здатність якого становила 3Гб/с. Сімейство пристроїв 5000 було випущено двома роками пізніше. Згідно з інформацією ресурсу The International Directory of Company Histories, ранні продукти Fortinet були для малих компаній і філій та користувалися популярністю в галузі кібербезпеки.

У 2004 році між компаніями Fortinet і Trend Micro почали виникати періодичні патентні суперечки. У 2009 році компанія вийшла на відкритий ринок і залучила кошти в сумі 156 млн доларів США за допомогою первинної публічної пропозиції. Протягом 2000-х років Fortinet розширювала асортимент своєї продукції, представляючи, серед інших, «пісочницю», рішення в області захисту бездротових точок доступу, і електронної пошти.

Компанія найбільш відома завдяки сімейству засобів забезпечення безпеки FortiGate – який є головним продуктом компанії Fortinet, які поєднують безліч функцій по захисту інформації.

Сімейство фізичних і віртуальних рішень FortiGate компанії Fortinet в області уніфікованого управління погрозами включає такі функції забезпечення безпеки, як

міжмережеві екрани, засоби запобігання вторгнень, веб-фільтри і захист від шкідливого програмного забезпечення або небажаної пошти. У сімейство входять продукти для малих компаній і філій, а також рішення для підприємств, центрів обробки даних і інтернет-провайдерів. Компанія також реалізує міжмережеві екрани нового покоління (Next Generation Firewalls, NGFW), які компанія Gartner охарактеризувала як пристрої, що поєднують в собі можливості брандмауера, VPN, системи запобігання вторгнень і інші функції забезпечення безпеки.

У цьому пристрої застосовані нові розробки в області безпеки мережі, які допоможуть захистити ресурси мережі, оптимізувати витрати на створення системи захисту. Головною особливістю пристроїв є застосування апаратних ресурсів спеціально для виконання ресурсномістких операцій: антивірусний аналіз сигнатурний і сигнатурний системний аналіз виявлення вторгнень.

Всі пристрої FortiGate - від серії FortiGate-30E для малих підприємств і вже закінчуючи моделями FortiGate-7500 для великих підприємств / постачальників послуг - об'єднали в собі операційну систему FortiOS, процесор FortiASIC та інші функції безпеки мережі. Продукти FortiGate мають високоефективним комплексом функцій для забезпечення безпеки і створення мереж, включаючи:

- Маршрутизація - статична, RIP, OSPF, BGP, політика маршрутизації на основі, маршрутизація групова;
- Екран міжмережевий - захищеність на основі політик трафіку, призначених для користувача груп, особистий набір сервісів безпеки для всіх категорій;
- Аутентифікація користувача по локальній базі користувачів, TACACS +, RADIUS, LDAP, Microsoft Active Directory;
- VPN-концентратор - IPSec VPN (LAN-к-LAN, Віддалений доступ), SSL VPN (веб режим, режим тунелю), PPTP, IKE v1 / v2, Diffie-Hellman до 2048;
- Антивірус - перевірка на віруси веб-трафіку (HTTP), вкладень електро. пошти (SMTP, POP3, IMAP), FTP, протоколів обміну швидкими повідомленнями (Yahoo, AIM, ICQ, MSN,) протокол передачі новин (NNTP). Автопоновлення сигнатур (push-режим). Апаратні прискорювачі на базі процесорів FortiASIC;

- Антиспам - он-лайн база репутацій, IP / електронної пошти DNSBL і ORDBL, BWL, HELO пошук DNS, заборона на контрольне слово, повернення електронної пошти на перевірку DNS;
- Система запобіжників вторгнення (IPS) - використовуються встановлені сигнатури для безпеки додатків, операційних систем, присутня можливість створення своїх сигнатур;
- Контроль до мережевого доступу (NAC) - контроль до мережевого доступу кінцевих користувачів пристроїв, перевірить наявність потрібного переліку встановлених програм на пристрої, за підсумками перевірки дозвіл / заборона доступ до мережі;
- Веб / контент фільтр - використання он-лайн класифікатора веб-сайтів, контроль ActiveX, Cookie, контроль URL, Java Applet, вмісту веб;
- Контроль додатків P2P, IM, VoIP, баз даних і більше 1000 додатків - контроль використання протоколів швидких повідомлень (Yahoo, AIM, ICQ, MSN,), P2P протоколів (WinNY, BitTorrent, eDonkey, Kazaa, Gnutella), протоколів голосової передачі поверх IP (SIP, H.323, SCCP, Скайп), захищеність різних додатків і протоколів (баз даних, систем архівування та ін.);
- Оптимізація і кешування трафіку WAN - підвищує ефективність використання смуги пропускання, оптимізує протоколи HTTP, TCP, FTP, CIFS, MAPI, кешування трафіку (моделі з FortiGate-51B, 81см, 310B, 620B, 111C, 3000, 5000 з жорстким диском);
- Запобігання витоків даних (DLP) - антіраспространеніе особистої інформації по FTP, HTTP, NNTP, ел. поштою, систему швидких повідомлень;

Інспектування трафіку SSL - перевірка інформації всередині тунелів SSL:

- антивірус, DLP, архівування контенту під протоколи IMAPS, HTTPS, POP3S, SMTPS;
- веб-фільтрація для протоколу HTTPS;
- антиспам для протоколів POP3S, IMAPS, SMTPS, (в моделях 111C, 110C, 310B, 620B, 3000, 5000);

- формування трафіку - гарантія / ліміт / пріоритети смуги передачі даних, для користувальницької групи, для конкретного IP-адреси, квотування всього обсягу інформації;
- NAT, балансування навантаження - статичний / динамічний NAT, базовий SIP / H.323 NAT traversal, NAT, баланс навантаження;
- Віртуальний домен (VDOM) - віртуалізація пристроїв. Побудова віртуальних пристроїв в рамках єдиного фізичного. Автономне управління політикою, функцією безпеки, таблицею маршрутизації, балками подій, поліпшенням трафіку;
- Висока доступність - режим спільної відмовостійкої роботи 2-ух пристроїв. Підтримуються режими Active / Standby, Active / Active;
- Підтримку IPv6 - підтримується протокол IPv6 - динамічна маршрутизація динамічна, екран міжмережевий, DNS, сканування на віруси трафіку IPv6, прозорий режим, адмін. доступ до пристрою;
- VLAN / LACP - підтримується VLAN 802.1q, підтримка канального об'єднання 802.1ad LACP;
- Подключаемості до 3G / CDMA мереж - підключення PCMCIA, USB, модемів;
- Моніторинг та управління - управління з Веб-інтерфейсу, CLI (ssh, телнет, консоль), Forti-менеджер, Forti-аналіз;
- Модуль розширення - моделі оснащені слотами розширення можливо доукомплектувати модулями;
- FortiGate-Voice-80C - об'єднання UTMFG-voice-80C пристрої з голосовим шлюзом (VoIP шлюз) і IP PBX.

На початку 2013 року компанія Fortinet включила в засоби Fortigate функцію брандмауера, призначену для роботи у внутрішніх мережах і працюючу на мікросхемах спеціального призначення (ASIC). Пізніше в 2014 році до платформи Amazon Web Services були додані віртуальні кошти FortiGate. У квітні 2016 року Fortinet представила адаптивну систему мережевої безпеки Fortinet (Fortinet Security

Fabric), призначену для забезпечення обміну інформацією між пристроями сторонніх виробників і пристроями або програмним забезпеченням Fortinet через API. Компанія також представила міжмережевий екран FortiGate 6040E 320 Гбіт/с, що включав нову мікросхему CP9 ASIC, яка виконувала частину обчислювальних задач центрального процесора і використовувалася в подальших рішеннях FortiGate.

Згідно зі звітом 2015 року фірми Dell'Oro Group, що займається аналізом інформаційних технологій, частка ринку засобів інформаційного захисту, яку займає Fortinet, становила вісім відсотків в 2014 році в порівнянні з часткою в 2,9 відсотка в 2012 році. Завдяки цьому компанія займає четверте місце серед всіх постачальників у своїй галузі. Згідно з даними Fortinet, малі компанії складають 35% всіх користувачів, підприємства - 28%, а великі компанії - 37% серед її клієнтів.

Інші продукти

Fortinet надає безліч інших програмних і апаратних продуктів, включаючи більше десятка рішень для комутації, настільних систем, служб VOIP, DNS, перевірки автентичності користувачів і інших завдань.

Також компанія Fortinet виробляє і поставляє на ринок бездротові версії своєї продукції FortiGate під назвою FortiWifi. Вперше ці пристрої були представлені в березні 2004 року. У серпні 2015 року Fortinet представила нове сімейство хмарних бездротових точок доступу. У березні 2014 року презентували сімейство продуктів FortiDDoS.

Операційна система

Устаткування Fortinet працює під управлінням операційної системи FortiOS, як ядра якої використовується модифікована версія ядра Linux, і файлової системи ext2. У веб-інтерфейсі адміністрування використовуються шаблонизатор jinja2 і django, серверна частина реалізована на мові Python.

2.2 Технології виявлення вірусів на базі Fortigate

Grayware Scan або сканування небажаних програм - ця технологія визначає небажані програми, які встановлюються без відома чи згоди користувача. Технічно ці програми є вірусами. Зазвичай вони йдуть у комплекті з іншими програмами, але при установці негативно впливають на систему, тому вони класифікуються як шкідливі програми. Часто такі програми можна знайти за допомогою простих grayware сигнатур від дослідницької бази FortiGuard.

Евристичне сканування - дана технологія заснована на ймовірностях, тому її використання може спричинити false positives ефекти, проте з її допомогою можна виявити віруси zero day. Zero day віруси - нові віруси, які ще не досліджені, і поки що не існує сигнатур, які могли б їх виявити. Евристичне сканування не застосовується за замовчуванням, його потрібно активувати у командному рядку.

Якщо всі можливості антивірусу активовані, FortiGate застосовує їх у такому порядку: антивірусне сканування, grayware сканування, евристичне сканування.

FortiGate може використовувати кілька антивірусних баз, залежно від завдань:

Звичайна антивірусна база (Normal) міститься у всіх моделях FortiGate'ів. Вона включає сигнатури для вірусів, які були виявлені в останні місяці. Це найменша антивірусна база, тому при її використанні сканування виконується найшвидше. Проте ця база не може виявити всі відомі віруси.

Розширена (Extend) - ця база підтримується більшістю моделей FortiGate. З її допомогою можна виявити віруси, які не активні. Багато платформ все ще вразливі для цих вірусів. Також ці віруси можуть дати проблеми в майбутньому.

І остання, екстремальна база (Extreme) — використовується в інфраструктурах, де потрібний високий рівень безпеки. З її допомогою можна виявити всі відомі віруси, включаючи віруси, націлені на застарілі операційні системи, які на даний момент не поширені. Цей тип бази сигнатур також підтримується не всіма моделями FortiGate.

Також є компактна база сигнатур, призначена для швидкого сканування.

Оновлювати антивірусні основи можливо різними способами.

Перший метод – Push Update – він дозволяє оновлювати бази відразу, як тільки дослідницька база FortiGuard випускає оновлення. Це корисно для інфраструктур, яким необхідний високий рівень безпеки, оскільки FortiGate отримуватиме термінові оновлення одразу ж після того, як вони з'являться.

Другий метод - встановити розклад. Таким чином, оновлення можна перевіряти кожну годину, день або тиждень. Тобто тут тимчасовий діапазон ставиться на вашу думку. Ці методи можна використати разом. Але треба мати на увазі — щоб оновлення проводилися, необхідно включити профіль антивірусу хоча б на одну фаєрвольну політику. Інакше оновлення не проводитимуться. Також можна завантажувати оновлення із сайту підтримки Fortinet, а потім вручну завантажити їх на FortiGate.

Режими сканування. Їх всього три - Full Mode у Flow Based режимі, Quick Mode у Flow Based режимі, і Full Mode у проксі режимі. Почнемо з Full Mode у Flow режимі. Допустимо, користувач хоче завантажити файл. Він надсилає запит. Сервер починає посилати йому пакети, у тому числі складається файл. Користувач одразу отримує ці пакети. Але перед тим, як передати ці пакети користувачеві, FortiGate їх кешує. Після того як FortiGate отримує останній пакет, він починає сканувати файл. У цей час останній пакет ставиться у чергу і не передається користувачеві. Якщо файл не містить вірусів, останній пакет надсилається користувачеві. Якщо ж вірус виявлено, FortiGate розриває з'єднання з користувачем.

Другий режим сканування, доступний у Flow Based - Quick Mode. Він використовує компактну базу сигнатур, яка містить менше сигнатур, ніж стандартна база. Також він має деякі обмеження порівняно з Full Mode:

- Він не може надсилати файли в пісочницю
- Він не може використовувати евристичний аналіз

- Він не може використовувати пакети, пов'язані з мобільними шкідливими програмами
- Деякі entry level моделі не підтримують цей режим.

Quick mode також перевіряє трафік на вміст вірусів, хробаків, троянів та шкідливих програм, але без буферизації. Це забезпечує кращу продуктивність, але в той же час можливість виявити вірус знижується.

У Proxy режимі доступний єдиний режим сканування Full Mode. При такому скануванні FortiGate спочатку зберігає весь файл у себе (якщо, звичайно, не перевищиться допустимий розмір файлів для сканування). Клієнт повинен чекати, поки завершиться сканування. Якщо під час сканування буде виявлено вірус, користувач буде повідомлено відразу. Оскільки FortiGate спочатку зберігає весь файл, а потім сканує його, це може забрати багато часу. через це з боку клієнта можливе завершення з'єднання до отримання файлу через тривалу затримку.

2.3 Технології запобігання вторгненням на базі Fortigate

В системі IPS необхідно розібрати відміну експлойтів від аномалій, а також зрозуміти, які механізми використовує FortiGate для захисту від них.

Експлойти - це відомі атаки, з конкретними патернами, які можна виявити за допомогою IPS, WAF або антивірусних сигнатур.

Аномалії - це незвичайна поведінка в мережі, наприклад незвичайно великий обсяг трафіку або більше, ніж зазвичай споживання CPU, аномалії необхідно відстежувати, оскільки вони можуть бути ознаками нової, ще невивченої атаки. Аномалії зазвичай виявляються за допомогою поведінкового аналізу – так званих rate-based сигнатур та DoS політик.

За підсумками - IPS на FortiGate використовує сигантурні бази для виявлення відомих атак, і Rate-Based сигнатури та політики DoS для виявлення різних аномалій.

За замовчуванням початковий набір IPS сигнатур включено до кожної версії операційної системи FortiGate. За допомогою оновлень FortiGate отримує нові

сигнатури. Таким чином, IPS залишається ефективним проти нових експлойтів. Сервіс FortiGuard оновлює сигнатури IPS досить часто.

Важливий момент, який стосується як IPS, так і антивірусу — якщо у вас закінчилися ліцензії, ви все одно можете використовувати останні отримані сигнатури. Але отримати нові без ліцензій не вдасться. Тому відсутність ліцензій вкрай небажана — з появою нових атак ви не зможете захиститись старими сигнатурами.

Основи IPS сигантур поділяються на стандартну і розширену. Звичайна база містить сигнатури для поширених атак, які дуже рідко або взагалі не викликають помилкових спрацьовувань. Передбачена дія для більшості таких сигнатур - блок.

