МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

«Порівняльний аналіз брандмауерів та рекомендації щодо їх застосування в інформаційних системах закладів освіти»

Завідувач випускаючої кафедри **Любчак В.О.**

Керівник роботи **Любчак В.О.**

Студентки групи КБ-81 **Козачок Ю.О.**

СУМИ 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

Затверджую_____

Зав. кафедрою Любчак В.О.

“_____” _____2022р.

ЗАВДАННЯ

до випускної роботи

Студентки четвертого курсу, групи КБ-81 спеціальності «Кібербезпека» денної форми навчання Козачок Юлії Олександрівни.

Тема: «Порівняльний аналіз брандмауерів та рекомендації щодо їх застосування в інформаційних системах закладів освіти»

Затверджена наказом по СумДУ

№_____від_____2022р.

Зміст пояснювальної записки: 1) інформаційний огляд аспектів захисту інформаційної системи; 2) формалізована постановка задачі й формування завдань дослідження; 3) огляд та опис існуючих програмних та апаратних брандмауерів; 4) дослідження питань захисту інформаційної системи закладу освіти; 5) аналіз отриманих результатів.

Дата видачі завдання “_____”_____2022р.

Керівник випускної роботи _____Любчак В.О.

Завдання приняла до виконання _____Козачок Ю.О.

РЕФЕРАТ

Записка: 37 с., 21 рис., 5 табл., 14 джерел.

Мета роботи – скласти вибірку програмних і апаратних брандмауерів та провести огляд з порівняльним аналізом об'єктів із цієї вибірки. Також одним із основних завдань є аналіз мережі СумДУ та дослідження питань її захисту на прикладі ІТ-інфраструктури кампусу «Центр» та надання рекомендацій щодо застосування брандмауерів в інформаційних системах закладів освіти на основі проведеного аналізу.

Об'єкт дослідження – програмні та апаратні брандмауери.

Предмет дослідження – порівняльний аналіз програмних та апаратних брандмауерів.

Результати роботи – у результаті роботи проведено інформаційний огляд та порівняння характеристик програмних та апаратних брандмауерів, розглянуто питання їх застосування для захисту інформаційної системи закладу освіти. Також проведено дослідження стану та складу сегменту мережі СумДУ. Під час практичної частини роботи були досліджені технічні характеристики брандмауерів Cisco, розроблено правило їх налаштування на фільтрацію та розроблено рекомендації щодо їх застосування.

ІНФОРМАЦІЙНА СИСТЕМА, МЕРЕЖЕВА БЕЗПЕКА, МЕРЕЖЕВА ЗАГРОЗА, ЗАХИСТ ВІД МЕРЕЖЕВИХ АТАК, ПРОГРАМНИЙ ТА АПАРАТНИЙ БРАНДМАУЕР

SUMMARY

Every company or institution in its activities today uses the wide range of opportunities provided by the Internet. However, along with the capabilities of the World Wide Web poses many threats to information security, and that is why special attention should be paid to network attacks on the information system and ways to protect against them.

The purpose of this work is to compile a sample of software and hardware firewalls and to conduct a comparative analysis of objects from this sample. Also, one of the main tasks is to analyze the SSU network and investigate its protection on the example of the IT-infrastructure of the campus "Center" and give recommendations on the use of firewalls in the information systems of educational institutions based on the analysis.

Actuality: Modern educational technologies in educational institutions are based on the intensive use of information resources and information systems. The security of these systems is very important for the proper functioning of the educational institution and for ensuring the proper quality of education. Confidentiality, integrity and availability of information are key, because their violation will lead to a negative impact on the educational process: financial losses, inconvenience to students, teachers and administration, etc.

This paper highlights one of the ways to ensure network security of the information system of the educational institution, namely the use of firewalls.

The object of the study: software and hardware firewalls

The subject of the study: comparative analysis of software and hardware firewalls

The objectives of the research:

- to explore aspects of information system protection from a theoretical point of view;
- to conduct a comparative analysis of the most popular software and hardware firewalls;
- to analyze the segment of SSU network, to study its composition and condition;
- to explore software solutions used in this network segment;
- on the basis of the conducted research to give recommendations on the use of firewalls in the information systems of educational institutions.

Methods: theoretical review of literature sources, scientific publications, documentation on the topic of work, as well as their systematization and generalization of information; comparative analysis of the studied objects (namely firewalls used in the network of the campus "Center" SSU); research and test of possible solutions in practice.

The structure and scope of diploma for the bachelor's degree: the paper consists of introduction, three chapters, conclusion and references, which contains 14 names. The total volume of diploma paper for bachelor's degree in 37 pages, including 21 Figures, 5 tables.

The first chapter describes the general aspects of information system protection. It includes information about network security threats, ways to protect against network attacks, then provides information about the firewall as one of the ways to protect the network.

It has been found that a firewall is a system based on software or hardware, which is a kind of intermediary between secure and untested networks, as well as their parts. The main function of a firewall is to filter out harmful and potentially dangerous content and connections. It also prevents unauthorized access to data by attackers, provides access control to network equipment and ports, collects the activity of applications and equipment in statistics. The firewall can be hardware or software. A hardware firewall is the first line of defense, as they are mostly configured on routers that contain customized hardware and software. It monitors every packet that reaches and leaves your network, checking its source, recipient address, and header if it can be trusted. Only when the packet is tested is it allowed to go through the hardware firewall and send it to the destination computer. A software firewall, on the other hand, is more specialized software when the number of users in an organization is relatively small. However, in large organizations, despite the security of the hardware firewall, it is also recommended to use a software firewall.

The second chapter provides an overview and comparison of the most popular solutions among software and hardware firewalls.

6 representatives of software firewalls for OS Windows were selected. The next step was to consider what functions a firewall provides (or does not provide). As a result, a table was created, which describes the main features of each of them. And after analyzing all the information, it was concluded that for optimal protection and prevention of threats, you should choose the Comodo firewall. Among the hardware firewalls, 8 representatives were selected, and their main characteristics and functions were compared in the form of a table. Based on the information in the table above, the number of PCs on the network and the complexity of implementing the presented hardware firewalls, it can be concluded that one of the best options would be to use a firewall from Cisco or Fortinet.

The third chapter provides information on the protection of the SSU network. It was found that the IT-ecosystem of Sumy State University is a set of territorial units (campuses): Main, Center, Medical Institute, Mechanical Engineering College, Shostka and Konotop Institute. The only information and telecommunication system of SSU has 4500 computers. It's a fairly powerful tool,

but it's outdated (less than half of computers are modern and support licensed Windows 10, the rest run on Windows 7 and Windows XP) and need protection.

That is why the introduction of a hardware firewall in this IT-infrastructure was considered on the example of the campus "Center". The first step was to analyze the network and build a diagram that clearly demonstrates the IT-structure of all sites and their relationship. From this diagram it became clear that the main distribution point is located in the building №2, and it is part of the firewalls to which this work is dedicated. The scheme of execution of DNS-requests of network users and the scheme of how HTTP and HTTPS requests pass through a firewall were also constructed.

Next, in the form of a table was shown a comparative characteristic of Cisco firewalls (ASA 5510 and one representative 5525-X), used to protect the studied network segment. The table shows that the Cisco ASA 5525-X is far superior to its "younger brother" in almost all criteria, and this is not surprising, because it is designed for enhanced protection against the latest threats and malware thanks to FirePOWER services that provide integrated protection from threats throughout the attack process: before, during, and after the attack.

An example of setting up a firewall for filtering was also created and recommendations on the use of firewalls in the SSU information system were provided.

CONCLUSION

1. Firewalls are one of the best ways to ensure enterprise network security;
2. Based on a comparative analysis of software firewalls, Comodo became the leader (on the option to protect computer ports from scanning; from changes to critical system files; from viruses, trojans, spyware and zero-day attacks, etc.);
3. Among the hardware firewalls, the leaders were Cisco and Fortinet (providing IPS Detection and Prevention), malware and spam protection, web-based connectivity (SSL VPN), application visibility and control, and URL filtering. -address, etc.);
4. Since the research segment of the network uses a new generation firewall Cisco ASA 5525-X, which has all the necessary functions, the use of software solutions becomes impractical, but software firewalls make sense to use on those corporate computers that are used outside the office, so the best option would be a Comodo firewall;
5. As a hardware protection of the network uses a fairly powerful base of Cisco ASA firewalls, but the representative model 5500-X is only one of several, so we must strive to replace the entire "fleet" of firewalls with these more modern and powerful models.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АБ – Адміністратор безпеки

ГРП – Головний розподільчий пункт

ІС – Інформаційна система

ІСЗО – Інформаційна система закладу освіти

ПЗ – Програмне забезпечення

ПК – Персональний комп'ютер

AMP – Розширений захист від шкідливих програм (Advanced Malware Protection)

AVC – Детальна видимість і контроль додатків (Application Visibility and Control)

DNS – Система доменних імен (Domain Name System)

IDS – Система виявлення вторгнень (Intrusion Detection System)

IPS – Система запобігання вторгненням (Intrusion Prevention System)

LAN – Локальна мережа (Local Area Network)

NAT – Перетворення мережевих адрес (Network Address Translation)

URL – Уніфікований покажчик ресурсу (Uniform Resource Locator)

VLAN – Віртуальна локальна мережа (Virtual Local Area Network)

VPN – Віртуальна приватна мережа (Virtual Private Network)

WAN – Глобальна мережа (Wide Area Network)

ВСТУП

Інформаційна безпека є важливою для забезпечення інтересів будь-якої держави. Створення розвиненого та захищеного середовища, яке має базуватися на новітніх автоматизованих технічних засобах, є передумовою розвитку суспільства та країни.

За останні роки в нашій країні відбулися якісні зміни, що були викликані посиленими впровадженням новочасних інформаційних технологій. Проте, той факт, що інформатизація вдосконалювалась з великою швидкістю, а також те, що вона проникнула в усі сфери, призвело, окрім безсумнівних плюсів, і до появи ряду суттєвих проблем. Як результат, було помічено зріст небезпеки несанкціонованого доступу до комп'ютерних та інформаційно-телекомунікаційних систем.

Сучасні технології навчання у закладах освіти ґрунтуються саме на інтенсивному використанні інформаційних ресурсів та інформаційних систем. Безпека цих систем має дуже важливе значення для нормального функціонування навчального закладу і для забезпечення належної якості освіти. Конфіденційність, цілісність та доступності інформації мають ключове значення, адже їх порушення приведе до негативного впливу на навчальний процес: фінансові збитки, незручності для студентів, викладачів та адміністрації закладу і т.д.

Дана робота висвітлює один із способів забезпечення мережевої безпеки інформаційної системи закладу освіти, а саме використання брандмауерів (мережевих екранів/фаєрволів).

РОЗДІЛ 1 – АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1 Загрози безпеки інформаційної системи

ІС – це сукупність організаційних і промислових методів обробки інформації, які створені для задоволення інформаційних вимог користувачів. Під обробкою розуміються наступні етапи: розшукування, збирання, зберігання, передача й обробка інформації [1].

Кожна ІС має 2 таких компонента:

- апаратне забезпечення – сукупність технічних засобів, які відповідають за функціонування системи (ПК, периферійні пристрої, додаткова апаратура та канали передачі даних);
- програмне забезпечення – набір програм, що використовуються для забезпечення роботи ІС [2].

Орієнтуючись на цю інформацію, можна побудувати приблизну модель ІСЗО (Рис. 1.1).

