МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Система інформаційної безпеки комп'ютерної мережі на базі обладнання Cisco PIX Firewall»

Виконавець: _____ Олександр ЯРЕМЧУК
(підпис)

Керівник: _____ Віталій КУРУШКІН
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Яремчук Олександр Вікторович
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Система інформаційної безпеки комп'ютерної мережі на базі обладнання Cisco PIX Firewall»
затверджена наказом ректора від «29» березня 2023 р. № 421/ст
2. Термін виконання роботи: з 22.05.2023 р. по 25.06.2023 р.
3. Вихідні дані до роботи: міжмережевий екран Cisco Secure Private Internet Exchange Firewall
4. Зміст пояснювальної записки: Вступ, огляд обладнання Cisco Secure Private Internet Exchange FIrewall, розробка структурної схеми проєкту мережі, налаштування брандмауера Cisco Secure PIX Firewall ,Висновки
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди презентації в програмному пакеті Microsoft PowerPoint, структурна схема проекту мережі

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	22.05.2023-24.05.2023	Виконано
2	Вступ	25.05.2023	Виконано
3	Вимоги щодо забезпечення інфораційної безпеки в компютерніймережі	26.05.2023-29.05.2023	Виконано
4	Програмне забезпечення та апаратні засоби брандмауерів Cisco PIX	30.05.2023-07.06.2023	Виконано
5	Система інформаційної безпеки комп'ютерної мережі на базі обладнання Cisco PIX Firewall	08.06.2023-14.06.2023	Виконано
6	Усунення недоліків та захист кваліфікаційної роботи	15.06.2023-25.06.2023	Виконано

7. Дата видачі завдання: “19" травня 2023 р.

Керівник кваліфікаційної роботи _____ Віталій КУРУШКІН
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Олександр ЯРЕМЧУК
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Система інформаційної безпеки комп'ютерної мережі на базі обладнання Cisco PIX Firewall» містить 69 сторінок, 21 рисунків, 3 таблиці, 6 використаних джерел.

Cisco, PIX, DMZ, VPN, NAT,

Об’єкт дослідження – система інформаційної безпеки на базі обладнання Cisco PIX Firewall.

Предмет дослідження – брандмауер Cisco Secure PIX Firewall.

Мета кваліфікаційної роботи – впровадження в схему проєкта системи інформаційної безпеки комп‘ютерної мережі на базі обладнання Cisco PIX Firewall.

Метод дослідження – проведення експериментів з конфігурацією та тестуванням системи інформаційної безпеки на базі обладнання Cisco PIX Firewall.

Матеріали кваліфікаційної роботи рекомендується використовувати при впровадженні систем інформаційної безпеки в домашніх мережах, невеликих мережах підприємств та при розробці правил корпоративної безпеки.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

DDoS (distributed denial of servise) – розподілена відмова в обслуговуванні.

DoS (denial of servise) – відмова в обслуговуванні.

IDS (intrusion detection system) – система виявлення вторгнень.

UTM (unified grows management) – універсальний пристрій, рішення у сфері комп'ютерної безпеки, що забезпечує потужний комплексний захист від мережевих загроз.

MITM (man in the middle) – атака в якій зловмисник перехоплює сеанс зв'язку між клієнтом і хостом.

SQL (structured query language) – мова програмування для взаємодії користувача з базами даних.

DNS (domain name system) – система доменних імен.

HTTP (hypertext transfer protocol) – протокол передачі гіпертексту.

VPN (virtual private network) – віртуальна приватна мережа.

VLAN (virtual local area network) – віртуальна локальна комп'ютерна мережа.

DMZ (demilitarized zone) – демілітаризована зона.

NAT (network address translation) – перетворення мережевих адрес.

IP (internet protocol) – Інтернет протокол.

SNMP (simple network management protocol) – простий протокол керування мережею.

RMON (remote network monitoring) – дистанційний моніторинг мережі.

RADIUS (remote authentication in dial-in user service) – віддалена автентифікація в службі підключеного користувача.

DHCP (dynamic host configuration protocol) – протокол динамічної конфігурації вузла.

PIX (private internet exchange) – приватний Інтернет обмін.

FTP (file transfer protocol) – протокол передавання файлів.

SMTP (simple mail transfer protocol) – простий протокол пересилання пошти.

RIP (routing information protocol) – протокол інформації про маршрутизацію.

PAT (port address translation) – трансляція адреси порту.

NIC (network interface controller) – контролер мережевих інтерфейсів.

TCP (transmission control protocol) – протокол керування передаванням.

Telnet (teletype network) – мережевий протокол для реалізації текстового інтерфейсу по мережі.

ASA (adaptive security algorithm) – адаптивний алгоритм безпеки.

TFTP (trivial file transfer protocol) – тривіальний протокол передачі файлів.

SPI (serial peripheral interface) – послідовний периферійний інтерфейс.

CLI (command line interface) – інтерфейс командного рядка.

CPE (customer premises equipment) – обладнання приміщень клієнта.

SSH (Secure Shell) – безпечна оболонка.

MPF (modular policy framework) – модульна структура політики.

ICMP (Internet Control Message Protocol) – міжмережевий протокол керуючих повідомлень.

LAN (local area network) – локальна комп'ютерна мережа .

WAN (wide area network) – глобальна мережа .

ВСТУП

Актуальність теми. Інформаційна безпека забезпечується комплексом соціально-правових, морально-етичних норм та технічними засобами. На технічному рівні для забезпечення захисту мережевих систем, безпеки віддаленого доступу та створення надійних політик безпеки застосовуються такі засоби захисту локальних та корпоративних мереж, як міжмережеві екрани. Проблема інформаційного захисту та безпеки локальних мереж є важливою та актуальною. Цілком вона не вирішена і на сьогоднішній день. Практично це одна із ключових проблем розвитку інформаційного суспільства.