Розширена база містить додаткові сигнатури атак, які сильно впливають на продуктивність системи, або які не можна заблокувати через їхню особливу природу. Через розмір такої бази вона недоступна для моделей FortiGate з маленьким диском або RAM. Для високозахищених середовищ може знадобитися використовувати розширену базу.

2.4 Технології профілів безпеки на базі Fortigate

Режим інспекції

Режими інспекції поділяються на:

- Flow Based
- Proxy Based.

За замовчуванням використовується режим Flow Based. Він перевіряє файли, коли вони проходять через FortiGate без буферизації. Як тільки пакет перебуває, він обробляється і передається далі, без очікування на отримання цілого файлу або веб-сторінки. Він вимагає менше ресурсів і забезпечує більшу продуктивність, ніж Proxy режим, але в той же час у ньому доступний не весь функціонал Security. Наприклад, систему запобігання витоку даних (DLP) можна використовувати лише в Proxy режимі.

Proxy режим працює інакше. Він створює два TCP з'єднання, одне між клієнтом та FortiGate'ом, друге між FortiGate'ом та сервером. Це дозволяє йому буферизувати трафік, тобто отримувати повний файл або веб-сторінку. Сканування файлів на різні загрози починається лише після того, як весь файл забуферизувався. Це дозволяє використовувати додаткові можливості, які недоступні у Flow based режимі. Як бачите, цей режим ніби протилежність Flow Based - безпека тут відіграє головну роль, а продуктивність відходить на другий план.

Web Filtering

Web Filtering допомагає контролювати або відстежувати, які веб-сайти відвідують користувачі. Після того, як встановлено з'єднання TCP, користувач за допомогою запиту GET запитує вміст певного веб сайту.

Якщо веб-сервер відповідає позитивно, він надсилає інформацію про веб-сайт у відповідь. Тут у справу вступає веб-фільтр. Він перевіряє вміст цієї відповіді. Під час перевірки FortiGate в режимі реального часу відправляє запит у FortiGuard Distribution Network (FDN), щоб визначити категорію даного веб-сайту. Після визначення категорії конкретного веб-сайту, веб-фільтр, залежно від налаштувань виконує конкретну дію.

У Flow режимі є три дії:

- Allow — дозволити доступ до веб-сайту.
- Block — заборонити доступ до веб-сайту.
- Monitor — дозволити доступ до веб-сайту та записати це в логі.

У Proxy режимі додаються ще дві дії:

- Warning – видавати користувачеві попередження про те, що він намагається відвідати певний ресурс та дати користувачеві вибір – продовжити або піти з веб-сайту.
- Authenticate — запит облікових даних користувача — це дозволяє дозволити певним групам доступ до заборонених категорій веб-сайтів.

Application Control

Application Control дозволяє контролювати роботу програм. Працює це за допомогою патернів різних додатків, так званих сигнатур. За цими сигнатурами він може визначити конкретну програму і застосувати до неї певні дії:

- Allow – дозволити
- Monitor — дозволити та записати це в логування
- Block – заборонити
- Quarantine — записати подію в логування та заблокувати IP адресу на певний час

HTTPS інспекція

Згідно зі статистикою, за кінець 2018 року частка HTTPS трафіку перевищила 70%. Тобто, без використання HTTPS інспекції ми зможемо проаналізувати лише близько 30% трафіку, що ходить по мережі.

Клієнт ініціює TLS запит до веб-сервера та отримує TLS відповідь, а також бачить цифровий сертифікат, який повинен бути довіреним для даного користувача. Після успішного TLS хендшейка починається передача даних у зашифрованому вигляді. І це добре. Ніхто не може отримати доступ до даних, якими ви обмінюєтеся з веб-сервером.

Однак для безпеки компаній це велика проблема, оскільки вони не можуть бачити цей трафік і перевіряти його вміст ні антивірусом, ні системою запобігання вторгненням, ні DLP системами, нічим. Також це негативно відображається на якості визначення додатків і веб ресурсів, що використовуються всередині мережі. Вирішити цю проблему покликана технологія HTTPS інспекції. Її суть дуже проста - фактично, пристрій, який займається інспекцією HTTPS, організує атаку Man In The Middle. Виглядає це приблизно так: FortiGate перехоплює запит користувача, організує з ним HTTPS з'єднання, і вже від себе піднімає HTTPS сесію з ресурсом, до якого звернувся користувач. При цьому на комп'ютері користувача буде видно сертифікат, випущений FortiGate'ом. Він повинен бути довіреним, щоб браузер дозволив підключення.

2.5 Технології міжмережевого екранування на базі Fortigate

Політики міжмережевого екранування є сукупність критеріїв, на відповідність яким перевіряються пакети, що потрапляють на міжмережевий екран. Тут варто відзначити, що FortiGate є state full фаєрволом, тобто міжмережевим екраном із запам'ятовуванням сесій. Це означає, що якщо перший пакет у сесії був дозволений політикою міжмережевого екранування, то далі будь-які пакети в рамках цієї сесії на відповідність політикам не перевіряються – ця сесія запам'ятовується та дозволяється. Далі перевіряється лише трафік у рамках контент-інспекцій.

Важливо: трафік перевіряється на відповідність політикам строго зверху вниз. Якщо трафік підпадає під всі критерії політики — дія, вказана у політиці, застосовується до цього трафіку (accept або deny). Якщо трафік не підійшов під критерії всіх політик, до нього застосовується неявна політика — Implicit Deny, і цей трафік відкидається.

Перші три критерії - це вхідні інтерфейси, вихідні інтерфейси і джерело. Як вхідний і вихідний інтерфейс можуть виступати як один, так кілька інтерфейсів. Однак за промовчанням використання кількох інтерфейсів у політиках вимкнено, у відео уроці показано як увімкнути цю опцію. Окремий випадок використання кількох інтерфейсів – інтерфейс Any. Він включає всі можливі інтерфейси. Також як інтерфейси можна використовувати попередньо налаштовану зону - логічну групу інтерфейсів.

Як джерело можна використовувати велику кількість об'єктів, вони представлені на слайді. Але є певні правила - як джерело обов'язково має бути зазначений хоча б один з наступних об'єктів: IP адреса або діапазон IP адрес, підмережа, FQDN, географічне розташування або об'єкти з бази даних інтернет сервісів. Далі, за бажанням, можна конкретизувати політику, обравши користувача, групу користувачів або конкретний пристрій. Користувачі та групи користувачів можуть бути як локальними, так і віддаленими.

Як і критерій джерело, критерій призначення може використовувати такі об'єкти: IP адреса або діапазон адрес, підмережі, FQDN, географічне розташування або об'єкти бази даних інтернет сервісів.

Якщо використовувати FQDN, необхідно переконайтися, що взаємодія FortiGate та DNS серверів налаштована коректно, оскільки Fortigate використовує DNS запити, щоб визначити IP-адреси FQDN імен.

Об'єкт Geography є групи або діапазони IP адрес, виділених певній країні. Такі об'єкти автоматично оновлюються через FortiGuard.

Також варто сказати пару слів про базу даних інтернет сервісів. Вона містить IP адреси, протоколи та номери портів популярних Інтернет-сервісів, таких як Amazon, Dropbox, Facebook і так далі. Ці дані також автоматично оновлюються через FortiGuard.

Критерій сервіс визначає протоколи передачі (UDP/TCP тощо), і навіть номери портів. Можна користуватися встановленими сервісами, за необхідності також можна створити власні.

І останній критерій – розклад. Його можливо розділити на два типи: тривалий та одноразовий. У тривалому можна вибирати необхідні дні тижня та визначати час. У такому разі політика, до якої прив'язаний конкретний критерій розкладу, перевірятиме дату та час проходження пакету. Другий тип – одноразовий розклад. У такому випадку можна встановити дату та проміжок часу, які необхідні (наприклад, через одноразові роботи співробітникам буде потрібно віддалений доступ у конкретний день і конкретний час).

2.6 Технології логування на базі Fortigate

У FotiGate логі поділяються на три типи: логі трафіку, логи подій та логи безпеки. Вони ж у свою чергу поділяються на підтипи.

Логи трафіку записують інформацію про поток трафіку, такі як запити та відповіді, якщо вони є. Цей тип містить підтипи Forward, Local та Sniffer.

Підтип Forward містить інформацію про трафік, який FortiGate або прийняв, або відхилив відповідно до політиків міжмережевого екранування.

Підтип Local містить інформацію про трафік безпосередньо з IP адреси FortiGate та з IP адрес, з яких здійснюється адміністрування. Наприклад, підключення до веб-інтерфейсу FortiGate.

Підтип Sniffer містить логі трафіку, отриманого за допомогою дзеркалювання трафіку.

Логи подій містять системні або адміністративні події, такі як додавання або зміна параметрів, встановлення і розрив VPN тунелів, події динамічної маршрутизації і так далі.

Третій тип є логі безпеки. Дані логи записуються події, пов'язані з вірусними атаками, відвідуваннями заборонених ресурсів, використанням заборонених додатків і так далі.

Зберігати логи можна в різних місцях — як на FortiGate, так і за його межами. Зберігання логів на FortiGate є локальним логуванням. Залежно від пристрою зберігати логи можна або у флеш-пам'яті пристрою, або на жорсткому диску. Як правило, моделі від middle мають жорсткий диск. Моделі з жорстким диском відрізнити досить просто - закінчується одиниця. Наприклад – FortiGate 100E йде без жорсткого диска, а FortiGate 101E – з жорстким диском.

Молодші і старі моделі зазвичай жорсткого диска не мають. У такому разі для запису логів використовується флеш-пам'ять. Однак варто враховувати, що постійний запис логів у флеш-пам'ять може скоротити її ефективність та термін служби. Тому запис логів у флеш-пам'ять за замовчуванням вимкнено. Вмикати її рекомендується лише для логування подій під час вирішення конкретних проблем.

При інтенсивному запису логів, неважливо, на жорсткий диск або флеш-пам'ять — продуктивність пристрою буде знижуватися.

Досить поширене зберігання логів на віддалених серверах. FortiGate може зберігати логи на серверах Syslog, на FortiAnalyzer або FortiManager. Також для зберігання ліг можна використовувати хмарний сервіс FortiCloud.

Syslog є сервером для центрального зберігання логів з мережевих пристроїв.

FortiCloud — це служба керування безпекою та зберігання логів, яка базується на передплаті. З її допомогою можна віддалено зберігати логи та будувати відповідні звіти. Якщо у вас досить маленька мережа, вдалим рішенням може бути використання даного хмарного сервісу, а не покупка додаткового обладнання. Існує безкоштовна версія FortiCloud, яка має на увазі тижневе зберігання логів. Після придбання підписки можна зберігати логи протягом року.

FortiAnalyzer та FortiManager є зовнішніми пристроями зберігання логів. Завдяки тому, що всі вони мають однакову операційну систему — FortiOS — інтеграція FortiGate з даними пристроями не становить жодних складнощів.

Але слід зазначити відмінності між пристроями FortiAnalyzer та FortiManager. Основною метою FortiManager є централізоване управління декількома пристроями FortiGate - тому обсяг пам'яті для зберігання логів на FortiManager суттєво менший, ніж на FortiAnalyzer (якщо, звичайно, порівнювати моделі з одного цінового сегмента).

Основною метою FortiAnalyzer якраз є збір та аналіз логів

2.7 Порівняння мережевого екрану Fortigate 60e та Fortigate 100e

Компанії постійно знаходяться в пошуку рішень для забезпечення комплексного відстеження і підвищеної безпеки рівня 7, що включають захист від загроз, запобігання вторгнень, фільтрацію веб-сайтів і контроль додатків. Однак при використанні точкових рішень відсутність інтеграції та погана видимість інфраструктури стають серйозними перешкодами при управлінні такими продуктами. За прогнозами компанії Gartner, до 2019 року підприємства будуть шифрувати 80% свого трафіку і саме в зашифрованому трафіку будуть приховані 50% кібератак, спрямованих на проникнення в мережі або вилучення даних. Таким чином, перевірка HTTPS-трафіку стає нагальною потребою.

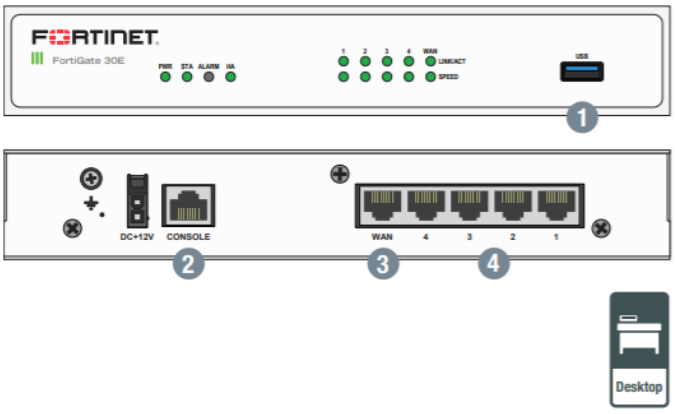
Міжмережевий екран наступного покоління FortiGate використовує спеціально розроблені лабораторією FortiGuard Labs процесори і служби безпеки з

використанням II для забезпечення максимального захисту і ефективної перевірки як незашифрованого, так і зашифрованого трафіку. FortiGate знижує витрати і складність рішень, забезпечує повне відстеження додатків, користувачів і мереж і кращий захист в своєму класі. Будучи невід'ємною частиною Fortinet Security Fabric, FortiGate підтримує взаємодію з усіма захисними рішеннями Fortinet і з рішеннями сторонніх постачальників в мультивендорної середовищі для обміну даними про погрози і підвищення рівня безпеки.

Для міжмережевих екранів наступного покоління FortiGate (NGFW) є безліч різних моделей - від апаратних засобів початкового рівня до пристроїв найвищого рівня - для задоволення найсуворіших вимог до продуктивної захисту від загроз. Це гарантує, що корпоративна мережа, центр обробки даних або внутрішній сегмент легко інтегруються в вашу середу.

Вони бувають різних рівнів, серед яких я б хотів виділити початкового рівня та бізнес класу, також існують рішення більш високих рівнів, але для задоволення більшості потреб вистачає пристроїв бізнес рівня.