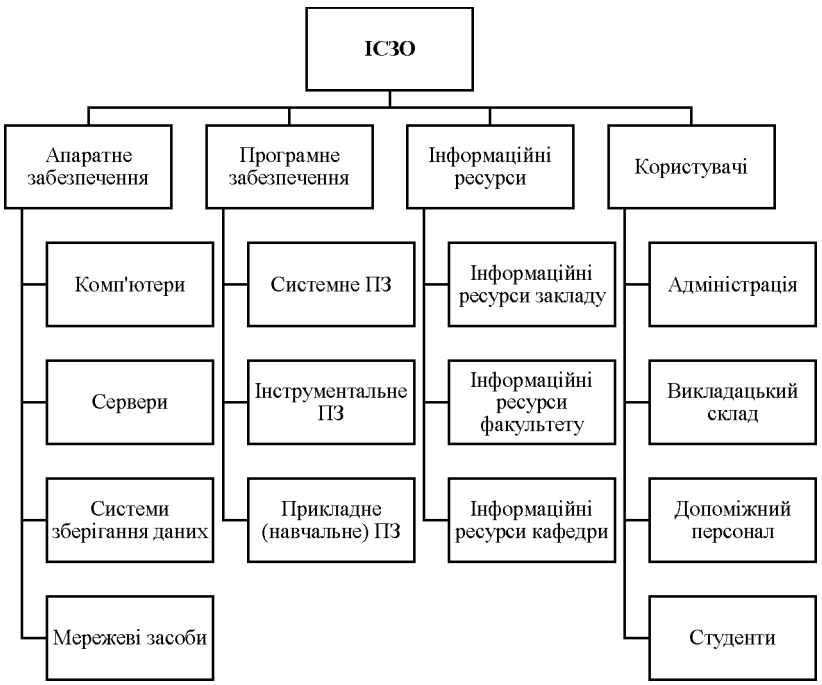


Рис. 1.1. Модель ІСЗО

Як бачимо, модель навчального закладу являє собою досить складну систему, не останнє місце в роботі якої забезпечують апаратні та програмні

засоби, що здійснюють її захист від потенційних загроз (як зовні, так і зсередини).

Дивлячись на це, слід розглянути найбільш ймовірні небезпеки, яким можуть піддатися модерні ІС. Класифікація загроз полягає у наступному:

- за критерієм безпеки інформації, який піддають атаці (доступність, цілісність, конфіденційність);
- за складовими ІС, що є ціллю цих загроз (інформація, програми, апаратне забезпечення);
- за способом реалізації (випадковий/цілеспрямований вплив природного/техногенного походження);
- за розміщенням джерела загроз (чи знаходиться воно всередині або ззовні ІС) [3].

Будь-яке підприємство або установа (у нашому випадку – навчальний заклад) у своїй діяльності сьогодні використовує широкі можливості, які дає Інтернет. Однак разом з можливостями всесвітня мережа приносить безліч загроз інформаційній безпеці, і саме тому особливу увагу слід приділяти саме мережевим атакам на ІС і способам захисту від них.

1.2 Способи захисту ІС від мережевих атак

Мережева атака – це певна дія, що здійснюється з метою отримання контролю над будь-якою локальної або віддаленої обчислювальною системою або комп'ютером. Зловмисники роблять мережеві атаки, щоб захопити управління над операційною системою, привести її до відмови в обслуговуванні або отримати доступ до захищеної інформації [4].

Серед основних принципів забезпечення безпеки ІС навчального закладу від мережевих атак можна виділити наступні:

1. Захист пристроїв, підключених до мережі.

2. Мережеві пристрої повинні бути стійкими до відмов і передбачати можливість швидкого відновлення.

3. Пропускна здатність мережі повинна безперервно контролюватися.

4. Локальна мережа підприємства повинна бути відмовостійкою і передбачати можливість швидкого відновлення в разі потреби.

Система мережевої безпеки являє собою комплекс засобів захисту, а не обмежується лише одним методом (навіть у випадку відмови частини обладнання, інша частина продовжує виконувати свою роботу, що полягає у захисті дані від ймовірних загроз). Вона:

- Здійснює захист від атак, що поступають як зсередини, так і ззовні (всі ймовірні небезпеки, які можуть мати негативний вплив на установу, можуть бути як зовнішнього, так і внутрішнього походження, а дієва система безпеки відслідковує активність в мережі, і у разі виявлення аномалій дає на них слушну реакцію та відповідь);
- Відповідає за те, щоб конфіденційний обмін даними можна було реалізувати в будь-яку годину та з будь-якого місця (співробітники можуть отримати безпечний доступ до мережі, знаходячись вдома);
- Ідентифікує користувачів, тим самим забезпечуючи доступ до інформації (це означає, що правила доступу можуть встановлюватися зважаючи на те, які робочі функції цей користувач має);
- Забезпечує надійність системи (технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням) [5].

Атаки на мережеву інфраструктуру можуть бути як активними, так і пасивними (в залежності від шкідливого програмного забезпечення, яке використовують зловмисники). Тому, щоб забезпечити безпеку мережі, використовуються комплексні заходи:

- балансувальники навантаження (балансувальник навантаження вирішує, на який сервер направити запит, за допомогою комбінації двох чинників: спочатку балансувальник визначає сервери, які можуть швидко і

адекватно зреагувати на запити, а потім він вибирає один з доступних серверів, керуючись попередньо сконфігурованими правилами [6]);

- системи виявлення та запобігання загрозам злому;
- засоби захисту від цільових атак;
- між-мережеві екрани (брандмауери);
- системи моніторингу мережі;
- шифровані канали передачі даних [7].

Про один з цих засобів забезпечення мережевої безпеки навчального закладу, а саме про мережевий екран, ми поговоримо більш детально.

1.3 Брандмауер як один із способів захисту мережі

Мережевий екран (брандмауер, фаєрвол) – це прилад, що відповідає за безпеку мережі, а також що відслідковує мережевий трафік (вхідний та вихідний) і на підставі встановленого набору правил безпеки приймає рішення: пропустити, блокувати або перенаправити по іншому маршруту конкретний трафік [8].

Брандмауер використовується для:

- Фільтрування трафіку, блокування додатків, які намагаються отримати доступ до незахищених системних служб.
- Запобігання несанкціонованому доступу до даних з боку зловмисників і припинення спроб відправки конфіденційної інформації.
- Забезпечення контролю доступу до мережевого обладнання та портів.
- Запису активності додатків/обладнання в статистику.
- Відправки повідомлень при виявленні підозрілої активності або спроб атакувати мережу підприємства [9].

Загальну схему взаємодії локальної мережі з глобальною через мережевий екран можна побачити нижче (Рис. 1.2).

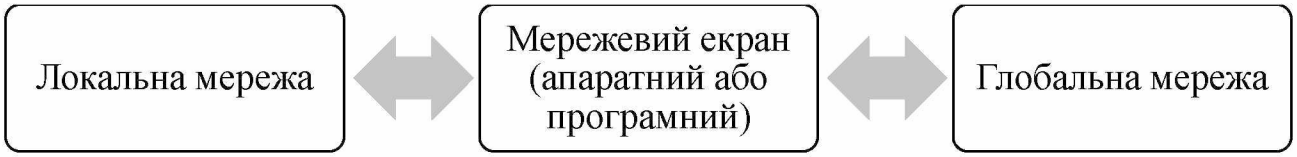


Рис. 1.2. Загальна схема взаємодії локальної та глобальної мережі через брандмауер

Фаєрвол являє собою систему, що базується на апаратному та програмному забезпеченні, та існує як посередник між мережами, які є безпечними, та тими, що являються неперевіреними. Брандмауер також відповідає за те, щоб фільтрувати шкідливі та потенційно небезпечні дані та з'єднання (одна з його головних функцій) [10].

Обмеженнями брандмауерів є:

1) Неможливість захистити від атак, які обходять брандмауер, наприклад, комп'ютери з можливістю підключення до Інтернет-провайдера або використання пулу модемів.

2) Не захищає від внутрішніх загроз, наприклад, незадоволеного працівника або того, хто співпрацює з зловмисником.

3) Не може захистити від передачі заражених вірусом програм або файлів [11].

Між-мережевий екран може бути апаратним або програмним. Нижче ми розглянемо більше детально кожен з них.

1. Апаратний брандмауер

Він є першим на шляху небезпечного трафіку, адже частіше за все він сконфігурований на маршрутизаторі, а, як відомо, саме роутер отримує дані, які надходять на ваш ПК, найпершим. Цей тип брандмауеру відповідає за контроль всіх пакетів, які виходять з вашої мережі, або навпаки прямують до неї. Фаєрвол перевіряє джерело цього пакету даних, адресу одержувача, а також заголовок. Тільки у тому випадку, коли брандмауер перевірив пакет та не знайшов його підозрілим, він проходить через мережевий екран та відправляється на комп'ютер, що є кінцевим адресатом [12].

Плюси апаратного брандмауеру:

✓ Його розміри та кількість енергії, що споживається ним

Зазвичай апаратні мережеві екрани мають менші розміри та енергоспоживання, ніж програмні.

✓ Простота налаштування та використання

Треба лише підключити його, увімкнути, задати певні правила, а все інше він зробить сам.

✓ Продуктивність

Апаратне рішення працює без сторонніх процесів та виконує тільки функцію, для якої безпосередньо він призначений, – фільтрацію пакетів.

✓ Надійність

Апаратний фаєрвол вважається більш надійним за тієї причини, що на них дуже рідко запущені сторонні послуги [13].

2. Програмний брандмауер

Він являє собою більш спеціалізоване програмне забезпечення, та використовується у тих випадках, якщо кількість користувачів в установі менша ніж та, для якої потрібен апаратний захист. Проте, незважаючи на надійність апаратного рішення, в тих організаціях, де кількість користувачів та об'єм мережі великий, рекомендується використовувати не лише апаратний брандмауер, а і програмний [12].

Плюси програмного брандмауеру:

✓ Розширена кількість надаваних функцій

Зазвичай кількість доступних функцій у програмних фаєрволів значно ширша, ніж у їх апаратних побратимів. Слід зазначити, що деякі з цих мережевих екранів містять в собі функції балансування навантаження, IDS/IPS та інші можливості, завдяки яким загальна безпека системи обробки даних значно підвищується.

✓ Захист мережі від внутрішніх загроз

Загрози безпеки не завжди є наслідком зовнішніх факторів, адже атаки можуть виходити і з внутрішніх ПК. Причиною такої атаки може стати, наприклад, колишній співробітник, що залишився незадоволений компанією, або взагалі будь-який користувач LAN.

✓ Функція розмежування локальної мережі без підмереж

Зазвичай у більшості установ до локальної мережі підключаються ПК (включи інше додаткове обладнання) різних відділів. У деяких випадках ці ПК не повинні бути пов'язаними між собою та взаємодіяти один з одним, тому одним з найкращих варіантів буде саме використання фаєрволу, основною функцією якого є захисту ІС персональних даних. Тоді, навіть якщо мережа буде досить великою, буде легко реалізувати її розмежування на підмережі за різними принципами фільтрації пакетів та взаємодії ПЗ за лічені хвилини.

✓ Розгортання на існуючих серверах

При використанні програмного брандмауеру немає потреби в тому, щоб витрачати кошти на ще одну «залізяку», адже достатнім буде на одному з серверів розгорнути мережевий екран і налаштувати NAT і маршрутизацію. Частіше за все ці дії реалізовуються з використанням графічного інтерфейсу фаєрвола і полягають лише у тому, щоб декілька разів клацнути мишею у потрібному місці.

✓ Ціна

Вартість програмного рішення частіше за все є нижче апаратного. Спостереження показали, що захист всією мережі програмним брандмауером за ціною дорівнює середньому апаратному рішенню [13].