Зв'язок роботи з науковими програмами, планами, темами.

Мета і завдання дослідження. впровадження в схему проєкта системи інформаційної безпеки комп'ютерної мережі на базі обладнання Cisco PIX Firewall

Завдання кваліфікаційної роботи:

1) визначення вимог щодо забезпечення інформаційної безпеки в комп'ютерній мережі;
2) огляд обладнання Cisco Secure Private Internet Exchange FIrewall;
3) розробка структурної схеми проєкту мережі.
4) налаштування брандмауера Cisco Secure PIX Firewall

Об'єктом дослідження – система інформаційної безпеки на базі обладнання Cisco PIX Firewall.

Предметом дослідження – брандмауер Cisco Secure PIX Firewall.

Методи досліджень. Аналіз літературних джерел, вивчення документації від Cisco, проведення експериментів з конфігурацією та тестуванням системи.

Практичне значення отриманих результатів.

Практичне значення отриманих результатів полягає у вдосконаленні системи інформаційної безпеки комп'ютерної мережі з використанням обладнання Cisco PIX Firewall. Результати дослідження можуть сприяти покращенню захисту інформації в мережі, забезпечити виявлення і запобігання можливим атакам та злому.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2023 р.

РОЗДІЛ 1
ВИМОГИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

1.1. Основні визначення безпеки мереж

Безпека мережі – це захист основної мережевої інфраструктури від несанкціонованого доступу, зловживання або крадіжки. Він передбачає створення безпечної інфраструктури для пристроїв, додатків, користувачів та додатків для надійної роботи.

Безпека мережі поєднує в собі кілька шарів захисних сил на краю та в мережі. Кожен мережевий рівень безпеки реалізує політику та управління. Уповноважені користувачі отримують доступ до мережевих ресурсів, але шкідливі суб'єкти блокуються від проведення атак та загроз.

На даний час, мережева архітектура стикається з постійними загрозами, які постійно змінюється, і правопорушники, які завжди намагаються знайти і використати вразливості. Дані вразливості існують в багатьох сферах. Тому на сьогоднішній день існує велика кількість інструментів та додатків для управління мережевою безпекою, які були створенні для боротьби з окремими загрозами і вразливостями, а також на усунення невідповідностей нормативним вимогам. Адже декілька хвилин простою можуть спричинити масштабні збої в роботі і завдати значних збитків та шкоди репутації організації, важливо, щоб дані заходи захисту були в наявності [1].

Типи мережевої безпеки:

- Брандмауер – це мережевий пристрій безпеки, який відстежує вхідний та вихідний мережевий трафік, і вирішує, чи дозволяти чи блокувати конкретний трафік на основі визначеного набору правил безпеки. Cisco пропонує як брандмауери, орієнтовані на загрозу, так і пристрої Unified Grows Management (UTM).

- Система профілактики вторгнень (IPS) сканує мережевий трафік для активних блоків атак. Безпечні прилади IPS роблять це шляхом співвідношення величезної кількості глобальної розвідки про загрозу не тільки блокують зловмисну діяльність, але й відстежують прогресування підозрюваних файлів та зловмисного програмного забезпечення в мережі, щоб запобігти поширенню спалахів та реінфекції. IPS повинна відстежувати активність у реальному часі та швидко реалізовувати дії щодо запобігання атакам.
- Безпека робочого навантаження захищає робочі навантаження, що рухаються в різних хмарних та гібридних середовищах. Ці розподілені навантаження мають більші атаки, які повинні бути забезпечені, не впливаючи на працездатність бізнесу.
- Визначена програмним забезпеченням сегментація ставить мережевий трафік у різні класифікації та полегшує застосування політики безпеки. В ідеалі класифікації базуються на ідентичності кінцевої точки, а не просто IP-адрес. Ви можете призначити права доступу на основі ролі, місцезнаходження та іншого, щоб правильний рівень доступу надавався потрібним людям.
- Віртуальна приватна мережа шифрує з'єднання з кінцевої точки до мережі, часто через Інтернет. Принцип роботи полягає в маскуванні IP-адрес користувачів і шифруванні даних, в результаті чого користувачі не мають дозволу на отримання таких даних. Як правило, VPN з віддаленим доступом використовує рівень IPSEC для аутентифікації зв'язку між пристроєм та мережею.

1.2. Категорії загроз

Зміст інформаційної безпеки включає в себе область інформації. Інформаційна область – це обсяг предметів, пов'язаних із створенням, трансформацією та споживанням інформації. В основі поняття «інформаційна безпека» лежить поняття «безпеки», яке знаходить своє відображення в Законі України «Про національну безпеку України».

Безпека – стан захищеності життєво важливих інтересів особистості, спільноти, суспільства, держави від внутрішніх та зовнішніх загроз;

Нині інформація є найважливішим активом більшості організацій. За останній час активізувалися кіберзлочинці, кібератаки стали складнішими та вузьконаправленими. Головно ціллю кіберзлочинів є викрадення приватної інформації, вимагання, шпигунство, заподіяння шкоди інфраструктурі [2].

Метою інформаційної безпеки є забезпечення конфіденційності, цілісності та доступності інформації для захисту установ від викрадення, втрат та отримання доступу до важливої інформації.

Інформаційна безпека – стан захисту життєво важливих інтересів особистості, суспільства, держави в інформаційній сфері від зовнішніх та внутрішніх загроз, забезпечуючи його формування, використання та розвиток.