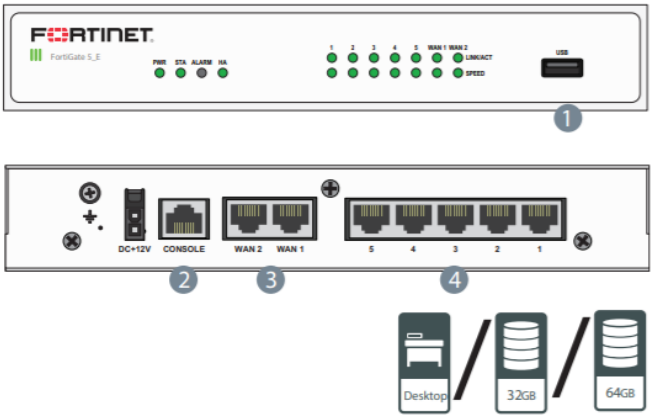
В початковому рівні представлено такі пристрої:



Interfaces

1. USB Port
2. Console Port
3. 1x GE RJ45 WAN Port
4. 4x GE RJ45 Switch Ports

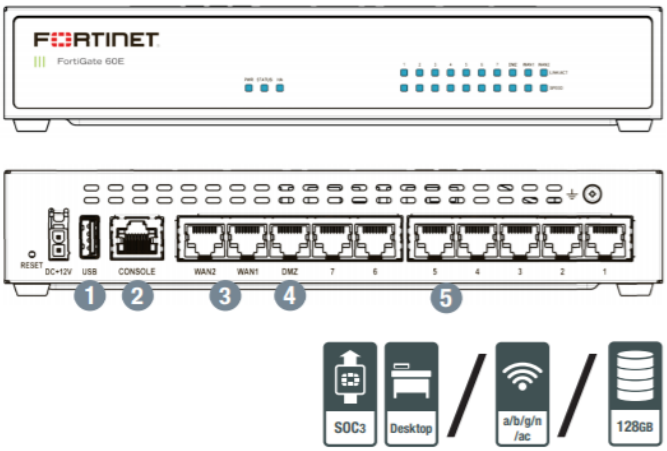
Рис 2.1 - FortiGate 30E



Интерфейсы

1. Порт USB
2. Консольный порт RJ45
3. 2 порта GE RJ45 WAN
4. 5 портов GE RJ45

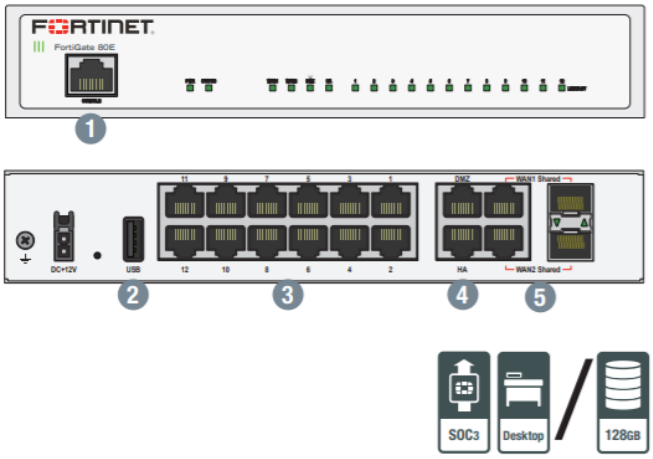
Рис 2.2 - FortiGate 50E



Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Port
5. 7x GE RJ45 Internal Ports

Рис 2.3 - FortiGate 60E

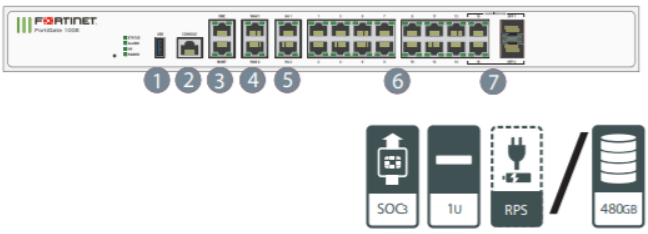


Interfaces

1. Console Port
2. USB Port
3. 12x GE RJ45 Ports
4. 2x GE RJ45 DMZ/HA Ports
5. 2x GE RJ45/SFP Shared Media Pairs

Рис 2.4 - FortiGate 80E

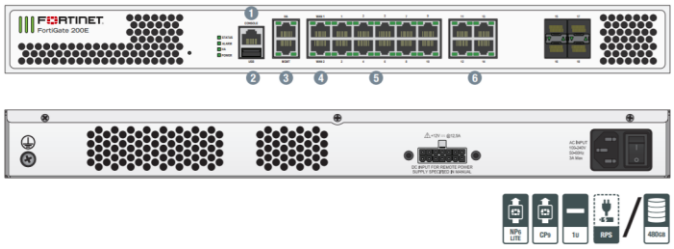
На бізнес рівні представлено більше 9 пристроїв, серед яких я б хотів виділити Fortigate 100e та Fortigate 200e, як одні з найпопулярніших та більш вживаних рішень в сфері малого та середнього бізнесу:



Интерфейсы

1. Объед1. Порт USB
2. Консольный порт
3. Порты 2x GE RJ45 MGMT/DMZ
4. Порты 2x GE RJ45 WAN
5. Порты 2x GE RJ45 HA
6. Порты 14x GE RJ45
7. Пары с разделяемой средой 2x GE RJ45/SFP

Рис 2.5 - Fortigate 100e



Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45 Management/HA Ports
4. 2x GE RJ45 WAN Ports
5. 14x GE RJ45 Ports
6. 4x GE SFP Slots

Рис 2.6 - Fortigate 200e

Для порівняння візьмемо дві моделі: Fortigate 60e та Fortigate 100e(Таблиця 2.1).

Таблиця 2.1 – Порівнялна характеристика Fortigate 60e та Fortigate 100e

	Fortigate 60e	Fortigate 100e
Ціна, грн	*32068*	*77621*
Максимальна пропускна здатність, Мбіт / с	*3000*	*7400*
Кількість одночасних сесій, млн	*1.3*	*2*
Максимальна пропускна здатність IPS (intrusion prevention system) , Мбіт / с	*400*	*500*
Одночасні користувачі SSL-VPN (максимум), шт	*200*	*300*
Кількість правил брандмауера	*5,000*	*10000*

Об'єкт нашого розгляду сьогодні - FortiGate-100E, який володіє «з коробки» безліччю функцій:

- Маршрутизатор (статична, динамічна маршрутизація RIP, OSPF, BGP, PIM);
- Міжмережевий екран;
- Система запобігання вторгнень (IPS);
- Антивірус і Антиспам;
- Контроль додатків;
- Вбудований бездротовий контролер;
- Web / контент-фільтрація;
- Режим відмовостійкості / кластеризації;
- Підтримка: IPv6, VLAN;
- VPN IPSec і SSL, VPN-концентратор;
- Шейпінг трафіку;
- Оптимізація WAN-трафіку;
- Інспектування SSL-трафіку;
- Запобігання витоку даних (DLP);
- Балансування навантаження на сервера;

- Поділ на віртуальні пристрої (домени) (VDOM);

- Контроль кінцевих точок;

- Аутентифікація користувачів в LDAP, RADIUS, TACACS +, Single Sign-On в Active Directory і eDirectory.

FortiGate Серії 100E є міжмережевий екран наступного покоління, що забезпечує гнучкість при розгортанні і всебічний захист підприємств від різних загроз. Використання апаратних процесорів безпеки, дозволяє забезпечувати високу продуктивність інспекції трафіку, ефективність системи безпеки і повну видимість.

Рішення щодо захисту великих філій організації:

Безпека

• Захист від відомих експлойтів, шкідливих програм і зловмисних сайтів з використанням безперервного аналізу загроз, здійснюваного службами забезпечення безпеки FortiGuard Labs;

• Ідентифікація тисяч додатків, в тому числі хмарних, для забезпечення глибокої інспекції мережевого трафіку;

• Захист від невідомих атак з використанням динамічного аналізу і автоматичного реагування на виникаючі загрози для раннього виявлення і захисту від цілеспрямованих атак продуктивність;

• Забезпечення кращих в своєму класі показників продуктивності в режимі всебічної інспекції трафіку і захисту від загроз. Використання спеціалізованих процесорів безпеки (SPU) при інспекції трафіку дозволяє забезпечити найнижчі затримки при проходженні трафіку крізь пристрій.;

• Найвища продуктивність в режимі інспекції SSL / TLS трафіку в галузі сертифікація;

• Протестовані і підтверджені незалежними організаціями найкращі показники ефективності захисту і продуктивності;

• Наявність ексклюзивних сертифікатів, виданих сторонніми організаціями, такими як NSS Labs, ICSA Labs, Virus Bulletin, AV Comparatives і іншими.

Мережеві технології

• Підтримка протоколів динамічної маршрутизації RIP, OSPF, BGP, IS-IS, статичної маршрутизації, PBR, функцій комутації, QoS з функціями шейпінгу, наявність контролера бездротової мережі, балансувальника навантаження L4, можливість використання віртуальних контекстів VDOM (аналог VRF) і висока продуктивність IPsec VPN, дозволяють компаніям отримати всі необхідні функції маршрутизатора і міжмережевого екрану нового покоління в рамках одного пристрою;

• Забезпечення гнучкого розгортання міжмережевого екранування наступного покоління і технології безпечного SD-WAN (Software-Defined Wide Area Networks - програмно-які визначаються розподілені мережі) управління;

• Єдина панель для центрів управління мережами (NOC) забезпечує повну видимість подій і швидке виявлення мережевих проблем на інтуїтивному рівні;

• Вбудований механізм перевірки відповідності до початкових установок вимогам різних галузевих стандартів і кращим практикам для підвищення загального рівня безпеки.

Архітектура інформаційної безпеки

Fortinet Security Fabric

• Високий рівень інтеграції між рішеннями Fortinet і рішеннями партнерів, з розвиненими функціями автоматизації зворотного захисної реакції і передачею інформації про загрози між усіма рішеннями Security Fabric;

• Автоматичне створення топології мережі, з виявленням пристроїв IoT (Інтернету речей) і забезпеченням повної видимості всіх процесів, що відбуваються.

Щоб налаштувати Fortinet Security Fabric необхідно перейти до розділу Мережі – Інтерфейси, обрати інтерфейс та ввімкнути FortiTelemetry та Device Detection.

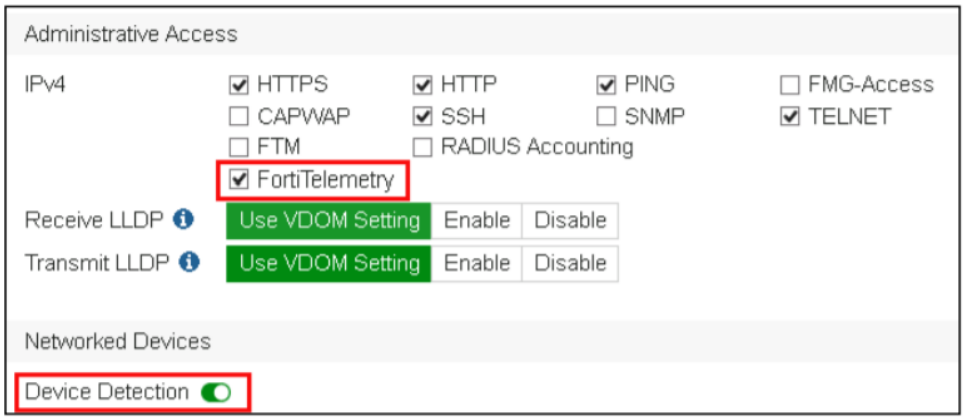


Рис. 2.7 Fortinet Security Fabric

3. АНАЛІЗ ПЕРЕЛІКУ МОЖЛИВОСТЕЙ МЕРЕЖЕВОГО ЕКРАНУ FORTIGATE 100E ТА РЕКОМЕНДАЦІЙ ЩОДО РОБОТИ З НИМ

3.1 Перше завантаження та початкове налаштування мережевого екрану за допомогою програмного забезпечення Putty

Щоб налаштувати, підтримувати та адмініструвати пристрій FortiGate, потрібно підключитися до нього. Є два способи:

- Веб-інтерфейс - графічний інтерфейс користувача (GUI) з веб-браузера. Він може відображати звіти та журнали, але не вистачає багатьох вдосконалених діагностичних команд.
- Інтерфейс командного рядка (CLI) - текстовий інтерфейс, подібний до команд DOS або UNIX, із захищеної оболонки (SSH) або терміналу Telnet або віджета консолі JavaScript CLI у веб-інтерфейсі (Система> Статус> Статус). Він надає доступ до багатьох розширених діагностичних команд, а також конфігурації, але не вистачає звітів та журналів.

Доступ до CLI та / або веб-інтерфейсу через вашу мережу ще не налаштований, якщо:

- Ви підключаєтеся вперше;
- Ви тільки що скинули конфігурацію до її типового стану;
- Ви щойно відновили прошивку.

У цих випадках потрібно спочатку підключити комп'ютер безпосередньо до FortiGate, використовуючи налаштування за замовчуванням. Через пряме з'єднання ви можете скористатися веб-інтерфейсом або CLI для налаштування основних мережевих налаштувань FortiGate. Після цього ви зможете розмістити мережевий екран Fortigate у своїй мережі та використовувати його через вашу мережу.

Підключення до веб-інтерфейсу

Ви можете підключитися до веб-інтерфейсу, використовуючи його налаштування за замовчуванням (Таблиця 3.1):

Таблиця 3.1 – Налаштування за замовчуванням для підключення до веб-інтерфейсу

Мережевий інтерфейс	Порт 1
URL-адреса	https://192.168.1.99/
Обліковий запис адміністратора	admin
Пароль	

Вимоги

- комп'ютер з мережевим портом Ethernet RJ-45;
- веб-браузер, такий як Microsoft Internet Explorer версії 6.0 або новішої, або Mozilla Firefox 3.5 або новішої версії;
- кабель Ethernet.

Для підключення до веб-інтерфейсу

1. На комп'ютері налаштуйте Ethernet-порт зі статичною IP-адресою 192.168.1.2 та з мережевою маскою 255.255.255.0(24);

2. За допомогою кабелю Ethernet підключіть порт Ethernet свого комп’ютера до порту приладу FortiGate;

3. Запустіть браузер і введіть таку URL-адресу: https://192.168.1.99/;

Для підтримки HTTPS-аутентифікації прилад FortiGate постачається з підписаним сертифікатом безпеки, який він подає клієнтам щоразу, коли вони ініціюють HTTPS-з'єднання з пристроєм FortiGate. Коли ви підключаєтесь, залежно від веб-браузера та попереднього доступу до пристрою FortiGate, у вашому браузері можуть відображатися два попередження щодо безпеки, пов’язані з цим сертифікатом:

Сертифікату не довіряється автоматично, оскільки він підписується самостійно, а не підписується дійсним органом сертифікації (CA). Сертифікати, що підписуються самостійно, не можуть бути перевірені належним (CA), а тому можуть

бути шахрайськими. Ви повинні вручну вказати, чи варто довіряти сертифікату чи ні.

Сертифікат може належати іншому веб-сайту. Поле загального імені у сертифікаті, яке зазвичай містить ім'я хоста веб-сайту, не відповідає точно вказаній URL-адресі. Це може вказувати на крадіжку ідентичності сервера, але також може просто вказувати, що сертифікат містить доменне ім’я, поки ви ввели IP-адресу. Ви повинні вручну вказати, нормально це порушення чи ні.

4. Перевірте та приймайте сертифікат постійно (веб-браузер більше не відображатиме попередження про самопідпис) або тимчасово. Ви не можете увійти, поки не приймете сертифікат;

5. У полі Ім'я введіть адміністратора та натисніть Увійти. (За замовчуванням для цього облікового запису немає пароля.);

Введені облікові дані для входу шифруються до того, як вони будуть надіслані на пристрій FortiGate. Якщо ваш логін вдалий, з’явиться веб-інтерфейс з вікном логіну, як на Рис 3.1.