На основі цієї інформації виникає багато питань. Який брандмауер краще та надійніше (апаратний чи програмний)? Чи треба використовувати їх окремо один від одного, або разом? Який мережевий екран використовувати в ІСЗО? Саме на ці питання спробуємо отримати відповідь у наступних розділах роботи.

РОЗДІЛ 2 – ПРОГРАМНІ ТА АПАРАТНІ БРАНДМАУЕРИ

2.1 Огляд та порівняння безкоштовних програмних брандмауерів

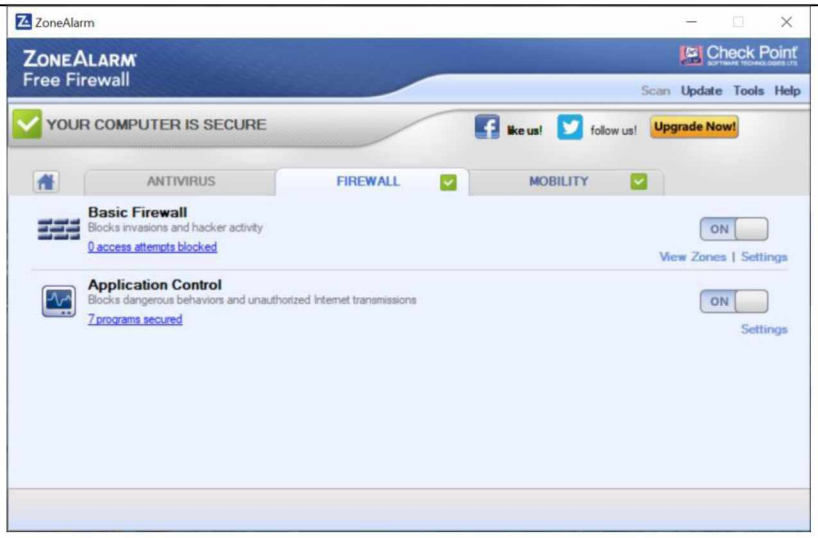
На сьогоднішній день на ПК з операційною системою Windows є власний програмний фаєрвол, але його можливості обмежені, до того ж він не дуже простий у використанні. Нижче (Таблиця 2.1) будуть перераховані та порівняні найкращі безкоштовні брандмауери для цієї ОС, що доступні на ринку.

Таблиця 2.1. Список безкоштовних брандмауерів

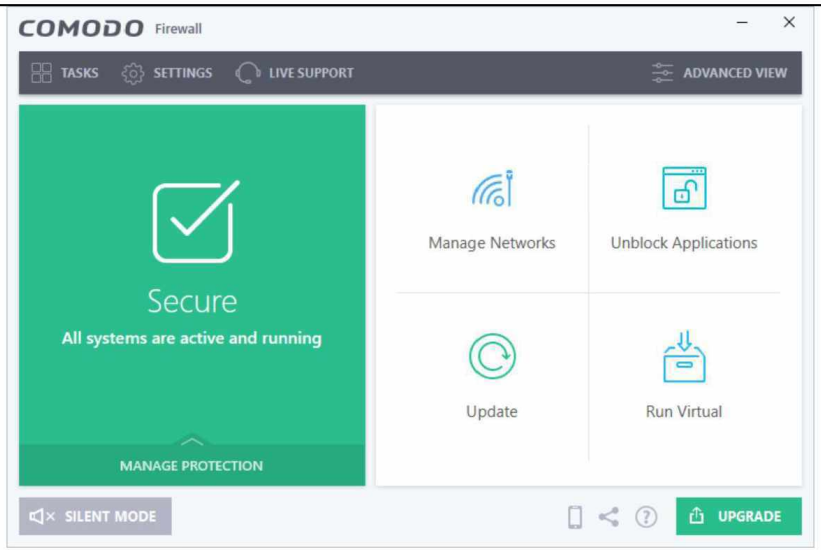
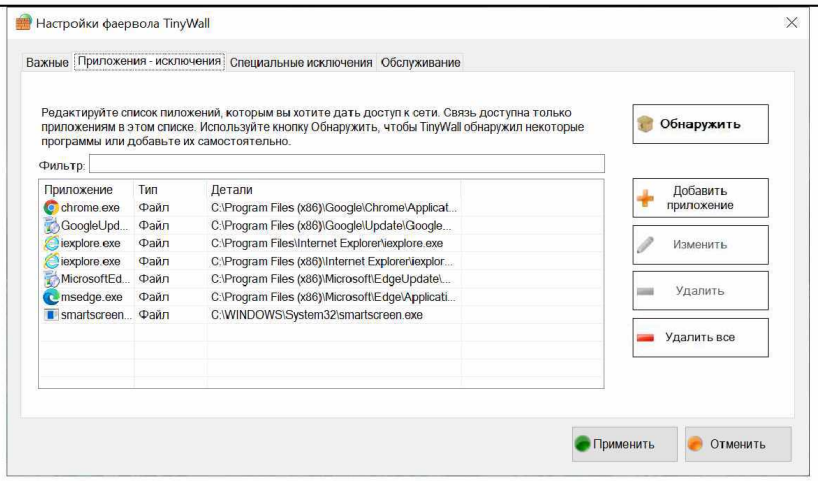
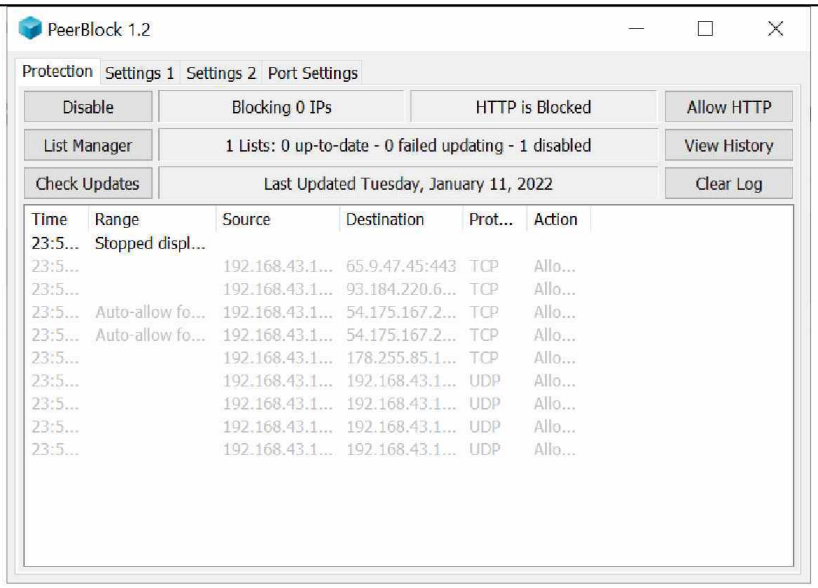
№	Назва	Сумісні версії Windows
1	ZoneAlarm	Windows 10 та Windows 7
2	Comodo	Windows 10, Windows 8, Windows 7, Windows Vista, XP
3	TinyWall	Windows 11, Windows 10, Windows 8.1, Windows 8 та Windows 7
4	PeerBlock	Windows 8, Windows 7 та Windows Vista
5	NetDefender	Windows 2000, Windows XP
6	Privatefirewall	Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, XP

Далі створимо таблицю (Таблиця 2.2), в якій буде показано інтерфейс кожного з фаєрволів, щоб можна було робити висновки щодо їх зрозумілості та інтуїтивності використання.

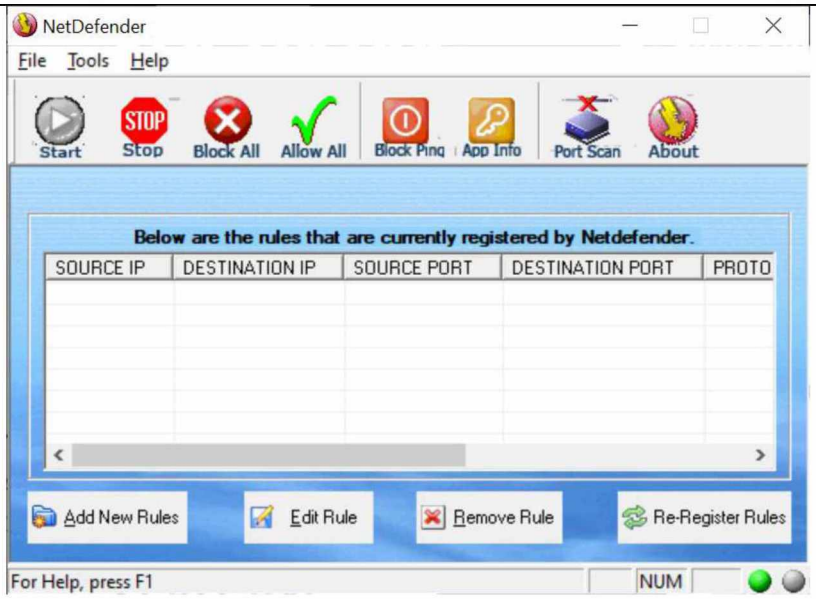
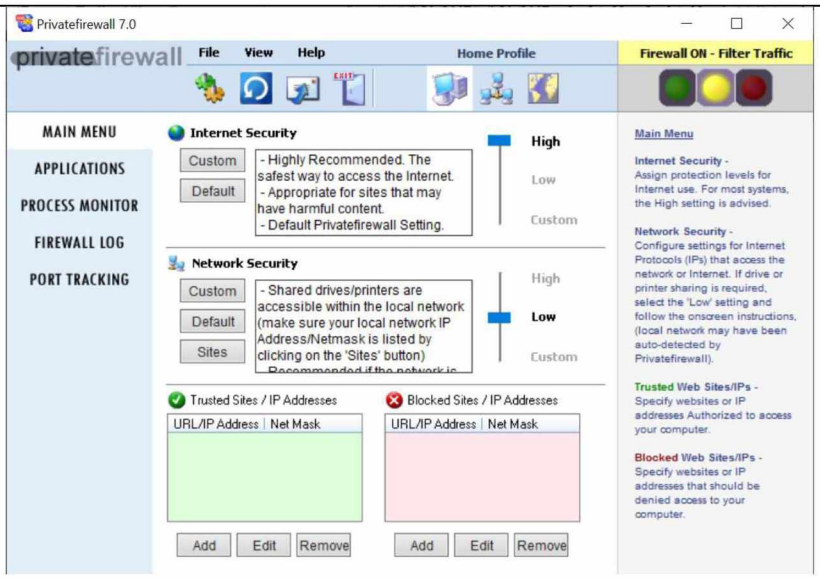
Таблиця 2.2. Інтерфейс брандмауерів

№	Назва	Інтерфейс
1	ZoneAlarm	

Продовження Таблиці 2.2

№	Назва	Інтерфейс
2	Comodo	
3	TinyWall	
4	PeerBlock	

Продовження Таблиці 2.2

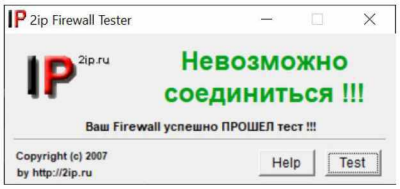
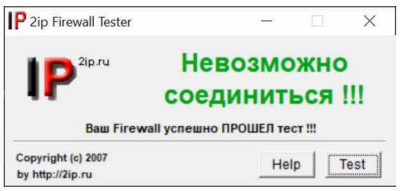
№	Назва	Інтерфейс
5	NetDefender	
6	Privatefirewall	

Тепер створимо таблицю (Таблиця 2.3), в якій будуть вказані основні можливості кожного з вищезазначених брандмауерів та подивимося, які функції надає (або не надає) кожен з них.