Слід зазначити, що одним із найважливіших аспектів інформаційної безпеки є визначення та класифікація можливих загроз безпеці.

Загроза безпеки – це набір умов та факторів, які створюють небезпеку для життєво важливих інтересів особистості, суспільства та держави.

Класифікація загроз може бути представлена у вигляді таблиці 1.

Таблиця 1.1

Види загроз

Загрози		Зовнішні	Внутрішні
Природні	Навмисні	Розвиток технологій	
	Ненавмисні	Стихійні лиха	1. Відмови техніки 2. Технічні збої
Штучні	Навмисні	1. Розробка ПЗ 2. Загроза цілісності 3. Відмова в обслуговуванні	1. Загроза розголошення (порушення конфіденційності) 2. Загроза цілісності 3. Відмова
	Ненавмисні	1. Політичні фактори 2. Соціальні фактори	Помилки ПЗ

1.3. Як порушується безпека мереж

Порушення безпеки даних - це випадок, в наслідок котрого не вповноважені особи отримують доступ до таємних даних або секретної інформації, враховуючи персональні дані (особисті файли, номери банківських рахунків) або корпоративні дані (записи даних про клієнтів, інтелектуальну власність, фінансову звітність).

Порушення безпеки даних відбувається, коли кіберзлочинець проникає в джерело даних і витягує конфіденційну інформацію. Це може бути зроблено через отримання доступу до комп'ютера або мережі задля крадіжки локальних файлів або шляхом дистанційного обходу мережевого захисту. Хоча більшість витоків даних пов'язані з хакерськими атаками або атаками шкідливих програм, інші методи порушення включають витоки інформації зсередини, шахрайство з платіжними картками, втрату або крадіжку фізичного жорсткого диска з файлами, а також людські помилки.

Більшість хакерських атак мотивуються фінансовою вигодою. Хакери можуть викрадати номери кредиток, банківських рахунків або іншу фінансову інформацію, щоб виводити кошти напряму з рахунків людей і компаній. Вони можуть викрадати персональну інформацію - номери соціального страхування та номери телефонів - для крадіжки особистої інформації (отримання кредитів та відкриття кредитних карток на ім'я своїх жертв) або для продажу в Dark Web, де за номер соціального страхування можна отримати до 1 долара, а за номер паспорта - до 2 000 доларів. Порушення безпеки даних може мати й інші цілі. Незаконні організації можуть викрадати комерційну таємницю у конкурентів. Урядові структури можуть зламувати державні системи, щоб викрасти інформацію про важливі політичні домовленості, військові операції або національну інфраструктуру. Деякі порушення є чисто диструктивними, коли хакери отримують доступ до секретних даних лише для того, щоб знищити або зіпсувати їх. Такі деструктивні атаки, на які припадає 17 відсотків порушень, згідно зі звітом "Вартість витоку даних 2022", часто є справою рук національних держав або хактивістських груп, які прагнуть завдати шкоди організаціям [3].

Навмисні порушення безпеки даних, спричинені внутрішніми чи зовнішніми загрозами, дотримуються однієї і тієї ж моделі:

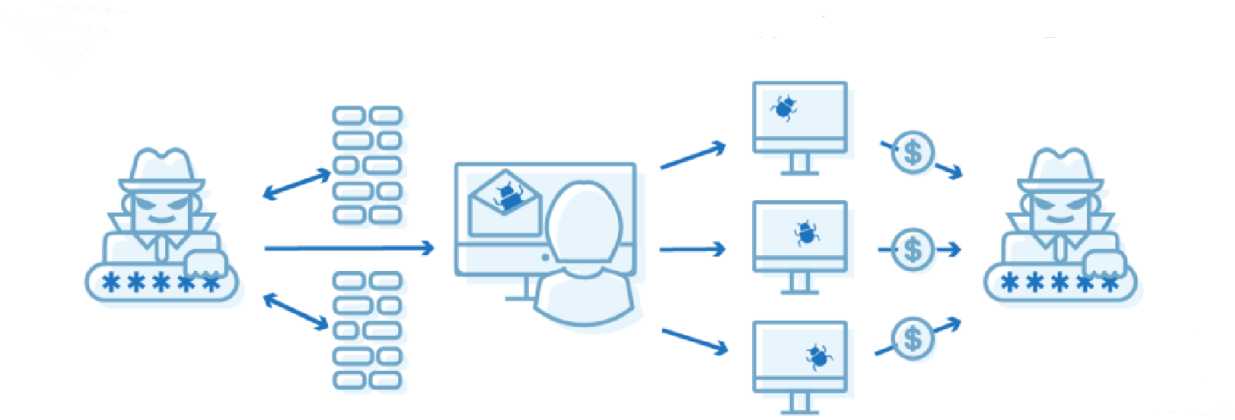

Рис. 1.1. Модель навмисного порушення безпеки даних

Дослідження(розвідка). Хакери підбирають мішень, а потім шукають вразливі місця, якими можна скористатись у комп'ютерній системі чи працівниках мішені. Крім того, вони також можуть купити раніше викрадену інформацію, яка дасть їм доступ до комп'ютерної мережі жертви.

Атака. Визначивши мішень і спосіб, хакер починає атаку. Хакер може почати проводити кампанію соціальної інженерії, безпосередньо експлуатувати вразливості в системі жертви, скористатися викраденими обліковими даними для входу в систему або застосувати будь-який з інших поширених способів атаки на мережу.

Порушення цілісності даних. Хакер знаходить потрібні йому дані і починає діяти. Це може включати в себе викрадення даних для використання або продажу, знищення даних або блокування даних за допомогою програми-вимагача з вимогою викупу.