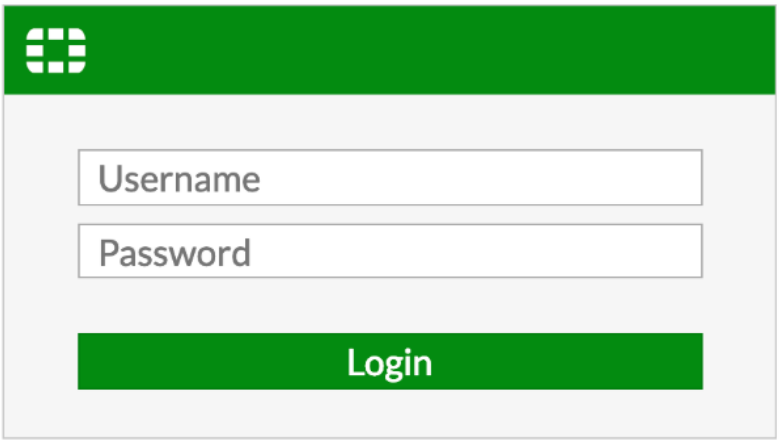


Рис 3.1 – Вікно логіну в веб-інтерфейс FortiGate 100e

Підключення до CLI

Використовуючи налаштування за замовчуванням, ви можете отримати доступ до CLI зі свого комп'ютера двома способами:

- підключення до локальної консолі;
- SSH-з'єднання, локальне або через мережу.

Безпечна оболонка (англ. Secure Shell - SSH) забезпечує як захищену аутентифікацію, так і безпечну комунікацію з CLI.

Параметри за замовчуванням для підключення до CLI через SSH (Таблиця 3.2)

Таблиця 3.2 - Налаштування за замовчуванням для підключення до CLI

Мережевий інтерфейс	Порт 1
URL-адреса	https://192.168.1.99/
Номер порту SSH	22
Обліковий запис адміністратора	admin
Пароль	-

Крім того, ви можете отримати доступ до CLI через SSH та пару публічно-приватних ключів. Однак, використовуючи цю опцію, ви спочатку отримуєте доступ до CLI за допомогою віджета консолі CLI (частина інформаційної панелі статусу веб-інтерфейсу) або через SSH та пароль для завантаження відкритого ключа.

Вимоги

- комп’ютер з портом Ethernet RJ-45;
- кабель Ethernet ;
- клієнт щоб ініціювати SSH, такий як PuTTY;

Для підключення до CLI за допомогою консольного кабелю

1. За допомогою кабелю RJ-45-DB-9 або нульового модему підключіть порт послідовного зв'язку комп'ютера (COM) до консольного порту пристрою FortiGate;

2. Переконайтесь, що пристрій FortiGate увімкнено;

3. На комп'ютері управління запустіть PuTTY;

4. У меню категорій зліва перейдіть до З'єднання> Серійний і налаштуйте параметри, які вказано в Таблиці 3.3:

Таблиця 3.3- Налаштування за замовчуванням для підключення через COM порт

Послідовна лінія для підключення	COM1 (або, якщо ваш комп'ютер має кілька послідовних портів, назва підключеного послідовного порту)
Швидкість (бод)	9600
Біти даних	8
Зупинка біт	1
Паритет	-
Управління потоком	-

5. У меню категорій ліворуч перейдіть до сесії та виберіть тип підключення з вибору послідовний;

6. Клацніть Відкрити;

7. Натисніть клавішу Enter, щоб ініціювати з'єднання;

З'являється запит на вхід.

8. Введіть адміністратора, а потім натисніть Enter двічі. (за замовчуванні не існує пароля для облікового запису адміністратора.);

CLI відображає наступний текст, за яким слід командний рядок:

«Ласкаво просимо!», тепер ви можете вводити команди та продовжувати перше налаштування вашого FortiGate

Вимоги

- комп’ютер з доступним портом послідовного зв'язку (COM);
- кабель RJ-45-до-DB-9 або нульовий модем, який вже є включений у ваш пакет FortiGate;
- програмне забезпечення для емуляції терміналів, наприклад – PuTTY.

Для підключення до CLI за допомогою SSH-з'єднання та пароля

1. На комп'ютері управління налаштуйте Ethernet-порт зі статичною IP-адресою 192.168.1.2 з мережевою маскою 255.255.255.0;

2. За допомогою кабелю Ethernet підключіть порт Ethernet свого комп’ютера до порту приладу FortiGate;

3. Переконайтеся, що пристрій FortiGate увімкнено;

4. На комп'ютері управління запустіть PuTTY;

5. Введіть ім'я хоста (або IP-адресу) 192.168.1.99;

6. У порту введіть 22;

7. З типу з'єднання виберіть SSH;

8. Виберіть Відкрити;

Клієнт SSH підключається до пристрою FortiGate.

Клієнт SSH може відображати попередження, якщо ви вперше підключаєтесь до пристрою FortiGate і його SSH-ключ ще не розпізнаний вашим клієнтом SSH або якщо ви раніше підключились до пристрою FortiGate, але він використовував іншу IP-адресу або ключ SSH.

Якщо ваш керуючий комп'ютер підключений безпосередньо до пристрою FortiGate, між ними немає мережевих хостів, це нормально.

9. Клацніть Так, щоб перевірити сертифікати і прийняти ключ SSH пристрою FortiGate. Ви не можете увійти, поки не приймете сертифікат;

CLI відображає запит на вхід.

10. Введіть адміністратора і натисніть Enter. (за замовчуванням у цього облікового запису немає пароля.);

CLI відображає підказку, наприклад:

FortiGate_100e #

Тепер ви можете вводити команди. Щоб продовжити оновленням програмного забезпечення, див. Оновлення програмного забезпечення. В іншому випадку, щоб продовжити, встановивши адміністративний пароль, див. Зміна пароля облікового запису адміністратора.

3.2 Загальний огляд графічного інтерфейсу мережевого екрану

Зазвичай CLI використовується тільки для первинної настройки, весь інший час більш зручніше використовувати веб або графічний інтерфейс(UI).

Для того щоб потрапити на веб інтерфейс ми будемо використовувати інструкцію з попереднього пункту, якщо ми намагаємося підключитися в перший раз, або в полі для URL адресу потрібно набрати наступне – https://ip-adress:9443, якщо ми вже виконали первинне базове налаштування та змінили IP адресу на іншу

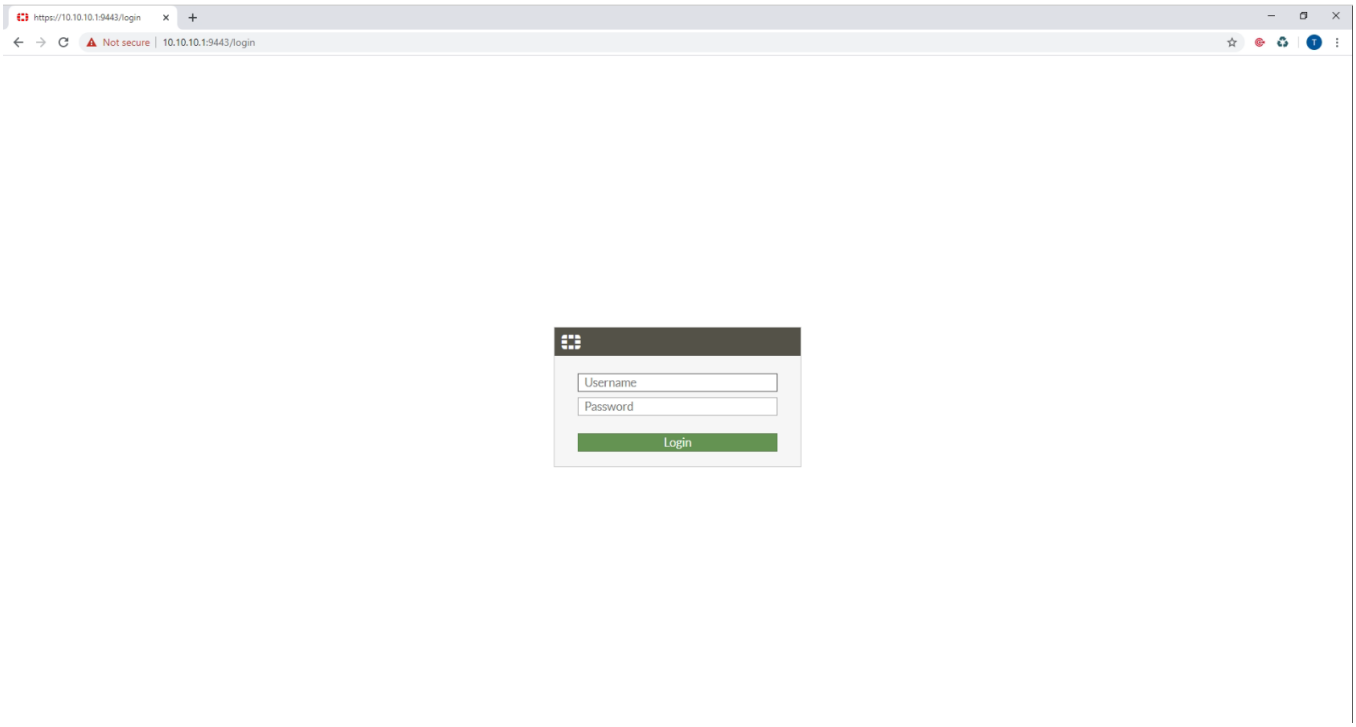


Рис. 3.2 – Вікно логіну в веб-інтерфейс Fortigate 100e

Базовий колір веб-інтерфейсу має зелений відтінок(Рис 3.3), але коли в вашій компанії є необхідність працювати наприклад з 3 або 4 мережевими екранами одинакової серії то є актуальної зміна кольору наприклад на меландж(Рис 3.4).

Також серед загального огляду веб-інтерфейсу, хочу відмітити такий пункт в меню налаштувань, як – Feature Visibility(Рис 3.5), саме в цьому меню, як зрозуміло з назви ми вибираємо які саме пункти в меню в нашому веб-інтерфейсі будуть активними та будуть відображатися в веб-інтерфейсі, як видно на Рис 3.5, серед активних ми маємо: Application Control, Web Filter, VPN саме їх ми сьогодні розглянемо більш детально.