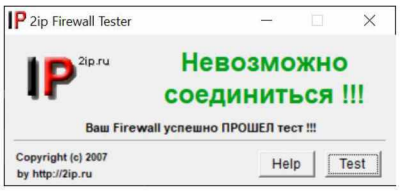
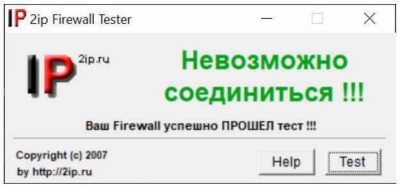
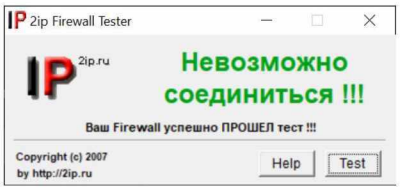
Останнім кроком нам треба перевірити правильність роботи брандмауера. Для цього ми завантажили додаткову утиліту ***2ip Firewall Tester***. При встановленому Інтернет-з'єднанні програма зробить спробу установки зв'язку з сервером розробників, і якщо з'єднання відбудеться, то висновок невтішний: або у вас взагалі немає мережевого екрану, або він не придатний до використання.

Якщо ж з'єднання встановити не вдасться, то в цьому випадку ваша система знаходиться під надійним захистом. Результати цієї перевірки будуть продемонстровані в останньому стовпчику таблиці.

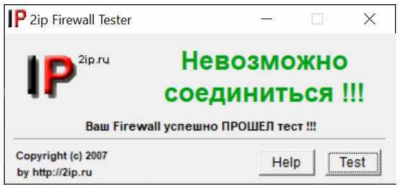
Таблиця 2.3. Характеристики програмних брандмауерів

Назва	**Ключові функції**	**Результат тестування**
ZoneAlarm	• Контроль програм; • Двосторонній фаєрвол (блокує хакерів та зовнішні вторгнення, робить комп'ютер невидимим у мережі); • Моніторинг кредитної картки; • Плагін ZoneAlarm Web Secure Free для браузера Google Chrome (блокує фішингові атаки та безпечно завантажує документи).	
Comodo	• Режим Stealth Mode, щоб зробити комп'ютер повністю невидимим для сканування портів; • Перевіряє цілісність кожної програми, перш ніж дозволити її завантаження в пам'ять комп'ютера; • Блокує віруси, трояни та програми-шпигуни; • Запобігає несанкціонованій зміні критично важливих системних файлів та записів реєстру Windows; • Включає функцію автоматичної пісочниці, яка повністю ізолює ненадійні файли; • Практично непробивний захист від руткітів, впровадження у процеси, кейлоггерів та інших загроз «нульового дня»; • Створення правил користувачів.	

Продовження Таблиці 2.3

Назва	Ключові функції	Результат тестування
TinyWall	• Активно блокує сотні троянів, вірусів та інтернет-хробаків; • Не вимагає від користувача технічних знань про порти, протоколи та деталі додатків; • Використовує мережеві зони, що дозволяє ставити різну поведінку фаєрволу, коли ви вдома, на роботі або в громадському місці; • Запобігає спробам зловмисного програмного забезпечення змінити параметри Брандмауера Windows.	
PeerBlock	• Запобігання мережному доступу до комп'ютера за допомогою незахищених пристроїв (веб-сервера, інші ПК), розміщених в Інтернеті; • Можливість імпортувати або створювати списки користувача; • Можливість завжди дозволяти комп'ютеру підключатися через порт 80 і 443, навіть якщо мережеві джерела знаходяться в чорному списку; • Перегляд журналу з'єднань або очистка лог-файлу.	
NetDefender	• Користувач може заблокувати весь трафік і дозволити весь трафік лише одним клацанням миші; • Міжмережевий екран із фільтрацією пакетів; • Користувач може визначити правило на основі IP-адреси джерела та призначення, номери порту джерела та призначення та протоколу, що використовується; • Сканер портів для сканування системи на наявність відкритих портів.	

Продовження Таблиці 2.3

Назва	Ключові функції	Результат тестування
Privatefirewall	• Антивірусний та антишпигунський захист від загроз «нульового дня»; • Захист від руткітів, експлойтів; • Фільтрування IPv6/IPv4-пакетів, веб-сайтів та IP-адрес; • Модуль Anti-Logger; • Контроль активності програм та процесів, а також захист реєстру Windows; • Виявлення аномалій у системі та в електронній пошті.	

За результатами тестування можна побачити, що всі безкоштовні програмні фаєрволи з нашої вибірки впоралися зі своєю основною задачею і заблокували встановлення зв’язку.

Висновок по програмним брандмауерам:

Усі безкоштовні брандмауери, які були перераховані вище, мають свої переваги і недоліки. Але, проаналізувавши всю цю інформацію, все ж таки можна прийти до висновку, що для оптимального захисту мережі від загроз треба надати перевагу фаєрволу Comodo.

Таке рішення з’явилося на основі наступних факторів:

- Простота, зрозумілість та зручність використання;
- Сучасний інтерфейс;
- Сумісність з більшістю версій Windows (Windows 10, Windows 8, Windows 7, Windows Vista, XP);
- Кількість та якість підтримуваних функцій (особливо важливими з яких є захист портів комп'ютера від сканування; від зміни критично важливих системних файлів; від вірусів, троянів, програм-шпигунів та атак «нульового дня»).

2.2 Огляд та порівняння апаратних брандмауерів

Наступним кроком будемо розглядати та порівнювати найпопулярніші апаратні брандмауери. Їх список можна побачити у Таблиці 2.4, в якій представлено назву фаєрволу та його ключові функції.

Таблиця 2.4. Характеристики апаратних брандмауерів

№	Назва	Ключові функції
1	SonicWall SuperMassive	• Забезпечення найкращого рівня контролю за поведінкою додатків; • Багаторівневий масштабований захист великих мереж з великою кількістю трафіку; • Спрощення адміністрування шляхом застосування політик на основі зібраних даних; • Повна деталізована ідентифікація додатків; • Визначення продуктивності трафіку в режимі реального часу.
2	ALTELL NEO	• Широкий модельний ряд апаратних платформ різної конфігурації; • Апаратна платформа Enterprise-класу (модель 340, форм-фактор 2U) має підвищену щільність мережевих інтерфейсів (до 65 портів RJ45 GbE/до 64 портів SFP GbE/до 16 портів SFP+ 10 GbE); • Продуктивність із шифрування (залежно від апаратної платформи) при використанні алгоритму IPsec становить від 18 Мбіт/с до 2,4 Гбіт/с, OpenVPN - від 14 Мбіт/с до 1,4 Гбіт/с.
3	Zyxel VPN	• Створення приватних віртуальних мереж (VPN); • Відстеження небезпечних IP-адрес за допомогою технології Geo Enforcer; • Блокування підозрілого трафіку за допомогою функції Content Filtering; • Обмеження доступу до небажаних програм та сайтів; • Можливість швидкого налаштування вбудованих сервісів; • Кластеризація та підвищена відмовостійкість.

Продовження Таблиці 2.4

№	Назва	Ключові функції
4	Cisco Firepower NGFW	• Швидке виявлення та блокування загроз; • Можливість цілодобово запобігати порушенням мережевої безпеки на автоматичному рівні; • Глибокий аналіз трафіку; • Автоматичне виявлення пріоритетів подій мережевої безпеки; • Моніторинг та контроль прикладних програм; • Захист від удосконаленого шкідливого ПЗ; • Фільтрування URL-адрес.
5	Cisco ASA (Adaptive Security Appliance)	• Можливості міжмережевого екранування з урахуванням станів з'єднань; • Аналіз прикладних протоколів на глибокому рівні; • Використовуються протоколи забезпечення захисту даних; • Можливість підключення до мережі через веб-інтерфейс (SSL VPN); • Використовуються протоколи динамічної маршрутизації.
6	Juniper SRX	• Захист від кіберзагроз для організацій будь-якого масштабу; • Комплексна мережна безпека; • Максимальна продуктивність та масштабованість; • Високий рівень відмовостійкості; • Підтримує швидкісну роботу мережі з можливістю використання кількох служб.
7	Fortinet FortiGate	• Міжмережеве екранування; • Виявлення та запобігання вторгненням (IPS); • IPSec та SSL VPN; • Захист від шкідливих програм (Антивірус); • Антиспам; • Web-фільтрація; • Контроль додатків; • WAN-оптимізація; • Балансування навантаження; • Маршрутизація/комутація.

Продовження Таблиці 2.4

№	Назва	Ключові функції
8	Huawei USG	• Контекстний/глибокий аналіз; • Безпека додатків та сервісів; • Виявлення та запобігання вторгненням; • Безпека веб-протоколів та додатків; • Безпека електронної пошти; • Захист від витоку чутливої та конфіденційної інформації; • Мережева безпека; • Маршрутизація; • Режими роботи та підвищення відмовостійкості/доступності; • Інтелектуальне управління.

Висновок по апаратним брандмауерам:

На основі інформації, наведеної вище в таблиці, кількості ПК в мережі та трудомісткості впровадження представлених апаратних фаєрволів, можна зробити висновок, що одним із найкращих варіантів буде використання брандмауеру від компанії Cisco або Fortinet.

Ключовими моментами для такого вибору стало наступне:

- Cisco та Fortinet – це відомі у всьому світі компанії, що спеціалізуються на розробці та продажу пристроїв мережевої безпеки, що призначені для великих організацій та телекомунікаційних підприємств;
- Співвідношення «ціна-якість» (середня ціна становить 100-180 тис. грн.);
- Кількість та якість підтримуваних функцій (особливо важливими з яких є система виявлення та запобігання вторгненням (IPS); захист від шкідливих програм, спаму; можливість підключення до мережі через веб-інтерфейс (SSL VPN); видимість і контроль додатків; фільтрація URL-адрес).

РОЗДІЛ 3 – ДОСЛІДЖЕННЯ ПИТАНЬ ЗАХИСТУ МЕРЕЖІ СУМДУ

3.1 Склад та стан мережі СумДУ

ІТ-екосистема Сумського державного університету (СумДУ) являє собою сукупність територіальних підрозділів (кампусів): Головний, Центр, Медичний інститут, Машинобудівний фаховий коледж, Шосткинський та Конотопський інститут. Загальну схему можна побачити нижче (Рис. 3.1).

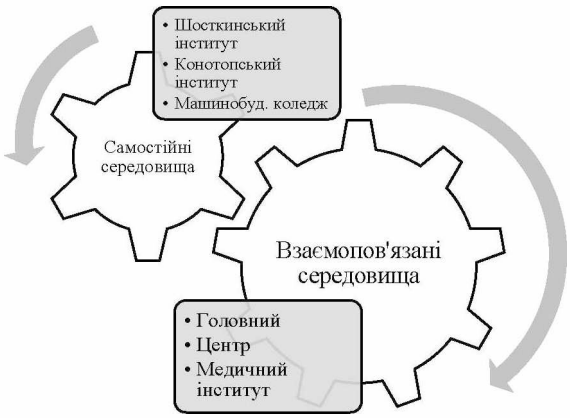


Рис. 3.1. Загальна схема ІТ-екосистеми СумДУ

Єдина інформаційно-телекомунікаційна система СумДУ налічує 4500 комп'ютерів. Вона являє собою досить потужний інструмент, проте вона застаріла (менше половини комп’ютерів сучасні і підтримують ліцензійний Windows 10, інша частина працює на Windows 7 та Windows XP) та потребує захисту.

У наступному розділі на прикладі кампусу «Центр» ми саме розглянемо впровадження апаратного фаєрволу в цю ІТ-інфраструктуру. Основними завданнями буде проаналізувати її та оптимізувати (якщо це буде необхідно).