Нижче зазначені найпоширеніші кібератаки, які використовуються для витоку даних:

- Фішинг - один з розповсюджених способів, за допомогою якого хакери отримують доступ до делікатної або конфіденційної інформації. Фішинг передбачає надсилання шахрайських електронних листів, які

виглядають як листи від надійної компанії, з метою обману одержувачів, щоб вони завантажили інфіковані вкладення або перейшли за шкідливим посиланням, зазвичай з метою крадіжки конфіденційної та фінансової інформації. Переважною ціллю даної атаки є фізичні та юридичні особи

- DoS - це тип кібератаки, за допомогою якої зловмисник намагається зробити комп'ютер або мережевий ресурс недоступним для цільових користувачів, тимчасово або на невизначений час порушуючи роботу хоста, підключеного до Інтернету. Зазвичай це досягається шляхом переповнення атакованого комп'ютера або ресурсу надлишковими запитами з метою перевантажити систему і запобігти виконанню деяких або всіх допустимих запитів. Переважною ціллю даної атаки є сайти або сервіси (банки).

- Шкідливе програмне забезпечення - це термін, що окреслює будь-яку програму або код, який завдає шкоди системі. Шкідливе програмне забезпечення призначене для інфікування комп'ютера і зазвичай маскується під попередження про небезпеку шкідливих програм. Фальшиве попередження намагається переконати користувачів завантажити різні типи програмного забезпечення, і хоча воно не пошкоджує фізичне обладнання систем, воно може вкрасти, зашифрувати або викрасти певні функції комп'ютера. Шкідливе програмне забезпечення можуть проникнути на ваш комп'ютер, коли ви переходите на зламані веб-сайти, завантажуєте заражені файли або відкриваєте електронні листи з пристрою, на якому відсутній захист від шкідливого програмного забезпечення. Переважною ціллю даної атаки є фізичні та юридичні особи.

Рис. 1.2. Діаграма витоків даних в США з 2006 по 2022 роки

У 2022 році було зафіксовано 1802 випадки порушення безпеки даних у Сполучених Штатах. При цьому в тому ж році понад 422 мільйони людей постраждали від компрометації даних, включаючи витік, витік чи викриття даних. Незважаючи на те, що це три різні випадки, вони мають одну спільну рису. В результаті всіх трьох інцидентів доступ до конфіденційних даних отримує несанкціонований суб'єкт [4].

У деяких галузях відбувається більше витоків інформації, ніж в інших. Це залежить від типу та обсягу персональних даних, які зберігають організації. Охорона здоров'я, фінансові послуги та виробництво були трьома галузями, на які припала найбільше витоків на території США в 2022 році. Протягом кількох останніх років число витоків даних у сфері охорони здоров'я постійно зростало. Щодо банківського сектору, то в 2020-2022 роках рівень компрометації даних виріс майже вдвічі, тоді як у сфері виробництва зафіксовано зростання кількості інцидентів, пов'язаних з порушенням безпеки даних, більш ніж утричі [4].

В 2020 році з стрімінгового сервісу для дорослих “CAM4” відбувся злив майже 11 мільярдів записів. На сьогоднішній день це вважається наймасштабнішим витоком даних, про який стало відомо. Другим за обсягом витоком даних є витік даних компанії Yahoo, який відбувся ще у 2013 році. Компанія заявила про один мільярд витоків даних, однак пізніше, у 2017 році, повідомила про три мільярди даних. В березні 2018 року стався третій за розміром витік даних, який зачепив індійську національну ідентифікаційну базу даних Aadhaar. Наслідком інциденту стало витік понад 1,1 мільярда записів [4].

1.4. Атака на мережі, види і захист від них

Кібератака – це зловмисна та навмисна спроба особи чи організації зламати інформаційну систему іншої особи чи організації. Зазвичай зловмисник шукає певної вигоди від порушення роботи мережі жертви.

Мережеві атаки, спрямовані в першу чергу на вразливі місця в периметрі вашої мережі, після чого вони поширюються на інші частини мережі, можна поділити на два типи: активні та пасивні.

- Активні мережеві атаки спрямовані на здобуття доступу до вашої мережі, щоб змінити, зашифрувати, пошкодити або стерти ваші дані. Таким чином, метою цього типу атак є завдання шкоди вашим даним.

- Пасивні мережеві атаки ,в свою чергу, намагаються отримати доступ до вашої мережі непомітно, не викликаючи тривоги. У результаті зловмисники не вносять жодних змін до ваших даних і намагаються не виказати своєї присутності у вашій мережі. Це робиться для того, щоб ви не знали, що вони проникли у вашу мережу. Вони можуть продовжувати отримувати доступ до вашої мережі та цифрових активів до тих пір, поки їх не вичистять.