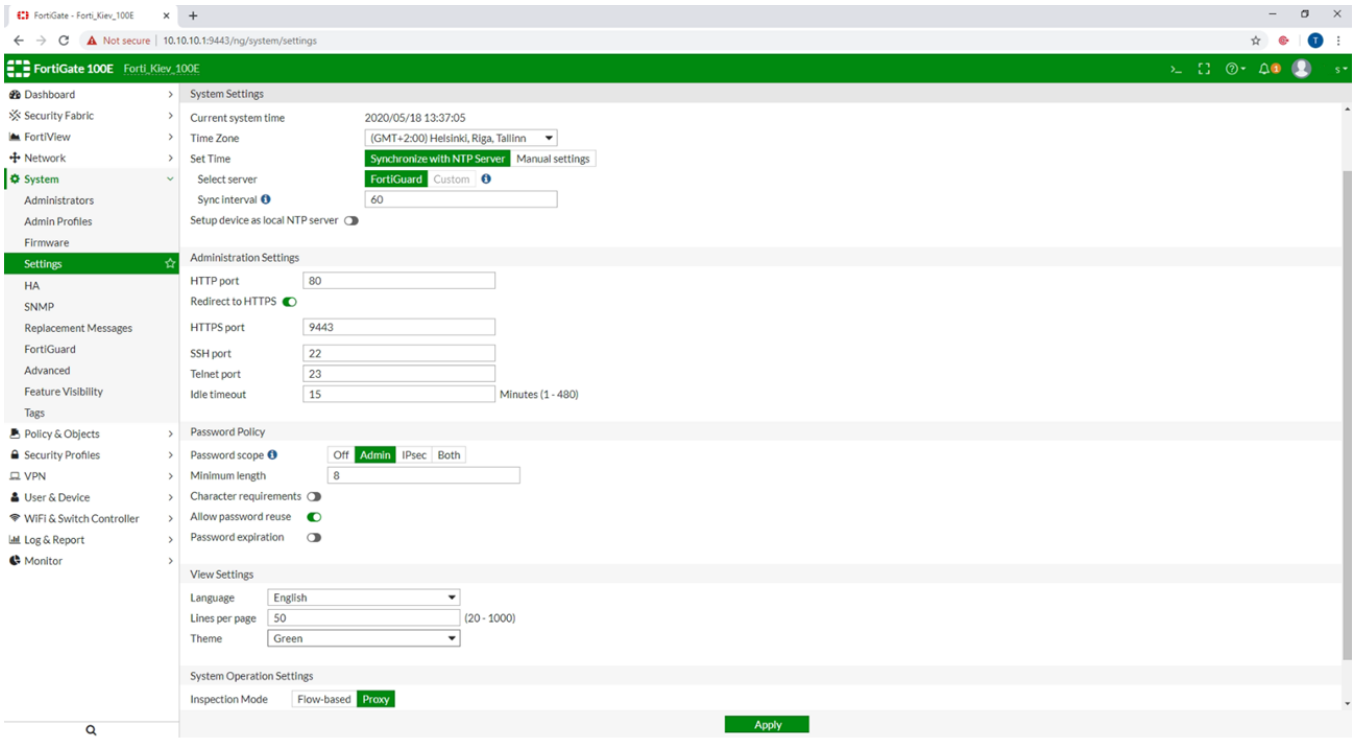


Рис 3.3 – Базовий колір веб-інтерфейсу

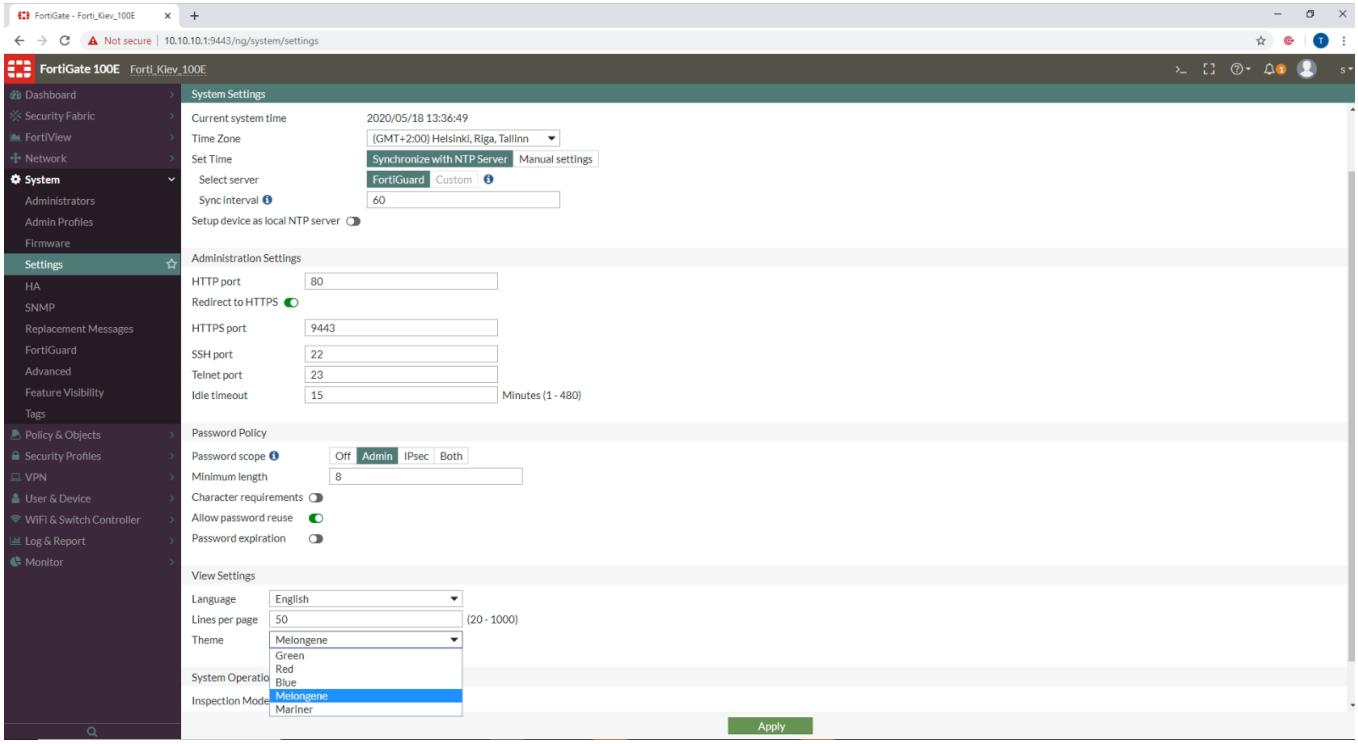


Рис 3.4 – Меланджовий колір веб-інтерфейсу

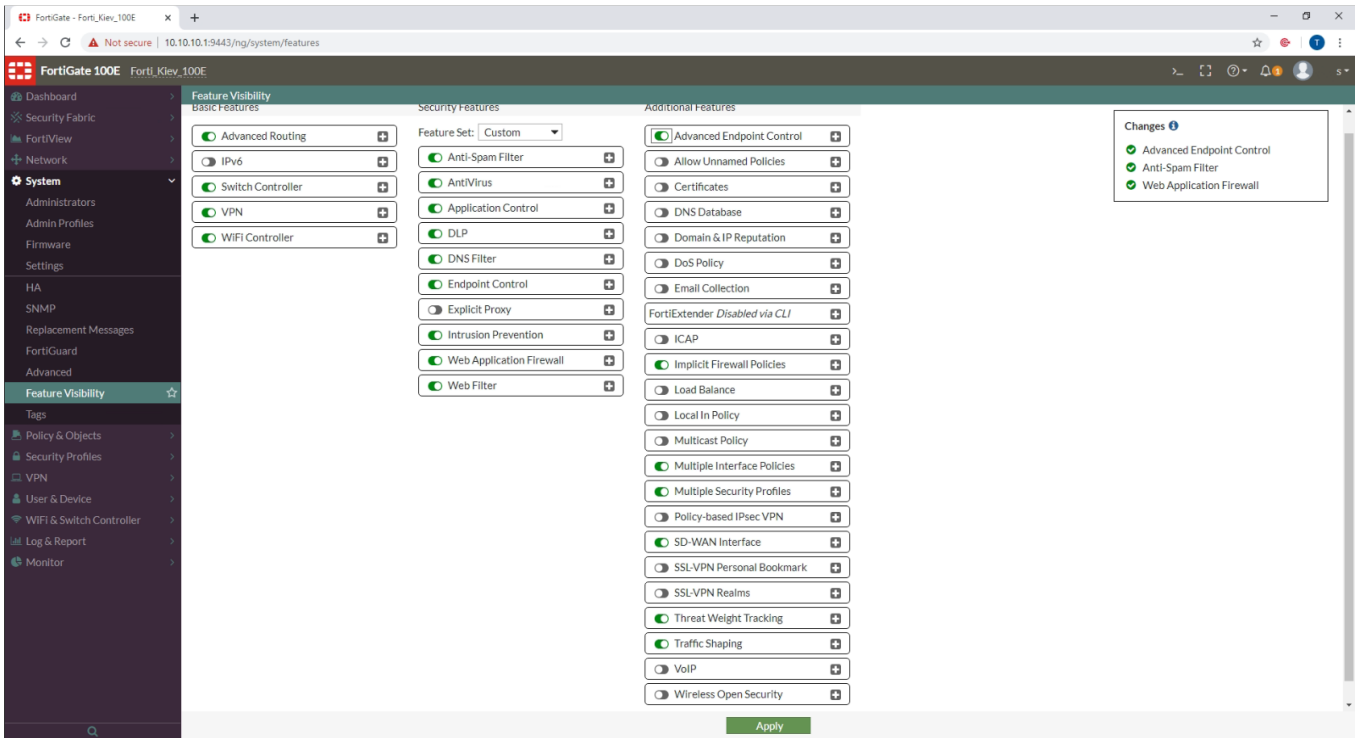


Рис 3.5 – Вигляд пункту меню Feature Visibility

3.2.1 Dashboard

На інформаційній панелі FortiOS передбачено місце для перегляду системної інформації в режимі реального часу. За замовчуванням на приладовій панелі відображаються основні статистичні дані самого блоку FortiGate, що забезпечує пам'ять та стан процесора(пункт 3 на Рис 3.6), а також статус здоров'я портів, незалежно від того, чи є вони активними чи ні та пропускну здатність каналів(пункт 1 та 2 на Рис 3.6).

Всередині інформаційної панелі знаходиться ряд менших вікон, які називаються віджетами(пункти 1,2,3,4,5 на Рис 3.6), які надають цю інформацію про стан. Крім того, що відображається за замовчуванням, ви можете додати ряд інших віджетів(Рис 3.7), які відображають іншу ключову інформацію про трафік, включаючи використання програми, трафік на IP-адресу, найпопулярніші атаки, історію трафіку та статистику ведення журналів.

Ви можете додати кілька інформаційних панелей, щоб відобразити дані, які ви хочете відстежувати, і додавати віджети відповідно (Рис 3.8). Конфігурація панелі інструментів доступна лише через GUI. Для налаштування та додавання віджетів

адміністратори повинні мати права читання та запису, коли вони перебувають у будь-якому меню. Якщо вони хочуть переглянути інформацію, адміністратори повинні мати привілеї для читання.

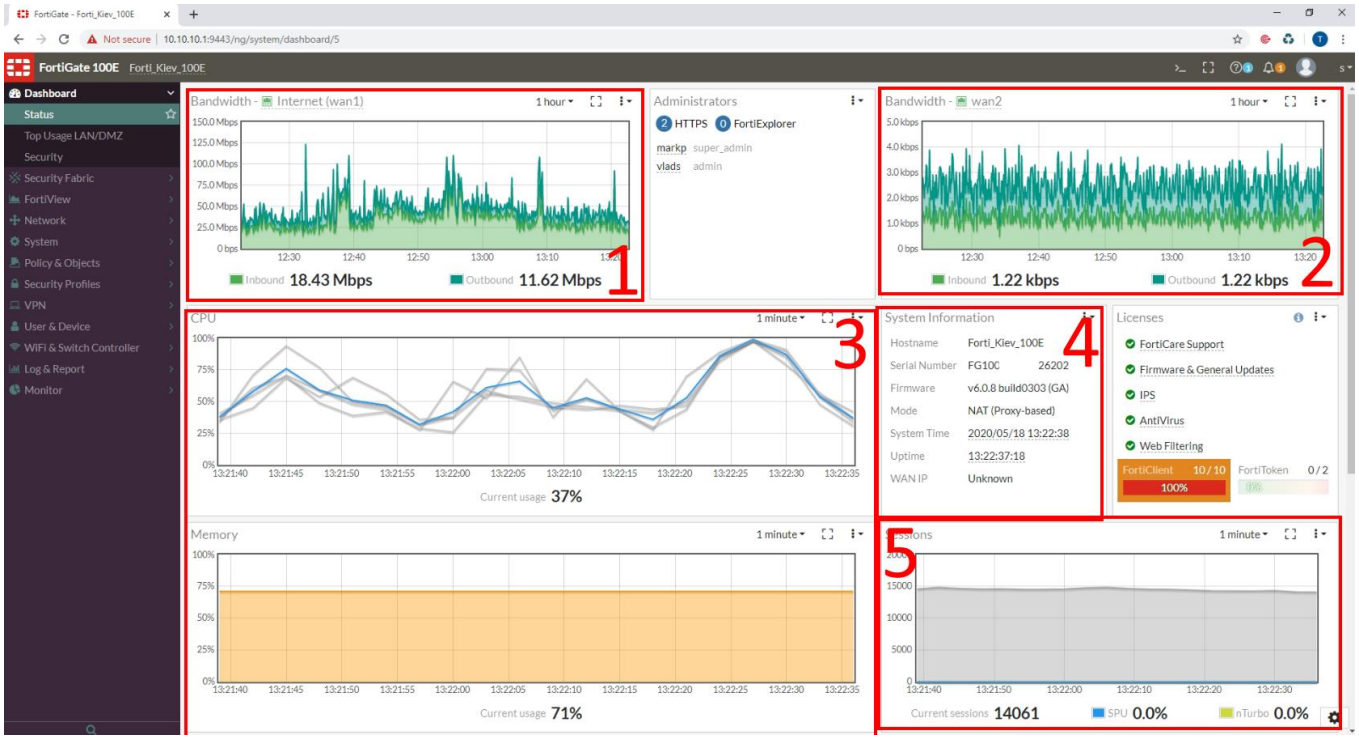


Рис 3.6 – Загальний вигляд панелі Dashboard з віджитами для моніторингу мережі

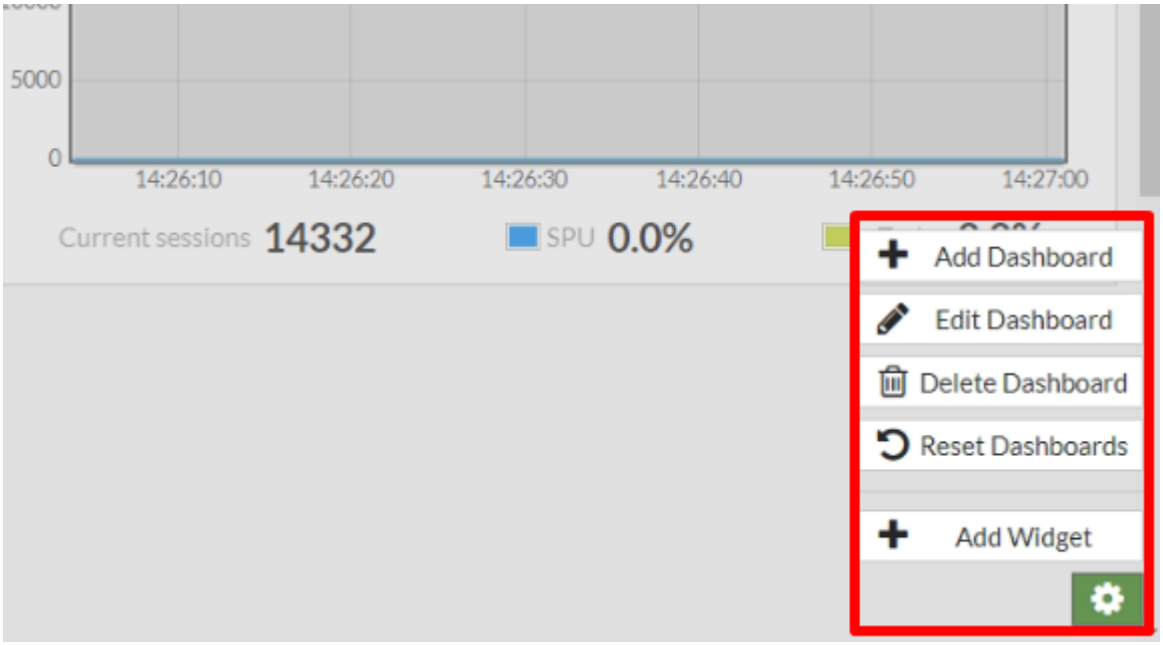


Рис 3.7 – Меню додавання віджетів на панель моніторингу

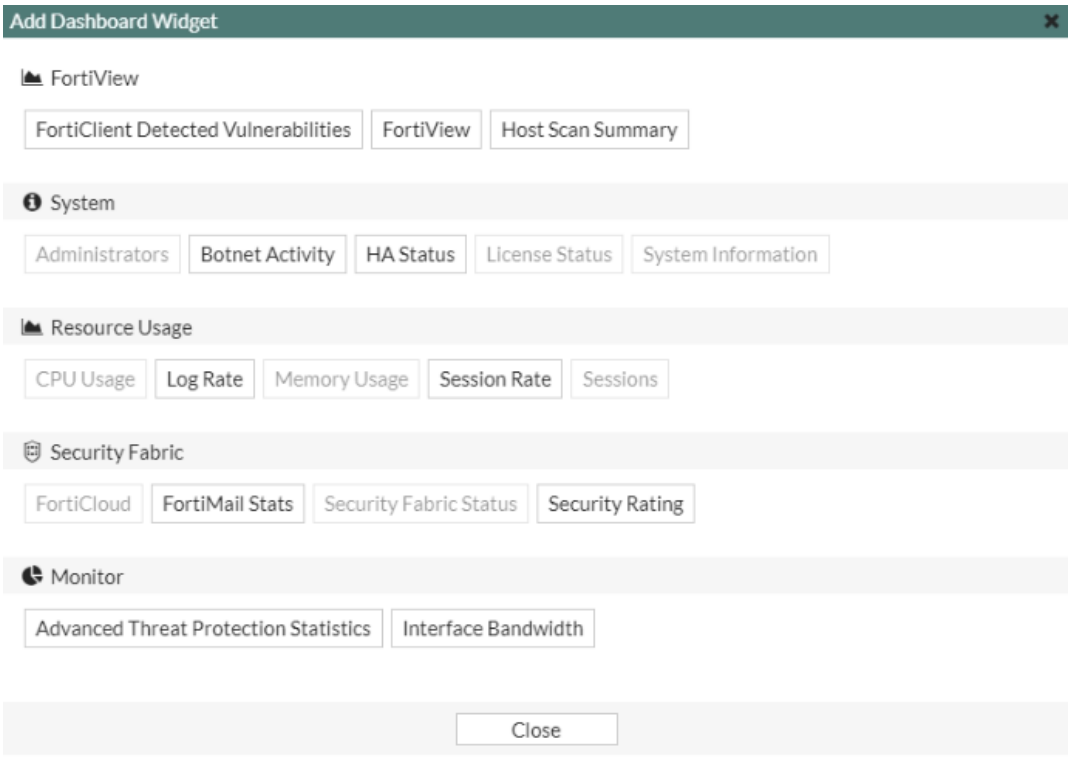


Рис 3.8 – Перелік доступних віджетів

3.2.2 FortiView

Ведення журналів та звітування є корисними компонентами, які допоможуть вам зрозуміти, що відбувається у вашій мережі, та повідомити про певні мережеві дії, такі як виявлення вірусу, відвідування недійсного веб-сайту, вторгнення, невдала спроба входу, і безліч інших.

Журнал записує трафік, який проходить через, починається або закінчується на FortiGate, і записує дії, які FortiGate вчинив під час сканування трафіку. Після того, як ця інформація записується у журнал повідомлення, вона зберігається у файлі журналу, який зберігається на журнальному пристрої (центральне місце зберігання повідомлень журналу). FortiGate підтримує кілька видів журналу, таких як FortiAnalyzer, FortiGateCloud та syslog-сервери. Приблизно 5% пам'яті використовується для буферизації журналів, що надсилаються на FortiAnalyzer. Системну пам'ять FortiGate та локальний диск також можна налаштувати для зберігання журналів, тому він також вважається пристроєм для зберігання журналів.