3.2 IT-інфраструктура кампусу «Центр»

Кампус «Центр» містить у собі такі складові: Корпус №1-3, чотири Гуртожитка, Манеж, Друкарня, Конгрес-центр та Університетська клініка (в т.ч. Розподільчі пункти) (Рис. 3.2).

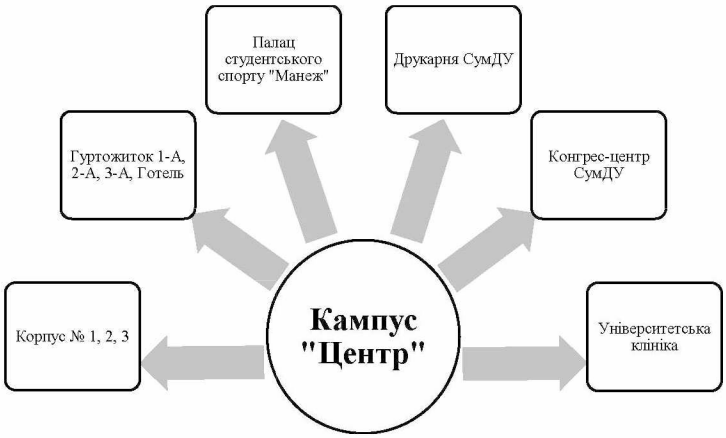


Рис. 3.2. Структура кампусу «Центр»

Наступним кроком був аналіз мережі та побудова схеми, що наглядно демонструє IT-структуру всіх майданчиків та їх взаємозв'язок.

З цієї схеми стало видно, що головний розподільчий пункт (Рис. 3.3) знаходиться у Корпусі №2. Загалом можна відмітити, що через нього вся IT-інфраструктура отримує двосторонній доступ до Інтернету, а також, що майданчики «Конгрес-центр» та «Корпус №3» обмінюються інформацією з ГРП на швидкості 10 гБіт/с, в той час як усі інші між собою – на швидкості 1 гБіт/с.

Сам ГРП налічує у собі два комутатори (пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі) Cisco 4500 – рівень ядра мережі, десять представників моделі 2960 – рівень доступу, один 9300 (рівень розподілення) та один 3560 з PoE (Power over Ethernet) живленням для під'єднання Wi-Fi точок доступу; Zyxel RS – комутатор провайдеру для ізольованого доступу до мережі Інтернет з гуртожитків; крайові (пограничні) маршрутизатори (пристрій, який на основі правил та таблиць маршрутизації відправляє пакети між різними сегментами мережі) Cisco C3925 та C3825, які розташовані на межі мережі (передає дані між локальною та глобальною

мережею); два контроллери Wi-Fi Cisco WC 2504 та мережеві екрани Cisco ASA 5510 і 5525-х.

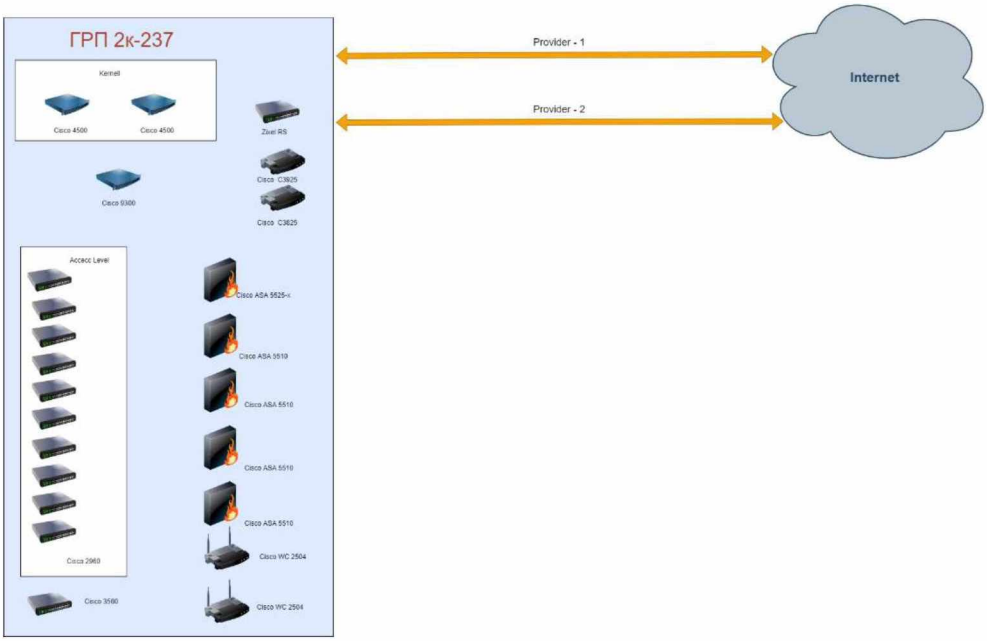


Рис. 3.3. Головний розподільчий пункт

Особливу роль у мережі в цілому та у ГРП зокрема відіграють блок з маршрутизаторів (Cisco WC 2504 (2 шт.), C3825, C3925) та п’яти брандмауерів (чотири представники Cisco ASA 5510 та один 5525-х). Саме через них проходить доступ мережі Інтернет до кампусу «Центр» (Рис. 3.4).

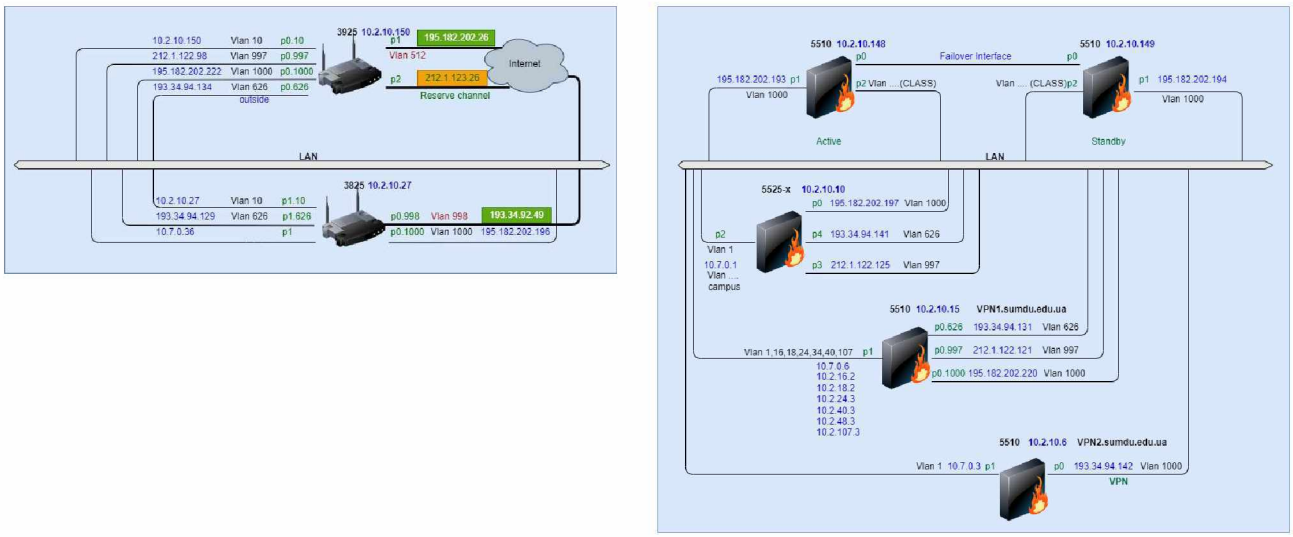


Рис. 3.4. Схема доступу до мережі Інтернет кампусу «Центр»

Наступним кроком було розглянуто те, як саме відбувається зв'язок користувачів з Інтернетом (Рис. 3.5). Користувач мережі кампусу «Центр» вводить запит у рядку браузера на користувацькому ПК. Той, у свою чергу, перенаправляє його на DNS-сервер, який шукає збіги між доменним ім'ям та IP. При виявленні збігів браузер запитує IP-адресу сервера і отримує у відповідь потрібну інформацію, після чого браузер відображає її.

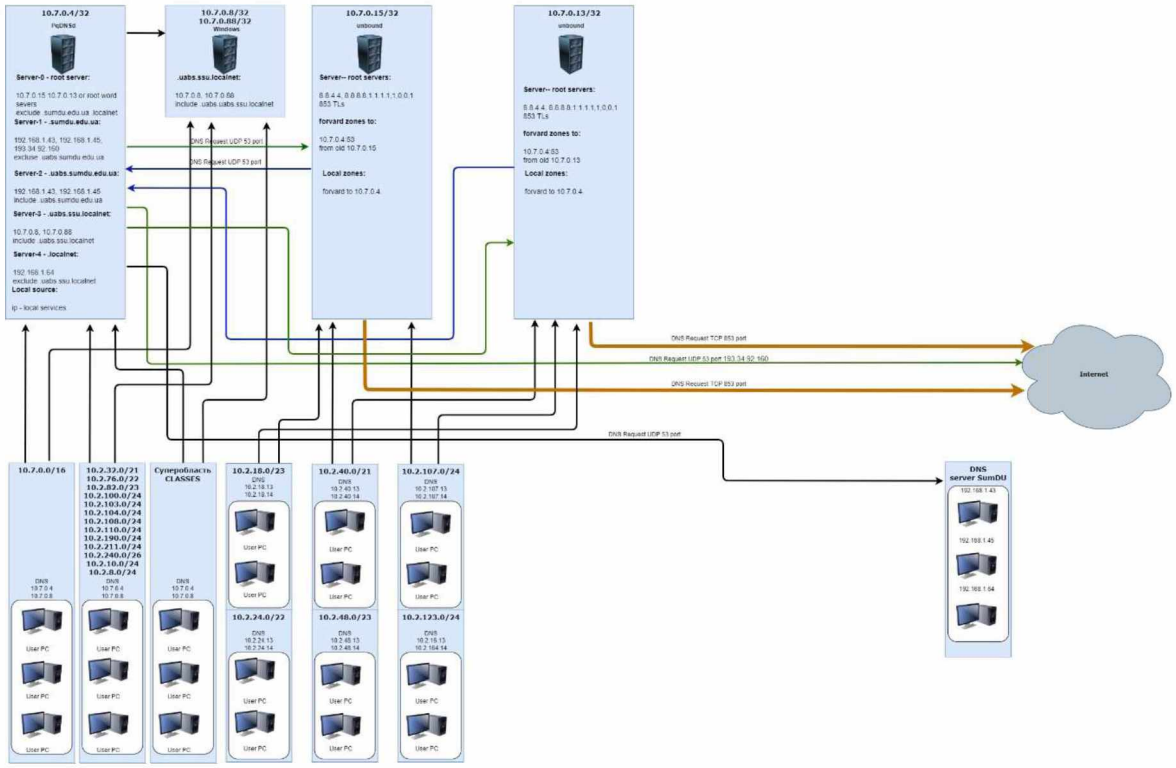


Рис. 3.5. Схема виконання DNS-запитів користувачів мережі

Тепер подивимося на те, як відрізняються http- та https-запити, які проходять через фаєрвол (Рис. 3.6). Як бачимо, по http інформація передається у звичайному (незашифрованому) вигляді (тобто користувач ПК надсилає запит, він проходить через брандмауер у розшифрованому стані, а далі, згідно з політикою, фаєрвол вирішує: чи пропускати цей трафік, чи він не відповідає встановленим правилам та спискам контроля доступу, і на виході ми знову отримуємо дані у незашифрованому вигляді), а по https - у зашифрованому.

Це шифрування даних потрібно для того, щоб зловмисники не змогли нічого прочитати, якщо інформація буде перехоплена.