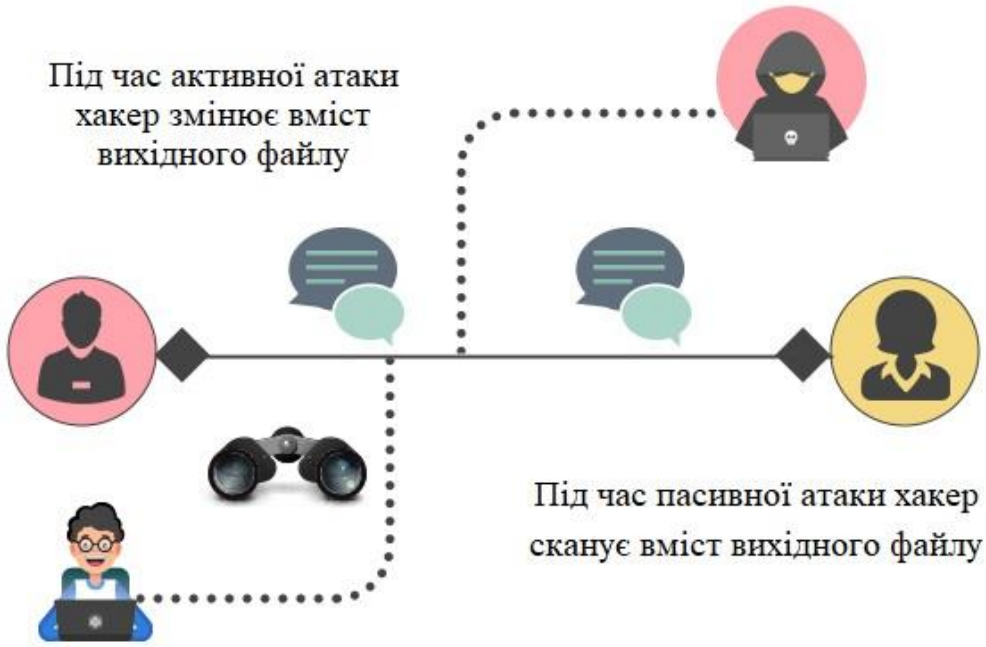

Рис. 1.3. Схема активних та пасивних атак

Незважаючи на тип атаки, якщо ваша команда не встигне помітити, що мережу атакують, вашим даним може бути завдано суттєвої шкоди. Наслідки можуть бути ще гіршими, якщо зловмисники зможуть використати інші напрямки загроз, такі як шкідливе програмне забезпечення, програми-вимагачі та вразливості в програмному забезпеченні, отримавши доступ до вашої мережі.

Типи атак спрямовані на мережеву безпеку

Шкідливе програмне забезпечення - це найшвидший тип шкідливого програмного забезпечення, яке хакер розробляє спеціально для себе, щоб вивести з ладу і пошкодити системи та мережі систем, а також здобути санкціонований доступ до особистої інформації. Шкідливе програмне забезпечення автоматично завантажується через Інтернет і швидко заражає всі підключені до мережі комп'ютери.

Вірус - це також шкідливе програмне забезпечення, але для того, щоб завдати шкоди системі, необхідна участь користувача. Вірус не може розмножуватися сам по собі; він потребує втручання людини за рахунок використання шкідливих посилань, наприклад, вкладень в електронних листах, які містять шкідливий код.

Ваші файли можуть бути зіпсованими, коли ви перейдете за шкідливими посиланнями, а ваша особиста інформація буде викрадена.

Найпоширенішою самостійною комп'ютерною шкідливою програмою є черв'як, який самовідтворюється без участі людини і поширюється мережею від однієї зараженої машини до іншої, використовуючи недоліки системи та передаючи "корисне навантаження", яке завдає шкоди комп'ютерам, на яких він перебуває. Хробакам не потрібен файл хоста для початку роботи; вони використовують той самий хост, що і система, в якій вони перебувають, і кількість хробаків зростає з часом. Черв'як проникає в систему через додаток і використовує його обчислювальну потужність, що призводить до того, що система не реагує на дії зловмисника.

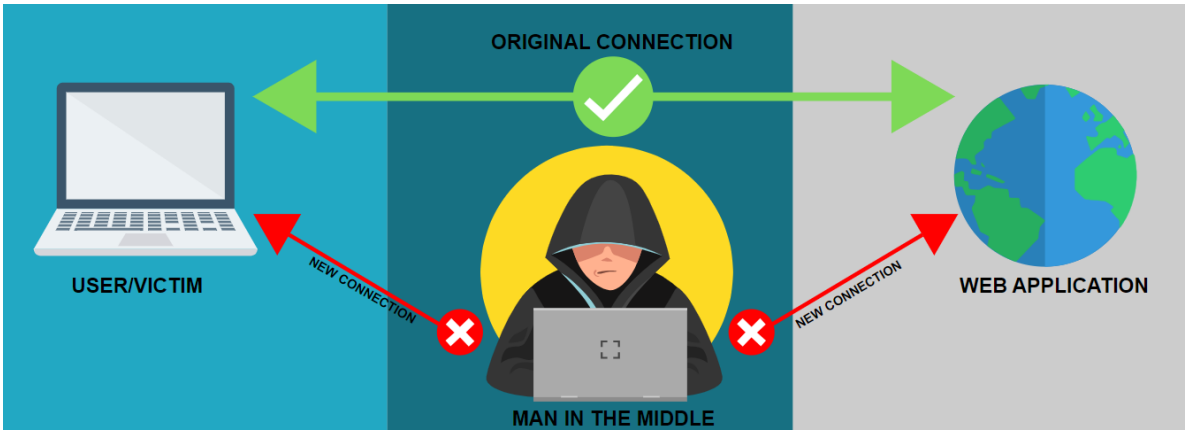

Рис. 1.4. Схема атаки “людина посередині”

Атаки типу"людина посередині" (MITM), також відомі як атаки підслуховування, виникають, коли зловмисники входять у двосторонню транзакцію. Як тільки зловмисники переривають трафік, вони можуть фільтрувати та викрадати дані. У незахищених публічних Wi-Fi зловмисники можуть вставитися між пристроєм відвідувача та мережею. Сам того не знаючи, відвідувач передає всю інформацію через зловмисника або після того, як зловмисне програмне забезпечення зламало пристрій, хакер може встановити програмне забезпечення для обробки всієї інформації жертви.