Звіти показують записану активність у більш читаному форматі. Звіт збирає всю інформацію журналу, яка йому потрібна, потім представляє його у графічному форматі з налаштованим дизайном та автоматично генерується діаграмами(Рис 3.9), що показують, що відбувається в мережі. Звіти можна створювати на пристроях FortiGate з веденням дискового журналу та на пристроях FortiAnalyzer.

FortiView - це більш всеосяжний інструмент звітності та моніторингу мережі. Він інтегрує дані в реальному часі та історичні дані в єдиний вигляд у FortiOS.

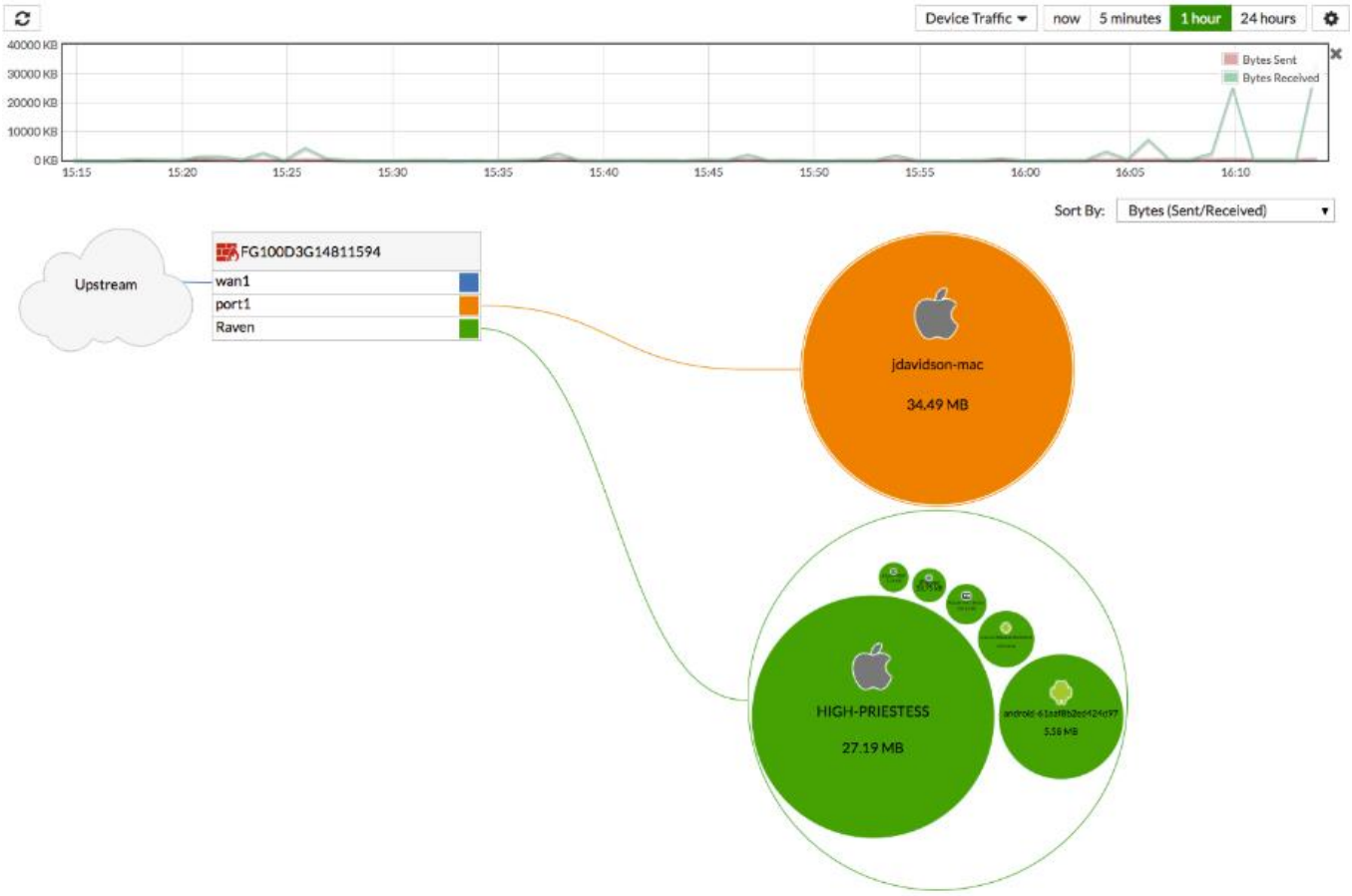


Рис 3.9 – Приклад створеної діаграми в результаті аналізу трафіку

3.2.3 Network

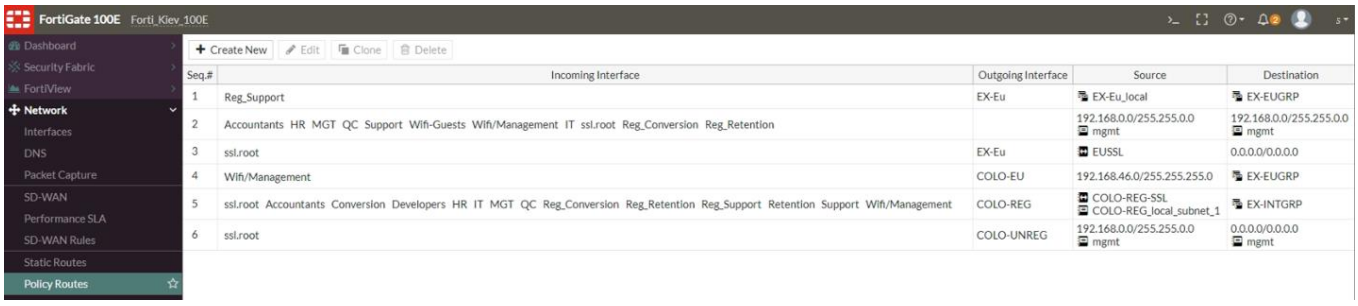


Рис 3.10 – Приклад налаштування різних маршрутів для віртуальних мереж в локальну підмережу та з неї в VPN

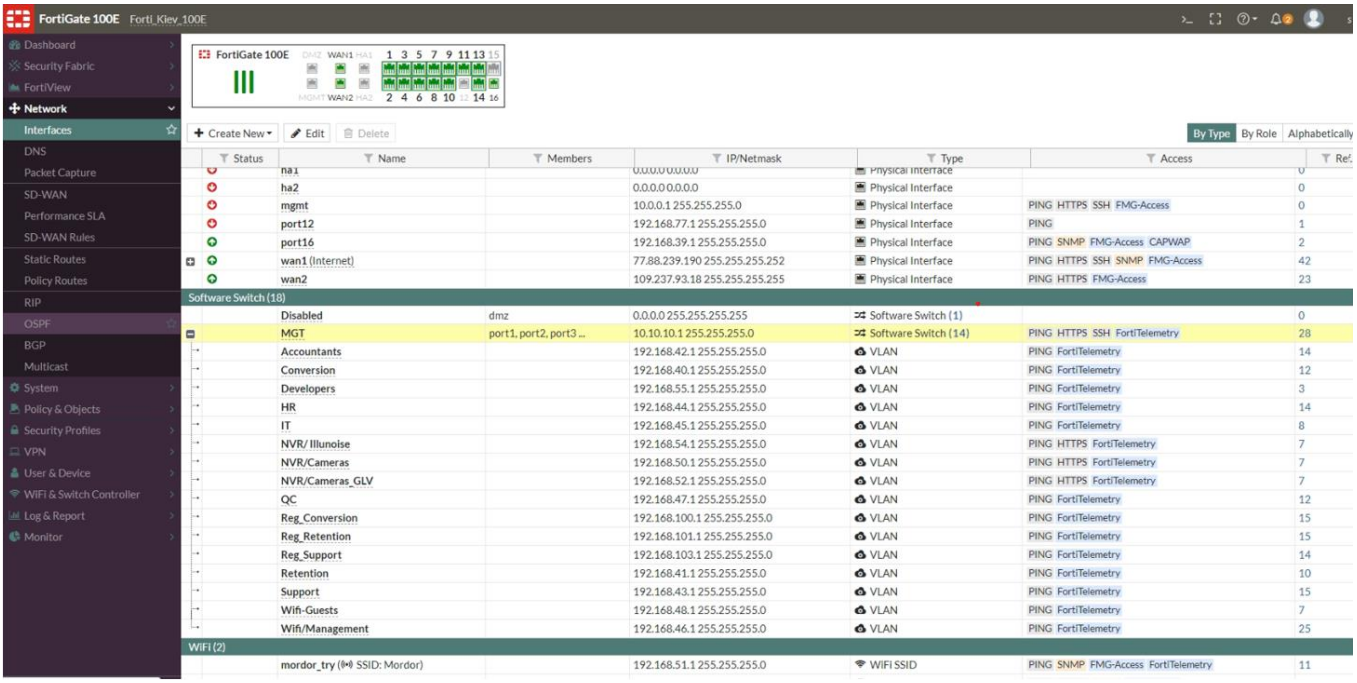


Рис 3.11 – Перелік активних інтерфейсів

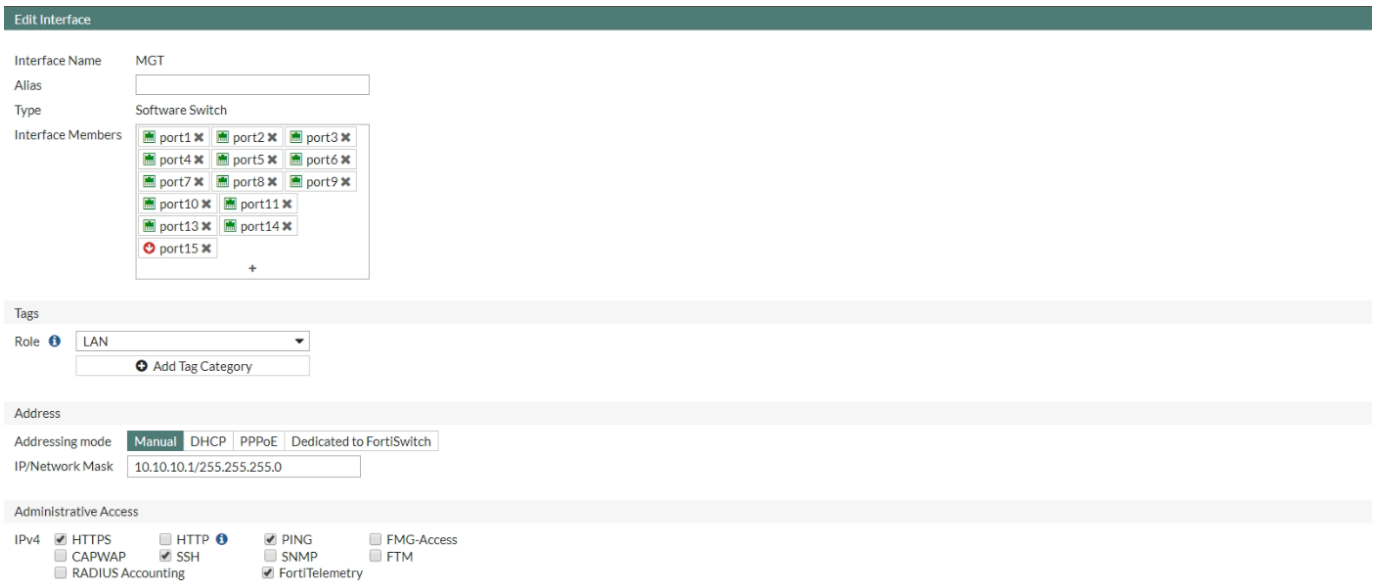


Рис 3.12 – Приклад об’єднання віртуальних інтерфейсів в одну мережу

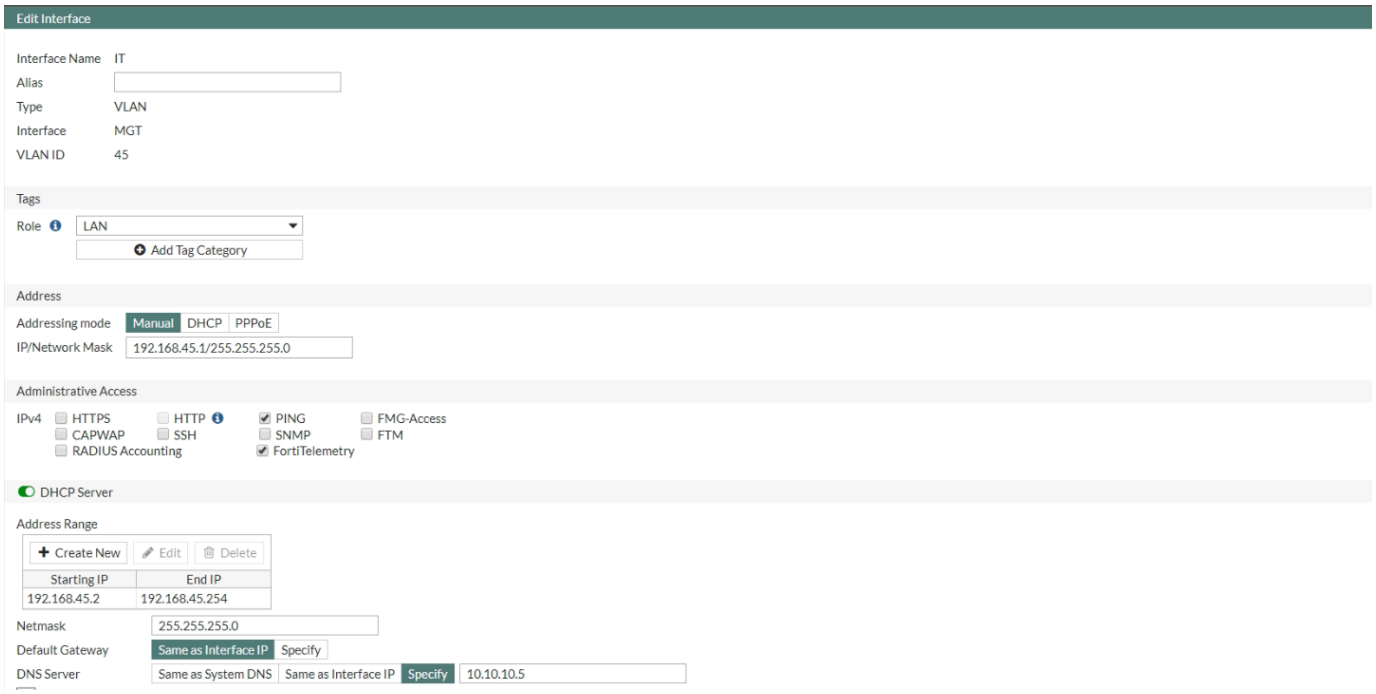


Рис 3.13 – Приклад створення віртуального інтерфейсу(VLAN)