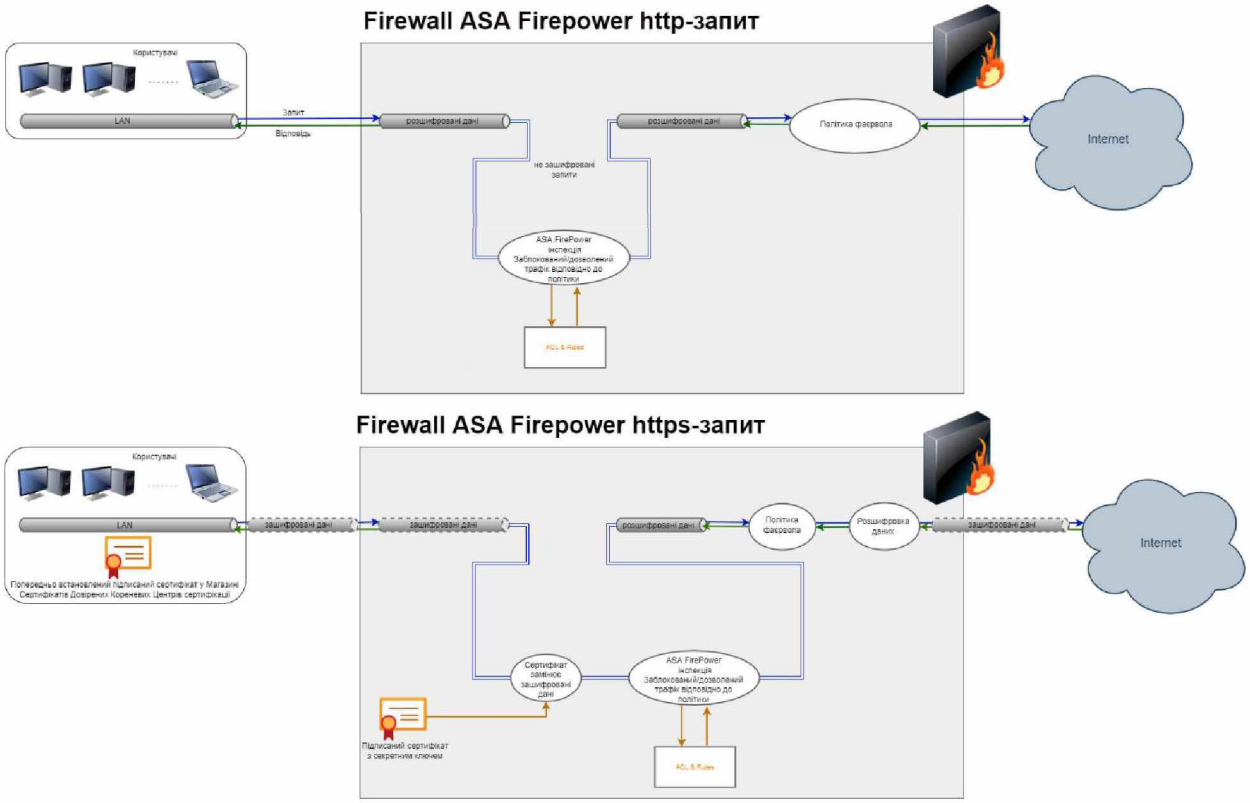


Рис. 3.6. HTTP та HTTPS запити

3.3 Брандмауери, що використовуються в кампусі «Центр»

З попередніх схем ми вже бачили, що для захисту IT-інфраструктури кампусу «Центр» застосовуються фаєрволи компанії Cisco, а саме моделі Cisco ASA 5510 (Рис. 3.7) та один представник 5525-X (Рис. 3.8). Вони слугують для того, щоб бути бар'єром між ненадійними мережами ззовні, яким не можна довіряти (наприклад, Інтернетом), та внутрішніми мережами кампусу, які знаходяться під контролем.

Рис. 3.7. Фаєрвол Cisco ASA 5510

Рис. 3.8. Фаєрвол Cisco ASA 5525-X

Нижче (Таблиця 3.1) можна побачити їх порівняльну характеристику. Вона здійснювалася на основі технічних характеристик кожного з мережевих екранів, які можна знайти в технічній документації Cisco [14].

Таблиця 3.1. Порівняння використовуваних брандмауерів

Характеристики	**Cisco ASA 5510**	**Cisco ASA 5525-X**
Статус підтримки від компанії Cisco	Підтримка зупинилася 30 вересня 2018 р.	Підтримується
Користувачі/вузли	Необмежено	Необмежено
Пропускна здатність IPS	До 300 Мбіт/с	До 600 Мбіт/с
Пропускна здатність 3DES/AES VPN	До 170 Мбіт/с	До 300 Мбіт/с
Піри IPsec VPN	250	750
Віртуальні інтерфейси (VLANs)	50 або 100	750
Нові підключення/секунду	9000	20000
Контексти безпеки (включено/максимум)	0/0 (Base) або 2/5 (Security Plus)	2/20
Висока доступність	Не підтримується або Active/Active та Active/Standby	Active/Active та Active/Standby
Пам'ять	256 МБ	8 ГБ
Інтерфейси передачі даних	4 порти Fast Ethernet або 2 Gigabit Ethernet + 2 Fast Ethernet портів	8 портів Gigabit Ethernet
Порти USB 2.0	2	2

Як бачимо, модель Cisco ASA 5525-X значно перевершує свого «молодшого побратима» майже по всім критеріям, і це не дивно, адже вона призначена саме для розширеного захисту від новітніх загроз та шкідливих програм.

Брандмауер Cisco ASA з сервісами FirePOWER забезпечує об’єднаний захист від загроз протягом всього процесу атаки: перед її початком, під час атаки

та після того, як вона завершилася. Це рішення значно розширює можливості фаєрволів нового покоління Cisco ASA серії 5500-X та перевершує інші сучасні мережеві екрани.

Основні функції брандмауерів нового покоління Cisco ASA з сервісами FirePOWER можна побачити нижче (Рис. 3.9).

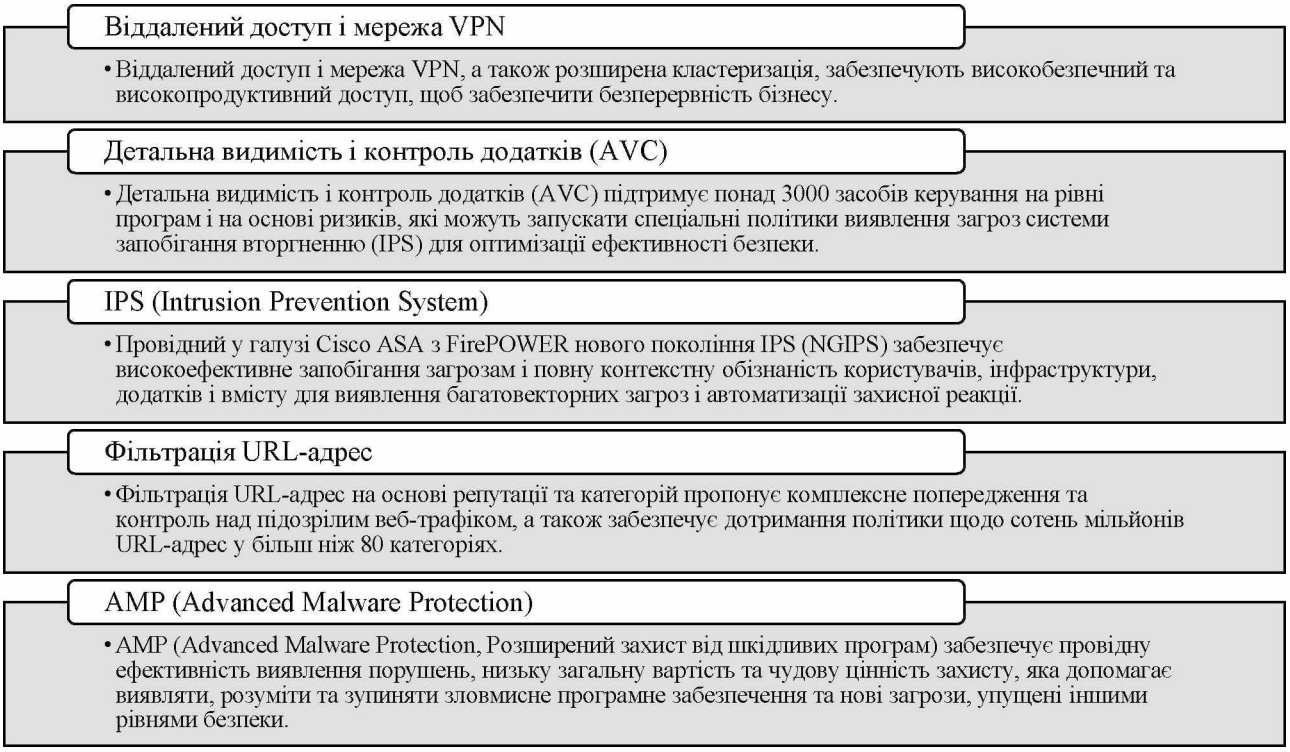


Рис. 3.9. Функції Cisco ASA з сервісами FirePOWER

Управління мережевим екраном Cisco ASA із сервісами FirePOWER здійснюється централізовано з консолі управління Cisco Firepower Management Center (Рис. 3.10), яка надає службам безпеки повний контроль усіх дій у мережі.

Завдяки Cisco Firepower Management Center адміністратори безпеки можуть оптимізувати операції, щоб співвідносити загрози, оцінити їх вплив, автоматично налаштовувати політику безпеки та легко приписувати ідентифікаційні дані користувачів подіям безпеки. Центр управління постійно відстежує те, як мережа змінюється з часом. Нові загрози автоматично оцінюються, щоб визначити ті, які можуть вплинути на ваш бізнес. Потім зусилля з реагування зосереджуються на виправленні, а захист мережі адаптується до мінливих умов загроз.