Атака з використанням мови структурованих запитів (SQL) відбувається на веб-сайти, що керуються базами даних, коли хакер маніпулює стандартним SQL-запитом. Вона здійснюється шляхом введення шкідливого коду у вразливий пошуковий рядок веб-сайту, що змушує сервер розкривати важливу інформацію. Це призводить до того, що зловмисник отримує можливість переглядати, редагувати та видаляти таблиці в базах даних. Зловмисники також можуть отримати права адміністратора.

Фішинг - це атака, яка виконується за допомогою метода соціальної інженерії. Хакер намагається обдурити жертву, погрожуючи, залякуючи або спокушаючи її. Зловмисники надсилають користувачам поштою шкідливі вкладення та посилання, видаючи себе за надійні джерела. Коли користувачі зацікавлено відкривають електронні листи, вони надають доступ до своєї системи, а в свою чергу і дані шахраям.

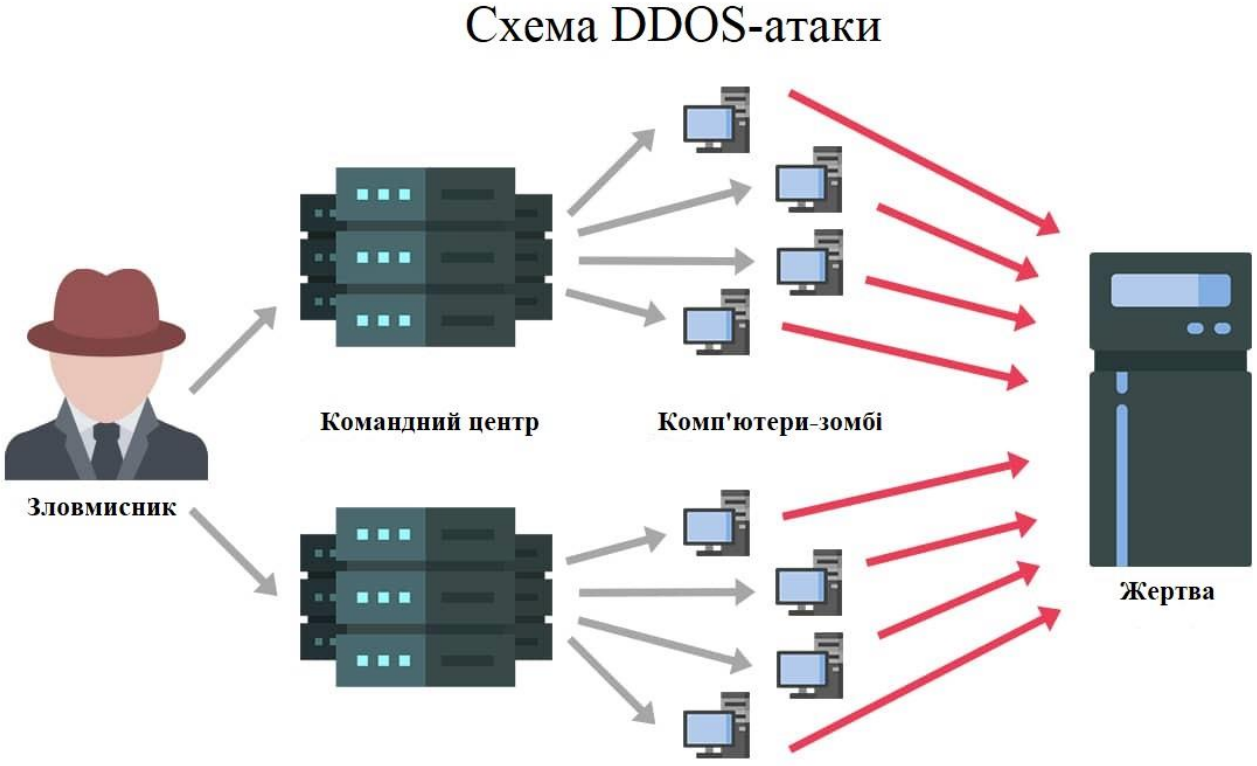

Рис. 1.5. Схема DDOS-атаки

DDoS (Distributed Denial of Service) є більш складним типом DoS-атаки. У такій атаці нападник використовує численні системи для засипання сервера жертви трафіком, що призводить до збоїв у роботі сервера або мережі, а жертва не може отримати до нього доступ.

Ботнет – це мережа пристроїв, заражених шкідливим програмним забезпеченням, наприклад вірусом. Зловмисники можуть керувати ботнетом як групою без відома власника з метою збільшення масштабу своїх атак. Часто ботнет використовується для перевантаження систем під час атаки розподіленої відмови в обслуговуванні (DDoS).