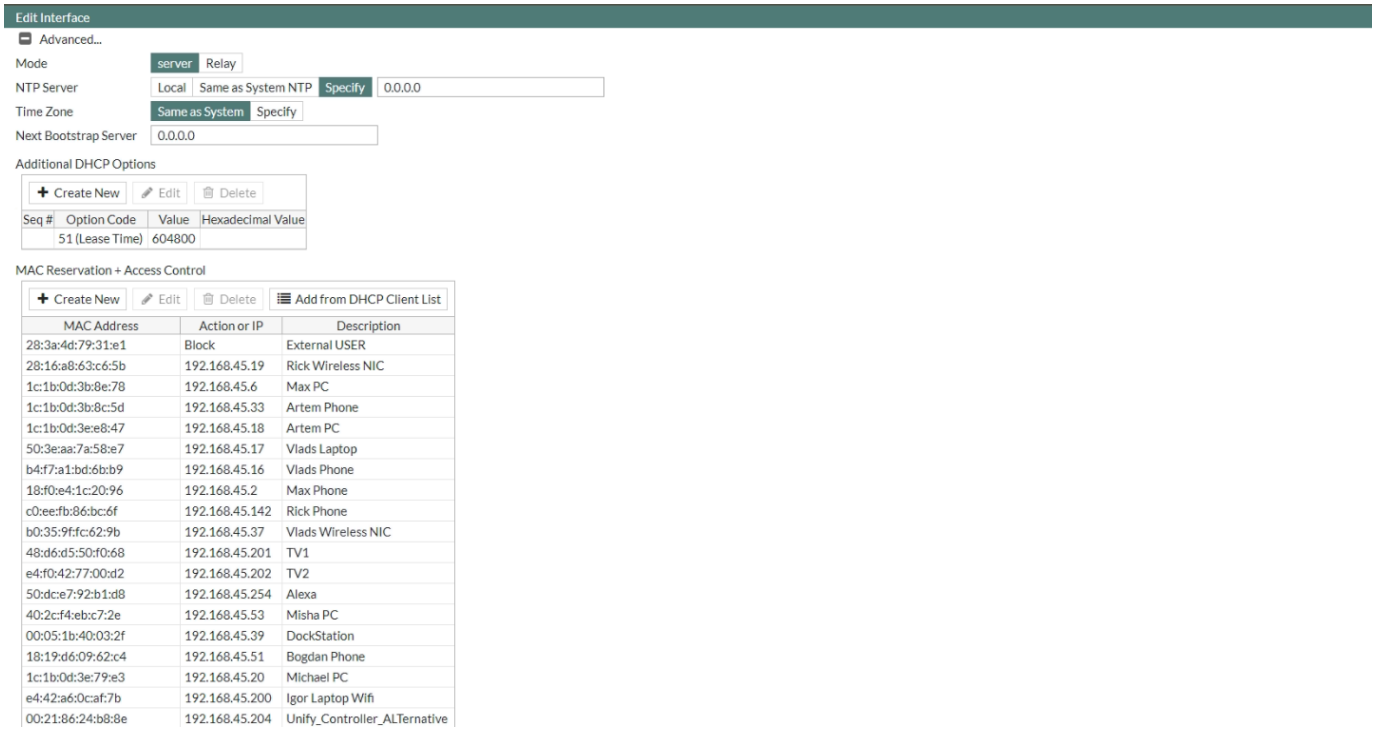


Рис 3.14 – Приклад реалізацію «Білого листа» по MAC адресам та з резервацією IP адресу в 45 VLAN’i

3.2.4 Policy and Objects

Панель "Політика та об'єкти"(Policy and Objects) дозволяє централізовано керувати та налаштовувати пристрої, якими керує підрозділ FortiManager. Сюди входять основні мережеві параметри для підключення пристрою до корпоративної мережі, антивірусні визначення, підписи захисту від вторгнення, правила доступу та керування та оновлення мікропрограмного забезпечення для пристроїв.

Усі зміни, пов’язані з політикою та об’єктами, слід вносити на пристрій FortiManager, а не на керовані пристрої.

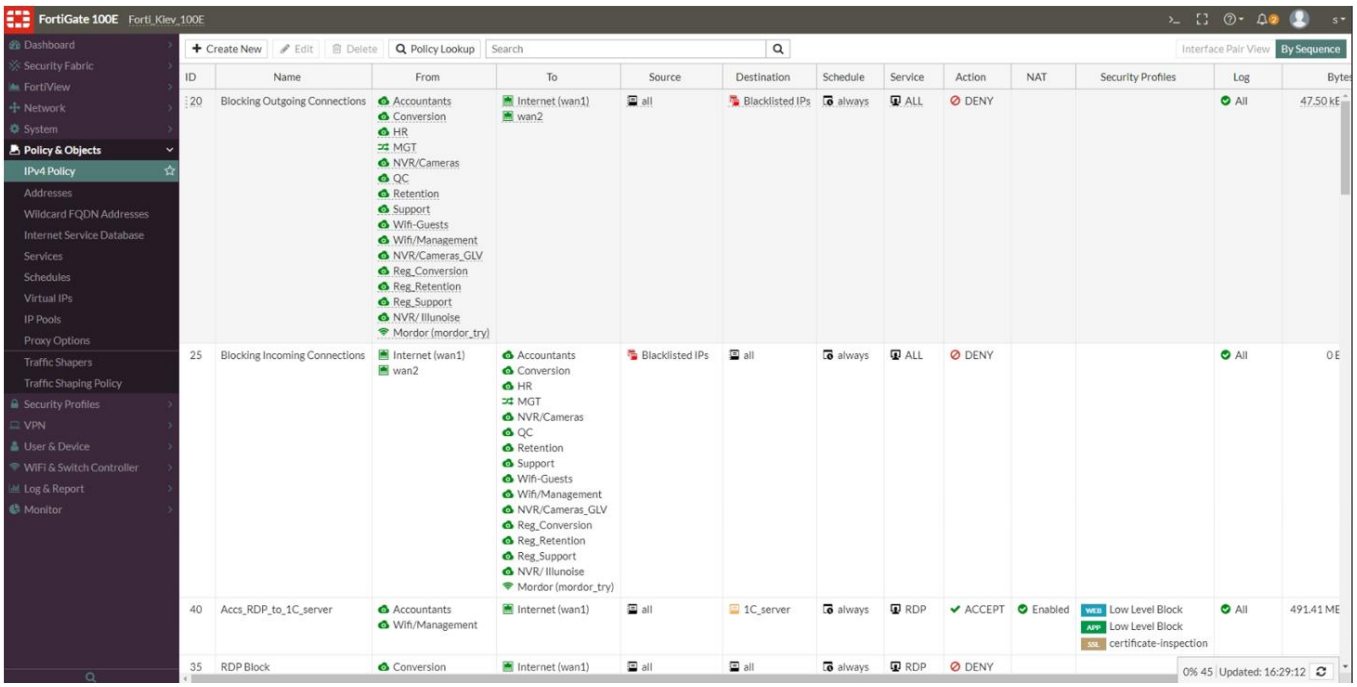


Рис 3.15 – Загальний вигляд вкладки IPv4 Policy

Рис 3.16 – Приклад створення мережевої політики для того щоб віртуальний мережевий інтерфейс мав доступ до глобальної мережі

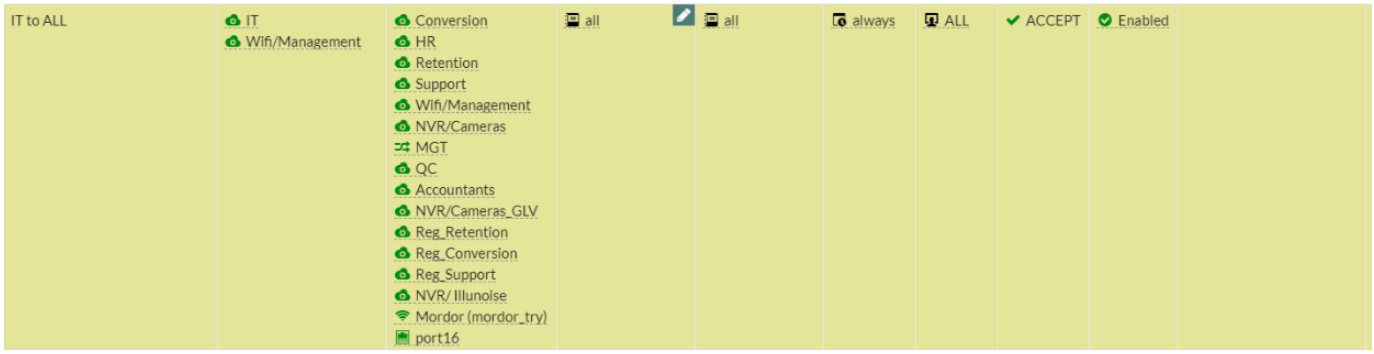


Рис 3.17 – Приклад створення мережевої політики для спілкування VLAN'ів в середені локальної мережі

3.2.5 Security Profiles

Цей розділ містить інформацію про налаштування функцій захисту FortiGate, включаючи:

- Антивірус
- Веб-фільтр
- DNS-фільтр
- Контроль додатків
- Профілактика інтрузії
- Фільтр електронної пошти
- Запобігання витоку даних
- Рішення VoIP
- ICAP
- Брандмауер веб-додатків
- Режими огляду
- Відміняє
- Спеціальні підписи

В забезпечені безпеки корпоративної мережі нас найбільше цікавлять веб-фільтри та контроль додатків, web-filter and application control відповідно, тому сьогодні ми будемо розглядати саме їх, почнемо з веб-фильтру.

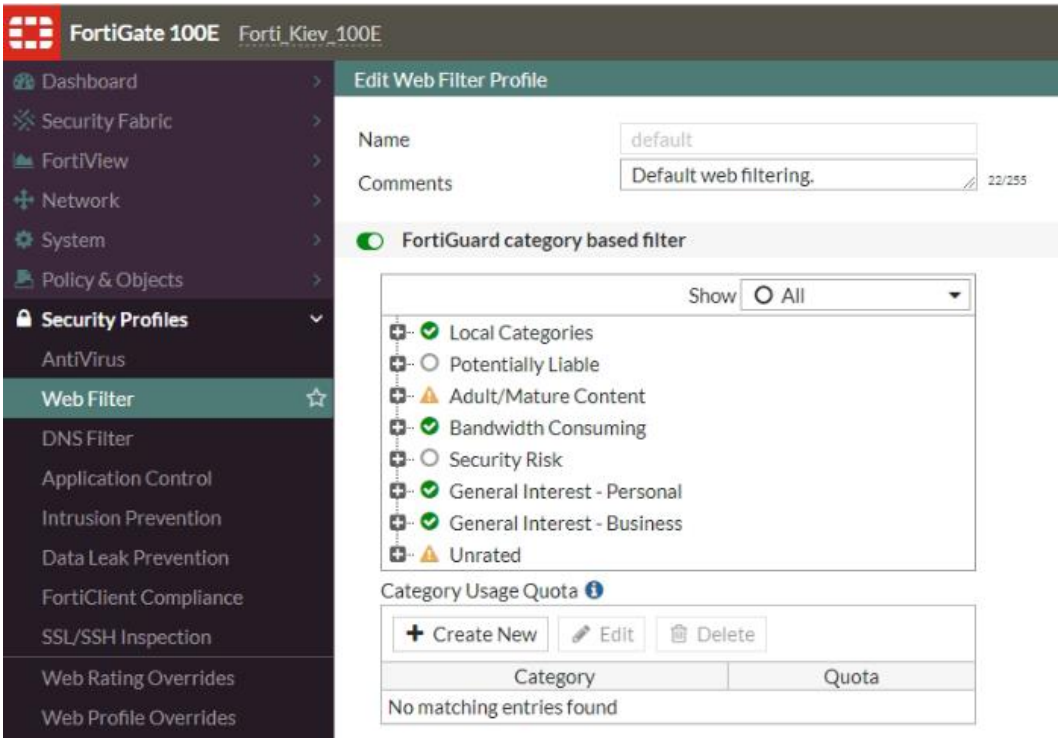


Рис 3.18 – Загальний вигляд стандартного веб фільтру

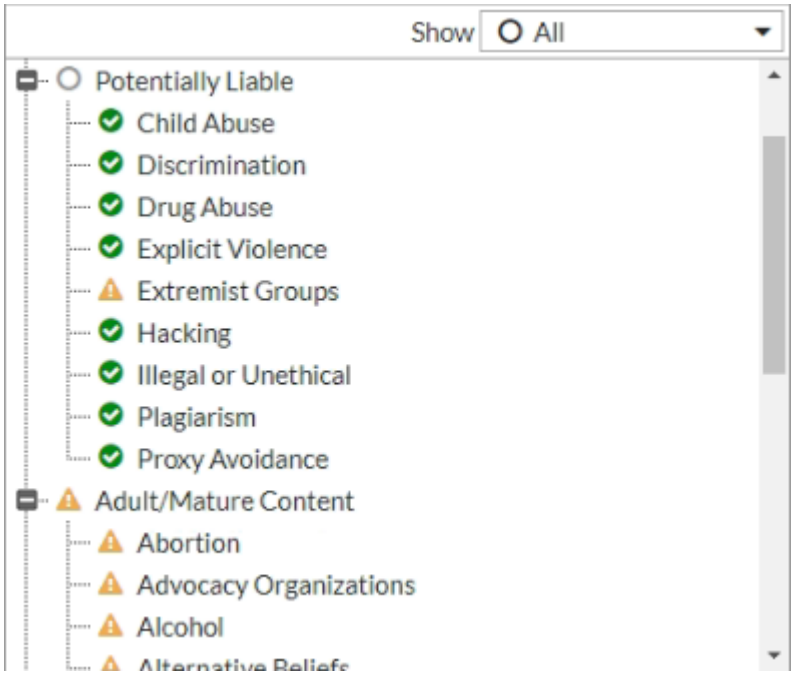
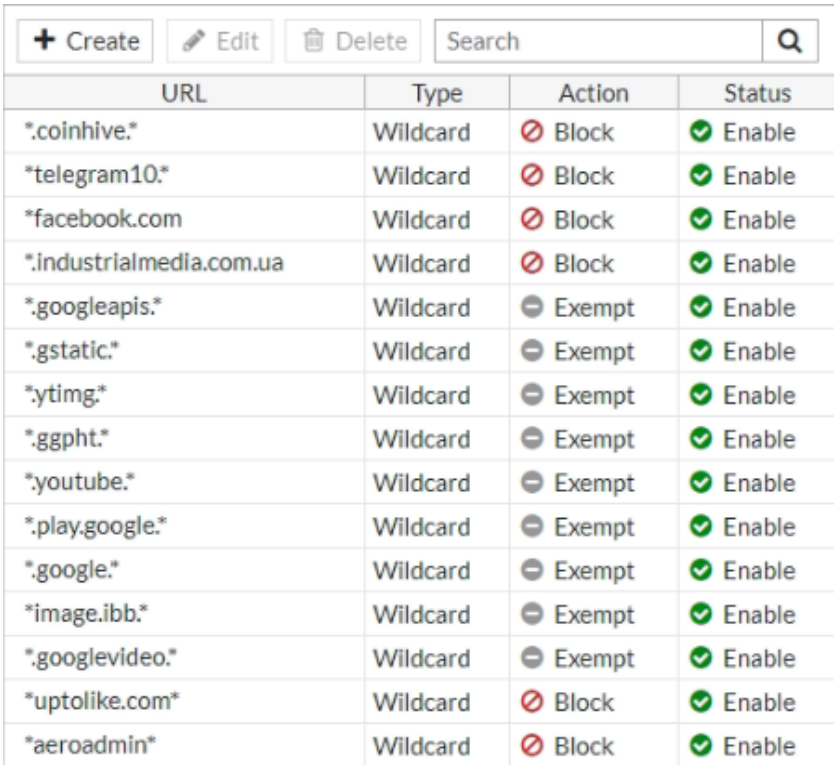