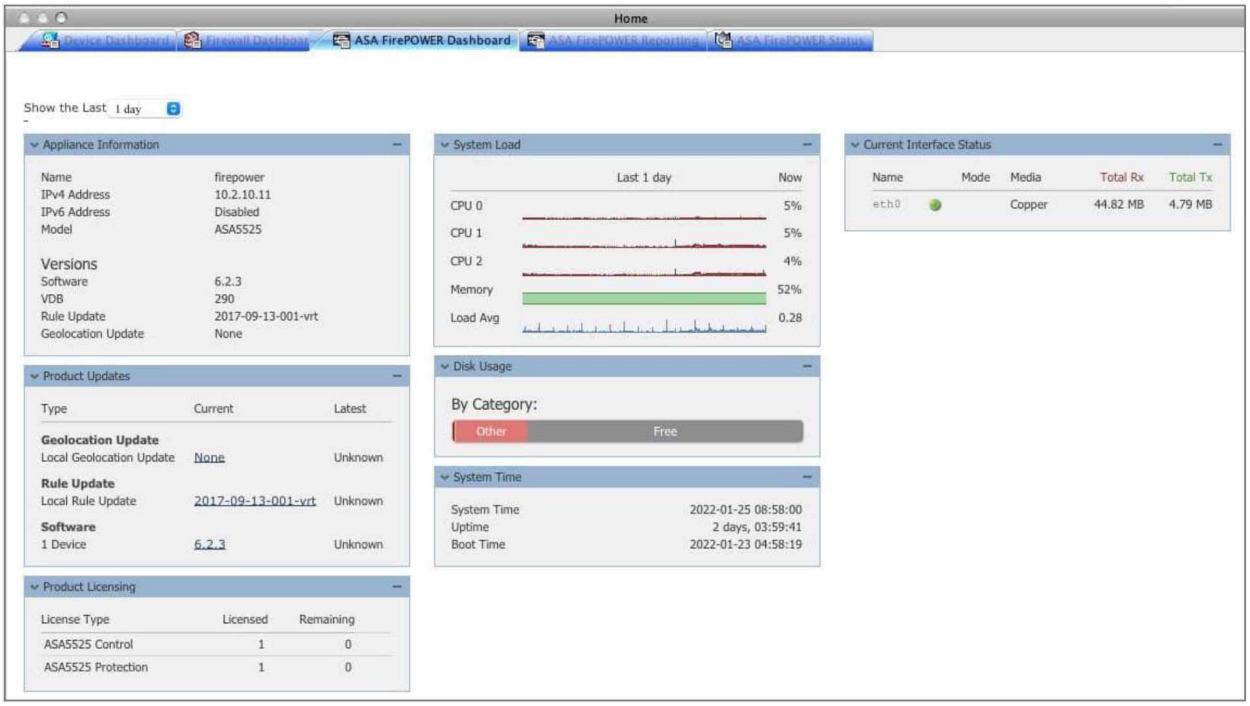


Рис. 3.10. Інтерфейс Cisco FirePOWER Management Center

З рисунку видно, що через консоль Cisco Firepower Management Center на вкладці *ASA FirePOWER Dashboard* адміністратор безпеки може переглядати наступну інформацію:

- Appliance Information (Інформація про пристрій);
- System Load (Завантаження системи);
- Current Interface Status (Поточний стан інтерфейсу);
- Product Updates (Оновлення продукту);
- Disk Usage (Використання диску);
- System Time (Системний час);
- Product Licensing (Ліцензування продукту).

Вкладка *ASA FirePOWER Reporting* (Рис. 3.11) в свою чергу надає АБ певну звітну інформацію.

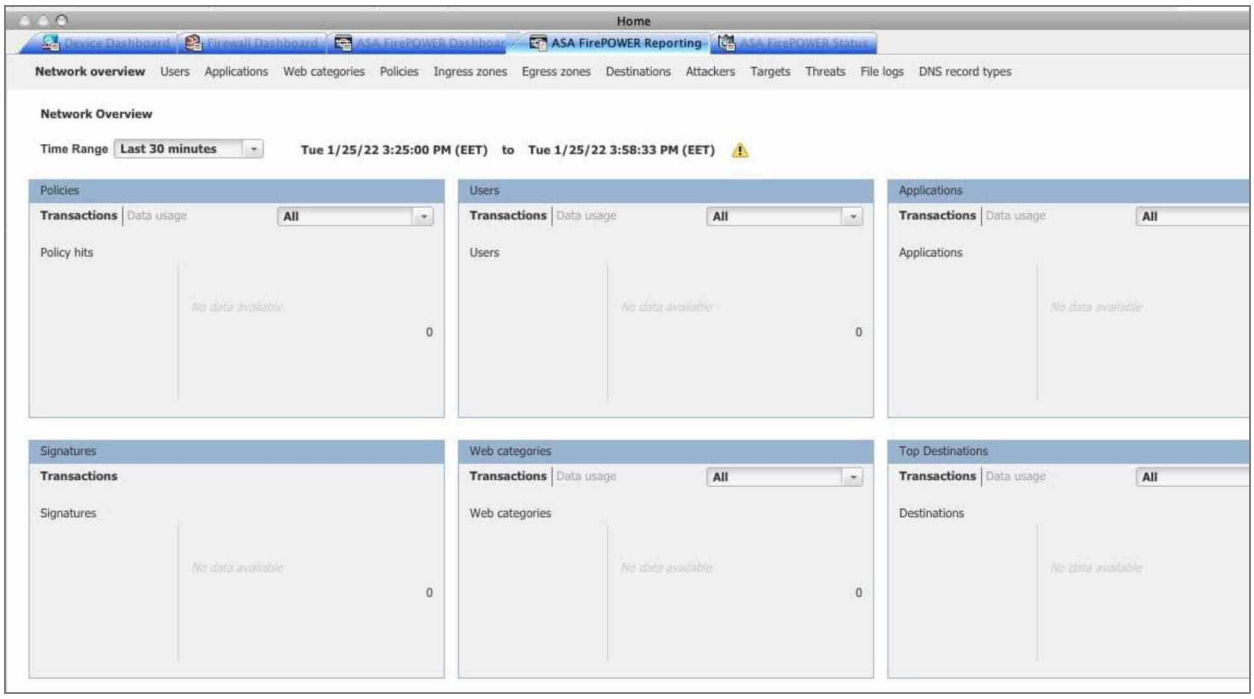


Рис. 3.11. Інтерфейс Cisco FirePOWER Management Center

З цієї вкладки можна отримати звіт по таким категоріям:

- Policies (Політики);
- Users (Користувачі);
- Applications (Додатки);
- Signatures (Сигнатури);
- Web categories (Веб-категорії);
- Top Destinations (Найпопулярніші напрямки).

Також консоль управління містить в собі вкладку (Рис. 3.12), що співвідносить всі події вторгнення з впливом атаки на ціль.

Рис. 3.12. Звітність про події вторгнення

Нижче (Рис. 3.13) можна побачити критерії, по яким здійснюється оцінка впливу атаки.

Рис. 3.13. Оцінка впливу

Це дозволяє аналітикам зосередитися на меншій групі подій, визначає пріоритетність загроз, що спрямовані на певні вразливості, та допомагає зосередити увагу аналітиків завдяки усуненню до 99% «шуму», пов'язаного з моніторингом безпеки та реагуванням.

Ці та інші розділи консолі дозволяють виявити, ідентифікувати, усунути та попередити на майбутнє загрози для мережі.

3.4 Приклад налаштування фаєрвола на фільтрацію

У цьому підрозділі роботи буде створено правило, за яким фаєрвол кампусу «Центр» буде налаштований на фільтрацію (заборону доступу) URL сайтів (доменів), в нашому випадку це http://ukr.net https://ukr.net, для комп'ютеру 10.7.0.25 у цій мережі, щоб перевірити: як він справляється з цією задачею.

На скріншоті (Рис. 3.14) показано правило з категорії «Standart Rules» під назвою «Block-http.ukr.net». Процес його створення продемонстрований на рисунках нижче.

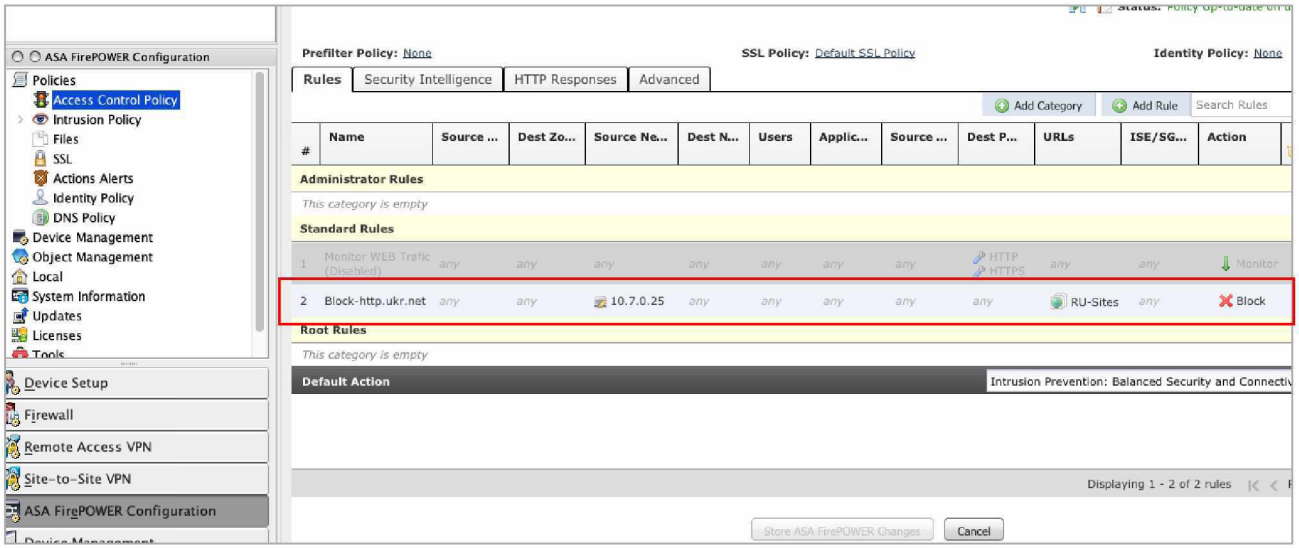


Рис. 3.14. Створене правило на брандмауері

Перш за все необхідно додати правило, в тому числі обрати для нього назву, поставити галочку навпроти пункту «Enabled» та вибрати зі списку дію (ми обрали Block), яка буде встановлена для нього.

Далі ми переходимо на вкладку «Networks» (Рис. 3.15) та обираємо об'єкт, на який буде поширюватися дія цього правила. Ним став ПК 10.7.0.25.

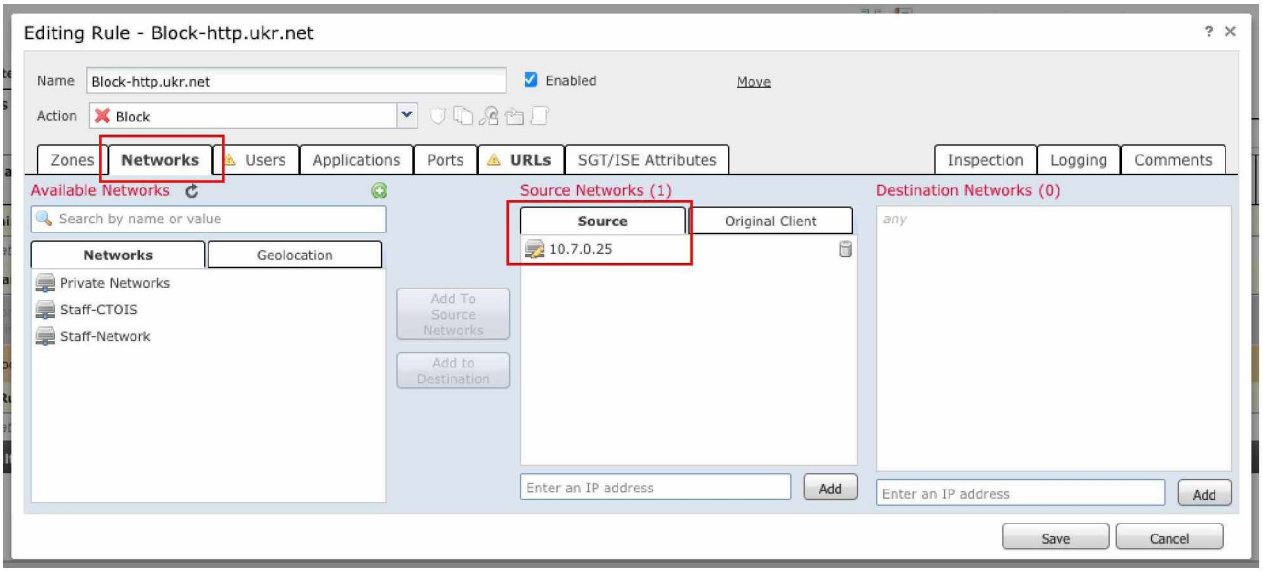


Рис. 3.15. Вкладка «Networks»

Наступним кроком обираємо вкладку «URLs» (Рис. 3.16), на якій в нас є можливість вказати заздалегідь створений URL-список, що має назву «RU-Sites».