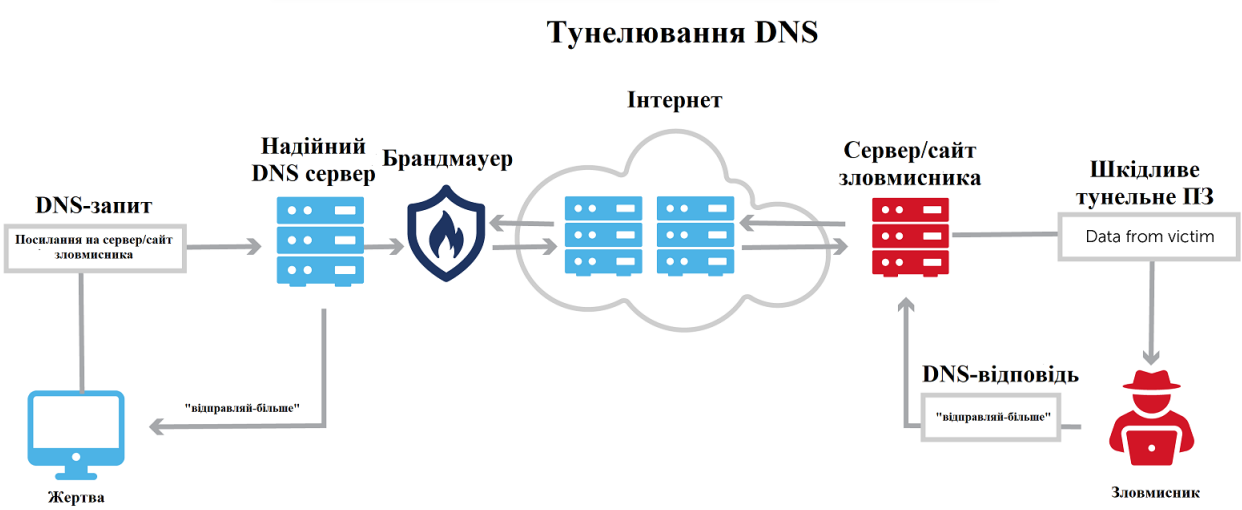

Рис. 1.6. Схема атаки “Тунелювання DNS”

Тунелювання DNS використовує протокол DNS для передачі трафіку, не пов’язаного з DNS, через порт 53. Він надсилає трафік HTTP та інших протоколів через DNS. Існують різні законні причини для використання DNS-тунелювання. Однак існують також зловмисні причини для використання VPN-служб DNS-тунелювання. Їх можна використовувати для маскування вихідного трафіку під DNS, приховуючи дані, які зазвичай передаються через Інтернет-з’єднання. Для зловмисного використання DNS-запити маніпулюють для викрадання даних із скомпрометованої системи в інфраструктуру зловмисника. Його також можна використовувати для зворотних викликів команд і керування з інфраструктури зловмисника до скомпрометованої системи.

Трояни - це небезпечна програма, яка здається безневинною через свій нешкідливий вигляд, але вона завдає серйозної шкоди, коли встановлюється та завантажується на комп'ютер. Це шкідлива програма, яка може змінювати налаштування комп'ютера та виконувати незвичні завдання, наприклад, видаляти таблиці розподілу файлів і викликати зависання машини. В основному він вбудовується в піратське програмне забезпечення, ігри та розповсюджується за допомогою методів соціальної інженерії, наприклад, через електронну пошту. Трояни можуть дати хакеру доступ до персональної інформації, такої як фінансові дані, імена користувачів, паролі тощо.

Перехоплювачі пакетів (сніффери) перехоплюють або зберігають копії кожного переданого пакета, коли пакети проходять через мережу в зоні бездротової передачі. Сніффер - це інструмент, який зловмисники використовують для збору приватної інформації, такої як соціальна інформація, фінансові дані, секрети виробництва, логіни користувачів та паролі.

Одним з найефективніших способів запобігати загрозам в мережевій безпеці є розподіл мережі на декілька частин згідно до вимог її безпеки. Цього можна досягти, зробивши підмережі в межах мережі чи створивши віртуальну локальну мережу (VLAN), котра буде виконуватиме функції самостійної мережі. Даний метод дозволяє обмежити можливий наслідок атаки однією зоною та змушує порушників вживати додаткових зусиль, щоб проникнути до інших зон мережі для отримання бажаного результату.

Забороняйте користувачам мережі мати вільний доступ до Інтернету. Всі Інтернет-запити повинні проходити через прозорий проксі-сервер, який дозволяє контролювати та керувати діями користувачів. Впевніться, що вихідні з’єднання насправді здійснює людина, а не бот. Наявність "білого списку" дозволених сайтів дасть змогу користувачам отримувати доступ лише до перевірених доменів та допоможе уникнути несанкціонованого доступу.

Встановлюйте брандмауери на кожному перетині між мережевими зонами, а не лише на межі мережі. Коли розгортання повноцінних брандмауерів неможливе, скористайтеся вбудованими функціями брандмауерів у комутаторах і

маршрутизаторах. Додатково, для захисту важливо мати пристрої від DDoS-атак або хмарні сервіси на краю мережі. Продумайте розміщення критично важливих пристроїв, як-от балансувальників навантаження - якщо їх розмістити за межами демілітаризованої зони (DMZ), вони не будуть захищені пристроями мережевої безпеки.