Рис 3.19 - FortiGuard category based filter

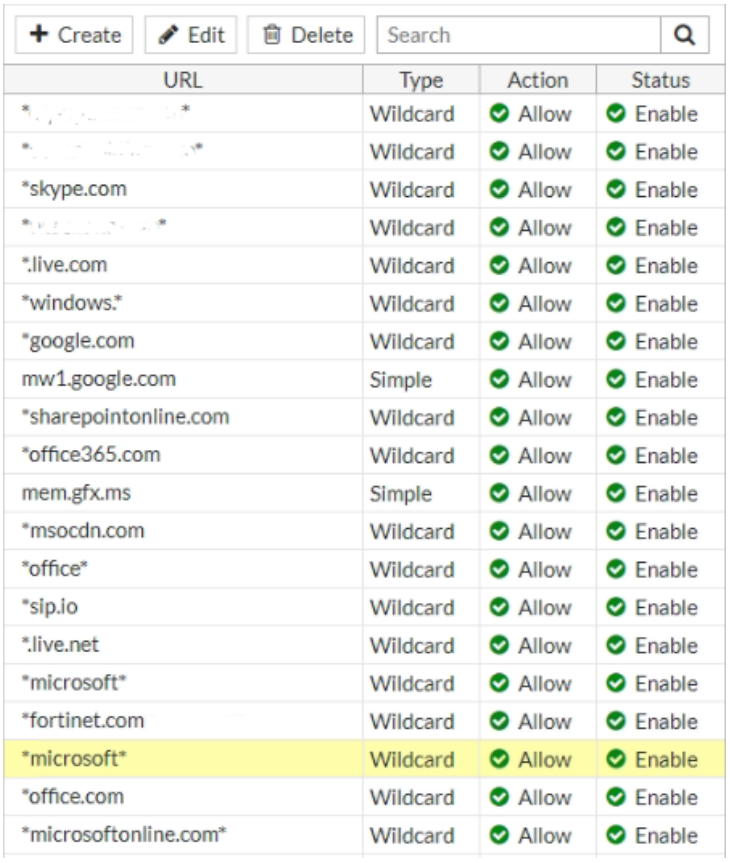
На Рис 3.19 представлені стандартні категорію з базами сігнатур які обновлюються кажного дня, ці категорії використовуються коли не потрібні уточненя по доступам до певних ресурсів, як на Рис 3.20, або Рис 3.31 на якому зображен приклад створення «Білого листа».



+ Create | Edit | Delete | Search

URL	Type	Action	Status
.coinhive.	Wildcard	Block	Enable
telegram10.	Wildcard	Block	Enable
*facebook.com	Wildcard	Block	Enable
*.industrialmedia.com.ua	Wildcard	Block	Enable
.googleapis.	Wildcard	Exempt	Enable
.gstatic.	Wildcard	Exempt	Enable
.ytimg.	Wildcard	Exempt	Enable
.ggpht.	Wildcard	Exempt	Enable
.youtube.	Wildcard	Exempt	Enable
.play.google.	Wildcard	Exempt	Enable
.google.	Wildcard	Exempt	Enable
image.ibb.	Wildcard	Exempt	Enable
.googlevideo.	Wildcard	Exempt	Enable
uptolike.com	Wildcard	Block	Enable
aeroadmin	Wildcard	Block	Enable

Рис 3.20 - Static URL Filter



+ Create | Edit | Delete | Search

URL	Type	Action	Status
*	Wildcard	Allow	Enable
*	Wildcard	Allow	Enable
*skype.com	Wildcard	Allow	Enable
*	Wildcard	Allow	Enable
*.live.com	Wildcard	Allow	Enable
windows.	Wildcard	Allow	Enable
*google.com	Wildcard	Allow	Enable
mw1.google.com	Simple	Allow	Enable
*sharepointonline.com	Wildcard	Allow	Enable
*office365.com	Wildcard	Allow	Enable
mem.gfx.ms	Simple	Allow	Enable
*msocdn.com	Wildcard	Allow	Enable
office	Wildcard	Allow	Enable
*sip.io	Wildcard	Allow	Enable
*.live.net	Wildcard	Allow	Enable
microsoft	Wildcard	Allow	Enable
*fortinet.com	Wildcard	Allow	Enable
microsoft	Wildcard	Allow	Enable
*office.com	Wildcard	Allow	Enable
microsoftonline.com	Wildcard	Allow	Enable

Рис 3.21 – Приклад створення «Білого списку» сайтів до яких надається доступ в конкретному профілі веб-фільтру.

На Рис 3.22 представлений приклад використання Application Control фільтру, який також має схожі базі сігнатур розбиті на категорії, як в веб фільтрі, кожна з категорій сігнатур має 4 статуси: monitor, allow, block, quarantine(Рис 3.23). Відповідно: спостереження за трафіком та оповіщення в разі чогось підозрілого, дозволяти весь трафік, забороняти весь трафік, поміщати весь трафік в карантин.

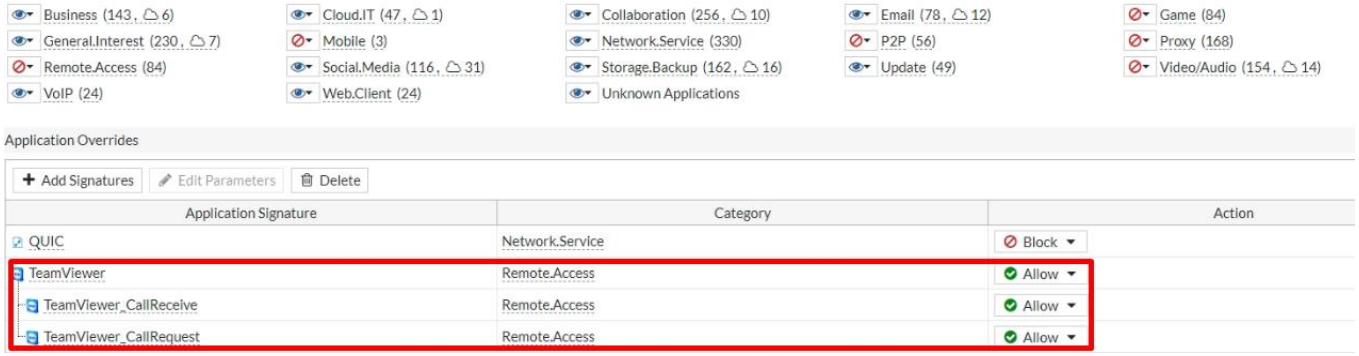


Рис 3.22 - Application Overrides

Також за допомогою Application Overrides можливо більш тонко виконувати налаштування фільтру, наприклад на Рис 3.22 всі додатки з категорії Remote.Access заблоковані, але в вікні Application Overrides є уточнення, яке дозволяє використання додатку TeamViewer не зважаючи на те, що він відноситься до категорії Remote.Access.

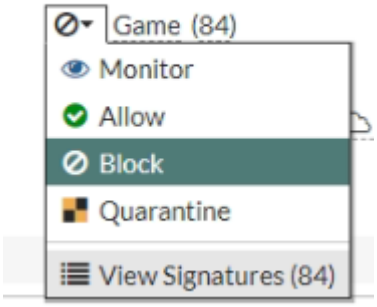


Рис 3.23 – Приклад статусів баз сігнатур

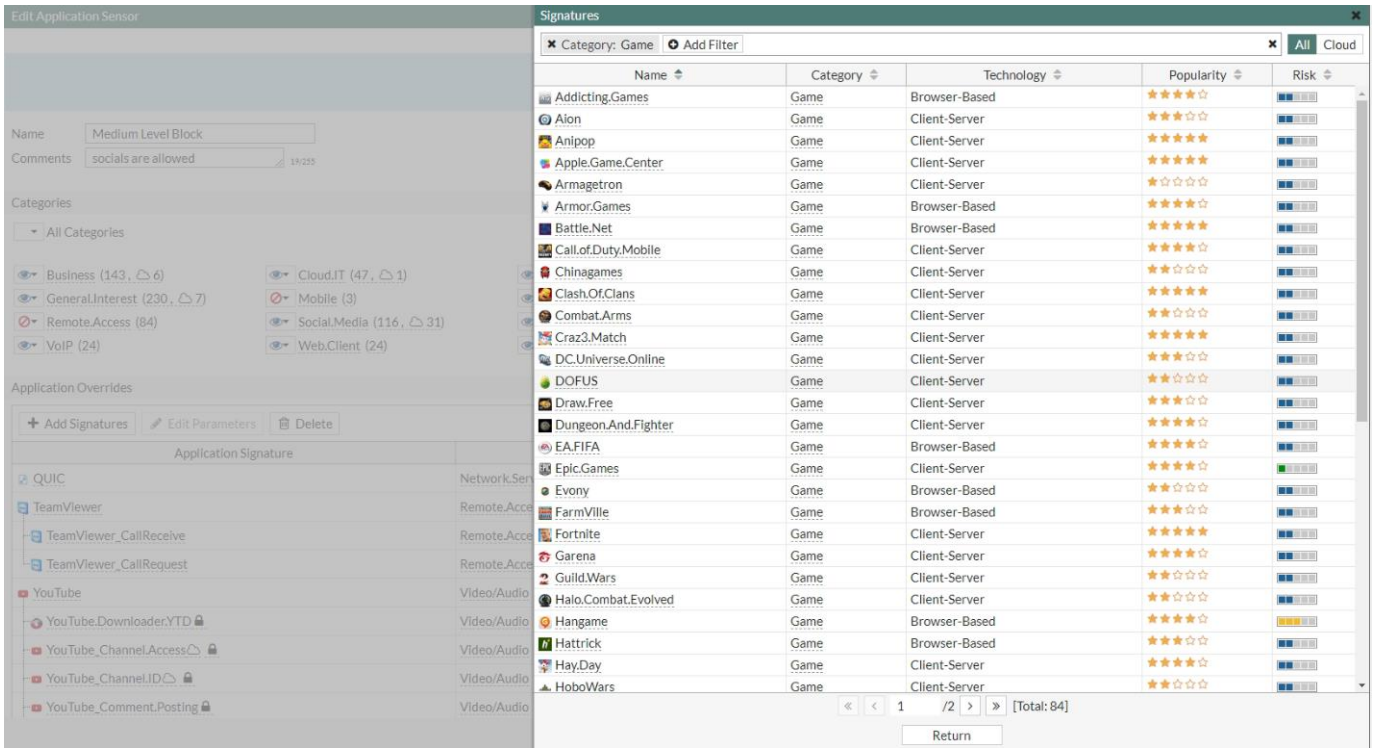


Рис 3.24 – Приклад додатків, які відносяться до категорії Game

ВИСНОВКИ

В результаті виконання цієї магістерської роботи було проведено аналіз проблем в забезпеченні кібербезпеки на підприємствах, аналіз сучасних загроз та розглянуто самі популярні їх види та було встановлено, що в сучасному світі для бізнесу, будь-якого розміру будь-то малий чи середній, або навіть великий необхідно перш за все піклуватися про безпеку своєї локальної мережі. Адже щодня зловмисники створюють нові види вірусів та хакерських атак.

Щоб забезпечити достатній захисту вашій мережі потрібно використовувати мережеві екрани які підходить вам під потреби конкретної корпоративної мережі.

В цьому дипломному проекті було розглянуто самі провідні рішення від компанії Fortinet, також було розглянуто перше налаштування та найважливіші з функцій такі як робота з Security Profiles та Policy and Objects, саме вони при правильному налаштуванні зможуть досить чітко реагувати та відслідковувати всі загрози, які будуть потрапляти в вашу локальну мережу, а завдяки фільтрам та базам сигнатур буде дуже легко обмежити неосвічених в мережевій грамоті людей від різних фішингових ресурсів та інших шкідників, яких ми також розглядали в цьому дипломному проекті.

В результаті чого я вважаю, що розглянутого мережевого екрану достатньо на компанію в який працює від 200 до 300 осіб, тому що саме таке навантаження одночасно є самим оптимальним для моделі Fortigate 100e, але крім кількості осіб потрібно враховувати кількість створенних вами фільтрів та SSL IPsec підключень, тому що це також впливає на продуктивність мережевого екрану. Мету роботи вважаю розкритою.

ПЕРЕЛІК ПОСИЛАНЬ

1. Збірник тез наукових доповідей (Київ, 30 березня 2018 року) АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ УДК 341.123(045)(0.034.2PDF) [Електронний ресурс] – Режим доступу World Wide Web – URL - https://bit.ly/2ZlslY2
2. Міжнародні стандарти інформаційної безпеки \ Міжнародна стандартизація: Стандарти для інформаційної безпеки [Електронний ресурс] – Режим доступу World Wide Web – URL - https://bit.ly/2XdJIHj \ https://bit.ly/2ZiWOWt
3. Антивірусні програми, види та класифікація [Електронний ресурс] – Режим доступу World Wide Web – URL - https://bit.ly/3bNKH6z
4. Забезпечення інформаційної безпеки підприємництва. Е. І. Низенко, В. П. Каленяк, Навчальний посібник, Київ 2006 [Текст] Розділ 1 стр 2 -50
5. Комп'ютерні мережі. Принципи, технології, протоколи, В. Олифер, Н. Олифер. Стандарти третього покоління. Петербург 2016 [Текст] Розділи 14/25/32
6. Fortinet NGFW introduce instruction [Електронний ресурс] – Режим доступу World Wide Web – URL - https://bit.ly/36cxD9s
7. Типы межсетевых экранов и используемые в них технологии. От 16.09.1999 [Електронний ресурс] – Режим доступу World Wide Web – URL - https://www.osp.ru/lan/1999/09/134421/
8. Комп'ютерні мережі, терміни, абревіатури, скорочення, стандарти [Електронний ресурс] – Режим доступу World Wide Web – URL - https://bit.ly/2Zj3x2I
9. FortiGate: Next-Generation Firewalls Models and Specifications [Електронний ресурс] – Режим доступу World Wide Web – URL - https://bit.ly/3bPnXTw
10. Fortigate CookBook, Configuring the network settings, Fortiview, Security profiles, Basic network collection [Електронний ресурс] – Режим доступу World Wide Web – URL - https://bit.ly/2ALaxLF
11. Network Scanning Cookbook: Practical network security using Nmap and Nessus 7 1st Edition, Sairam Jetty USA 2018 [Текст] Розділи 2/5/12/18
12. Fortigate Documents library, Logging and reporting overview, Chapter: Policy & Objects, Chapter 29 - System Administration > Monitoring > Dashboard [Електронний ресурс] – Режим доступу World Wide Web – URL - https://bit.ly/2TogzIm

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)