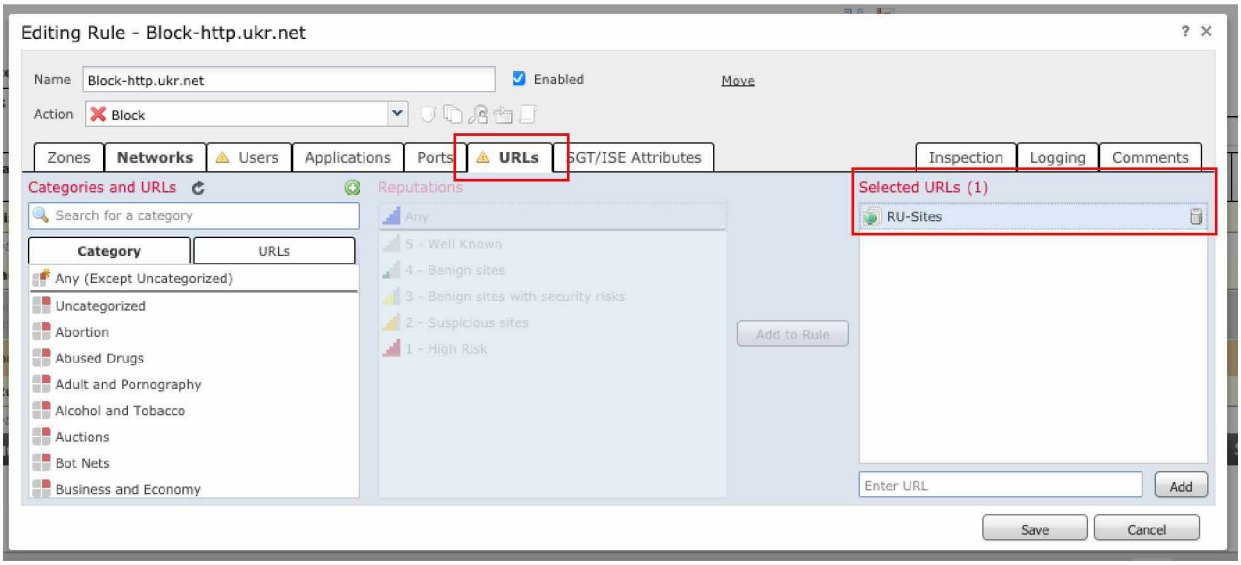


Рис. 3.16. Вкладка «URLs»

Цей список (Рис. 3.17) зберігається в конфігураціях ASA FirePOWER у розділі «URL Lists and Feeds».

Рис. 3.17. RU-Sites List

Принцип його створення полягав в тому, що у текстовий файл «RU-domain.txt» були внесені URL сайтів (доменів), після чого цей файл був завантажений у нашу Cisco ASA FirePOWER (Рис. 3.18).

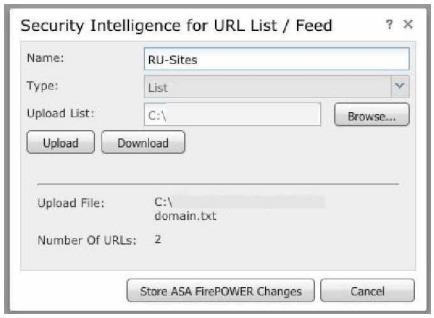


Рис. 3.18. Завантажений файл зі списком URL

У результаті проведених дій для ПК 10.7.0.25 були відфільтровані URL зі створеного нами списку. Результат роботи правила можна побачити нижче (Рис. 3.19).

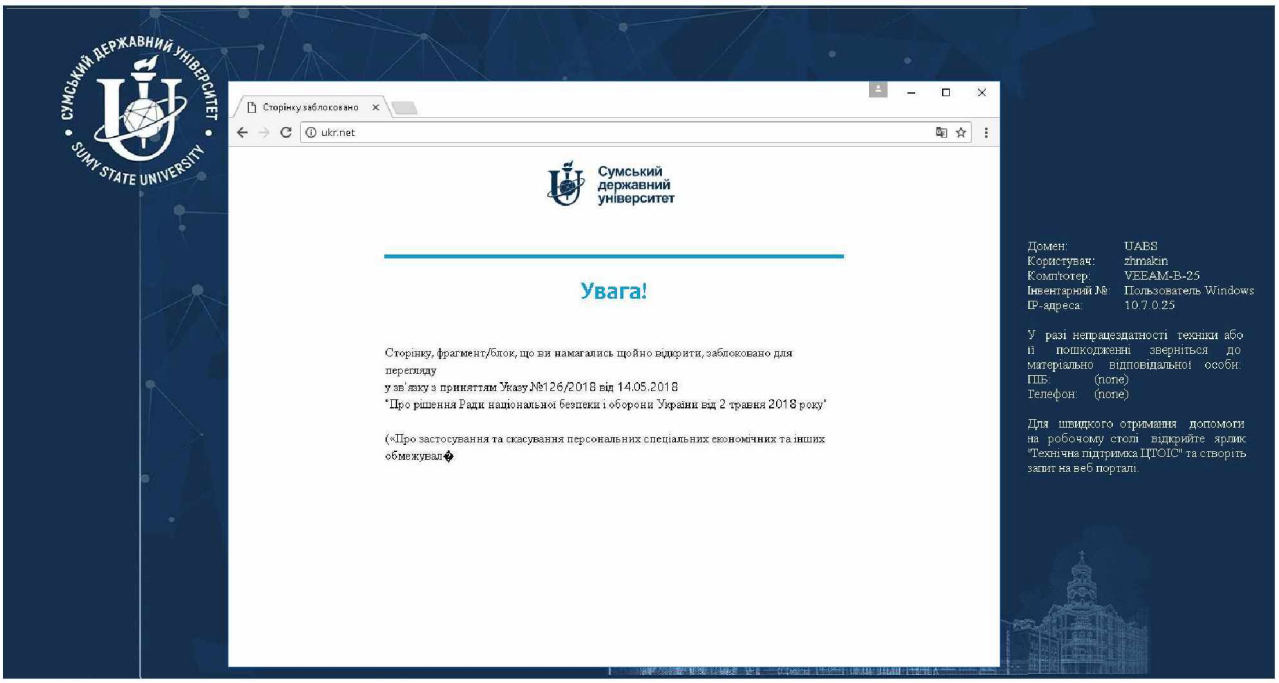


Рис. 3.19. Результат роботи створеного правила

3.5 Рекомендації щодо використання брандмауерів у ІС СумДУ

На прикладі кампусу «Центр» ІТ-екосистеми СумДУ було розглянуто впровадження апаратного брандмауера у мережу. Орієнтуючись на її поточний склад і стан, можна дати наступні рекомендації:

1. Так як в мережі використовується брандмауер нового покоління Cisco ASA 5525-X, що має всі необхідні функції, то використання програмних рішень стає недоцільним.

Проте, програмні фаєрволи є сенс застосовувати на тих корпоративних комп'ютерах, які використовуються поза офісом. Найбільш оптимальним варіантом буде мережевий екран Comodo, який робить невидимими для хакерів порти комп'ютера, блокує шкідливе ПЗ від передачі ваших особистих даних через Інтернет, та надає багато інших корисних послуг. Також важливим є те, що

цей брандмауер доступний майже на всіх версіях Windows, що дозволить уникнути проблем з завантаженням та сумісністю.

2. У якості апаратного захисту мережі використовується досить потужна база з фаєрволів Cisco ASA, в тому числі брандмауер Cisco ASA з сервісами FirePOWER, що забезпечує об'єднаний захист від загроз протягом всього процесу атаки: перед її початком, під час атаки та після того, як вона завершилася.

Проте, представник моделі Cisco 5525-X є лише одним з декількох, тому потрібно прагнути до того, щоб замінити весь «парк» брандмауерів на ці більш сучасні та потужні моделі.

ВИСНОВКИ

Отже, можна зробити висновок, що мережеві екрани дійсно є одним із найкращих способів забезпечення мережевої безпеки підприємства (у нашому випадку закладу освіти), і у попередніх розділах була представлена доцільність та способи їх використання.

На основі огляду та порівнянні характеристик, що проводилися як для програмних рішень, так і для апаратних, було зроблено певні висновки по кожній з цих категорій брандмауерів. Зважаючи на ключові функції кожного мережевого екрану, були виділені наступні представники: серед програмних фаєрволів лідером став Comodo (надає опції захисту портів комп'ютера від сканування; від зміни критично важливих системних файлів; від вірусів, троянів, програм-шпигунів та атак «нульового дня» та ін.), а серед апаратних – фаєрволи від компанії Cisco та Fortinet (надають опції системи виявлення та запобігання вторгненням (IPS); захисту від шкідливих програм, спаму; можливість підключення до мережі через веб-інтерфейс (SSL VPN); видимість і контроль додатків; фільтрація URL-адрес та ін.).

Також, на прикладі сегменту мережі СумДУ було визначено які саме фаєрволи (моделі Cisco ASA 5510 та один представник 5525-X) використовуються, за результатами огляду літератури та документації досліджені їх основні технічні характеристики та функції, створено правило налаштування брандмауеру на фільтрацію визначених URL, і надані рекомендації щодо їх оптимального застосування у інформаційній системі закладу освіти.

Наступним кроком на шляху дослідження буде розглянути не тільки один сегмент, а більш велику частину мережі, і також проаналізувати та розробити рекомендації вже стосовно мережі в цілому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Учасники проектів Вікімедіа. Інформаційна система – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Інформаційна_система (дата звернення: 10.01.2022).
2. Запорожець О. О. Інформаційні системи, їх види. Апаратне та програмне забезпечення інформаційної системи. URL: http://www.kievoit.ippo.kubg.edu.ua/kievoit/2013/95/95.html (дата звернення: 10.01.2022).
3. Види інформаційних загроз. *Google Sites*. URL: https://sites.google.com/site/vidiinformacijnihzagrozinform/ (дата звернення: 10.01.2022).
4. Що таке мережева атака. *UAEU Українська ТОП Газета*. URL: https://uaeu.top/digital-online/shcho-take-merezheva-ataka.html (дата звернення: 12.01.2022).
5. Учасники проектів Вікімедіа. Безпека мережі – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Безпека_мережі (дата звернення: 12.01.2022).
6. Що таке балансування навантаження. URL: https://jak.koshachek.com/articles/shho-take-balansuvannja-navantazhennja.html (дата звернення: 20.05.2022).
7. Що таке мережева безпека: її типи та управління. *Огляди, Ігри, Розваги*. URL: https://uk.myservername.com/what-is-network-security (дата звернення: 12.01.2022).
8. What is a firewall?. *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html#~types-of-firewalls (date of access: 12.01.2022).
9. Міжмережевий екран - захист локальної мережі. *Google Sites*. URL: https://sites.google.com/site/zahistlokalnoiemerezi/zahist/mizmerezevij-ekran (дата звернення: 12.01.2022).

10. Брандмауер - що таке брандмауер (файрвол), як працює ця функція?. *ESET*. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/brandmauer/ (дата звернення: 12.01.2022).
11. DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY. INFORMATION SECURITY [R15A0519] LECTURE NOTES B.TECH III YEAR - II SEM(R15) (2018-19). 138 p.
12. Difference between hardware firewall and software firewall. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/difference-between-hardware-firewall-and-software-firewall/ (date of access: 20.05.2022).
13. Hardware firewalls: vs. software firewalls?. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/hardware-firewalls-better-than-software (date of access: 20.05.2022).
14. Cisco ASA 5500 Series Adaptive Security Appliances Data Sheet. *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-345385.html (date of access: 21.05.2022).