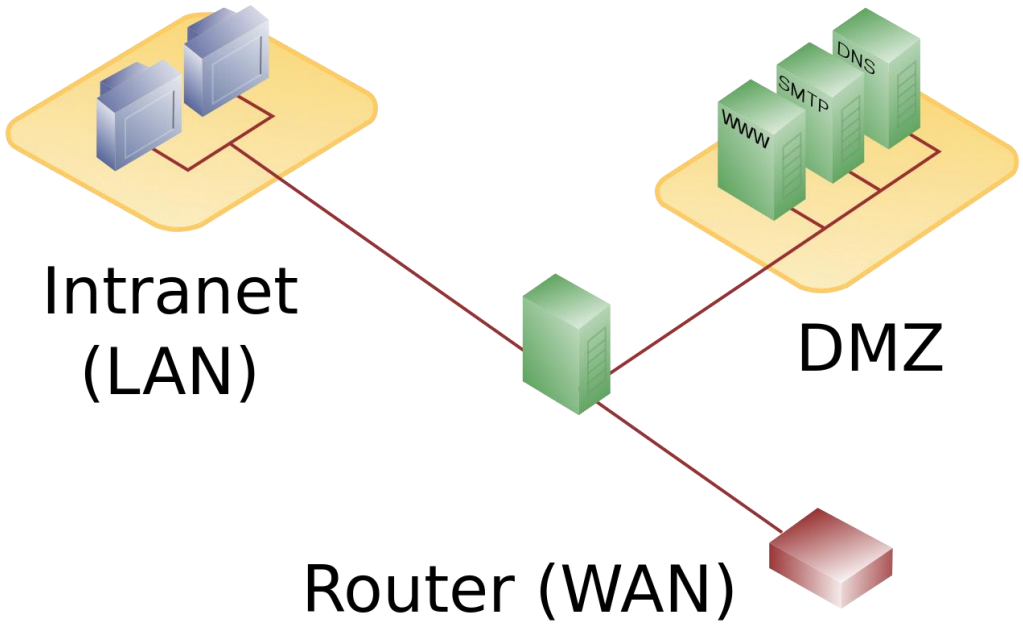

Рис. 1.7. Схема з одним міжмережевим екраном

Використання трансляції мережевих адрес (NAT) забезпечить додатковий рівень безпеки. NAT дозволяє перетворити внутрішні IP-адреси в загальнодоступні мережеві адреси, даючи змогу підключити кілька комп'ютерів до Інтернету за допомогою однієї IP-адреси. Завдяки NAT вхідний або вихідний трафік повинен проходити через пристрій NAT, що значно ускладнює зловмисникам ідентифікацію конкретних хостів.

Гарантуйте собі повну видимість вхідного, вихідного та внутрішнього мережевого трафіку з можливістю автоматичного виявлення загроз, а також розуміння їхнього контексту та впливу. Поєднуючи дані з різних засобів захисту, можна отримати чітку картину мережевої активності, розуміючи, що атаки часто спрямовані на велику кількість систем, облікових записів користувачів

1.5. Політика безпеки мереж і її забезпечення

Без політики безпеки доступність вашої мережі може бути порушена. Політика починається з оцінки ризику для мережі та створення команди для реагування. Продовження політики вимагає впровадження практики керування змінами безпеки та моніторингу мережі на наявність порушень безпеки. Нарешті, процес перегляду змінює існуючу політику та адаптує її до отриманих уроків.

Даний документ можна розділити на три напрямки: підготовка, запобігання та реагування. Розглянемо кожен із цих кроків детальніше.

Перш ніж запровадити політику безпеки, ви повинні зробити наступне:

- Створення заяв про політику використання.
- Проведіть аналіз ризиків.
- Створіть структуру групи безпеки.

Рекомендовано створювати заявки про політику використання, які окреслюють ролі та обов’язки користувачів щодо безпеки. Ви можете почати із загальної політики, яка охоплює всі мережеві системи та дані у вашій компанії. Цей документ має надати широкій спільноті користувачів розуміння політики безпеки, її мети, вказівок щодо покращення їх практик безпеки та визначення їхніх обов’язків щодо безпеки. Якщо ваша компанія визначила конкретні дії, які можуть призвести до покарання або дисциплінарного впливу на працівника, ці дії та те, як їх уникнути, мають бути чітко сформульовані в цьому документі.

Наступним кроком є створення заяви про прийнятне використання для партнерів, щоб надати партнерам розуміння інформації, яка їм доступна, очікуваного використання цієї інформації, а також поведінки працівників вашої компанії. Ви повинні чітко пояснити будь-які конкретні дії, які були визначені як атаки на безпеку, і покарання, які будуть вжиті у разі виявлення атаки на безпеку.

Нарешті, створіть заяву про прийнятне використання для адміністратора, щоб пояснити процедури адміністрування облікових записів користувачів, застосування політики та перевірки привілеїв. Якщо ваша компанія має конкретну політику щодо паролів користувачів або подальшої обробки даних, також чітко представте цю

політику. Щоб забезпечити однаковість, перевірте політику на відповідність заявам про прийнятне використання партнером і політику прийнятного використання користувачами. Переконайтеся, що вимоги адміністратора, перелічені в політиці прийнятного використання, відображені в планах навчання та оцінці ефективності.

Аналіз ризиків має визначити ризики для вашої мережі, мережевих ресурсів і даних. Це не означає, що ви повинні визначити кожну можливу точку входу в мережу або всі можливі засоби атаки. Метою аналізу ризиків є ідентифікація частин вашої мережі, присвоєння рейтингу загрози кожній частині та застосування належного рівня безпеки. Це допомагає підтримувати працездатний баланс між безпекою та необхідним доступом до мережі.

Призначте кожному мережевому ресурсу один із трьох таких рівнів ризику:

- Системи з низьким рівнем ризику або дані, які в разі зламу (перегляд даних неавторизованим персоналом, пошкодження даних або втрата даних) не порушують бізнес і не спричинять юридичних чи фінансових наслідків. Цільову систему або дані можна легко відновити й не допускати подальшого доступу інших систем.
- Системи середнього ризику або дані, які в разі зламу (дані переглянуті неавторизованим персоналом, дані пошкоджені або втрачені) спричинять помірні збої в бізнесі, незначні юридичні чи фінансові наслідки або нададуть подальший доступ до інших систем. Цільова система або дані потребують помірних зусиль для відновлення або процес відновлення руйнує систему.
- Системи високого ризику або дані, які в разі зламу (перегляд даних неавторизованим персоналом, пошкодження даних або втрата даних) спричинять серйозні збої в бізнесі, спричинять серйозні правові чи фінансові наслідки або загрожуватимуть здоров’ю та безпеці людини. Цільова система або дані потребують значних зусиль для відновлення або процес відновлення заважає бізнесу чи іншим системи.

Призначте рівень ризику кожному з наступного: пристрої базової мережі, пристрої розподільної мережі, пристрої мережі доступу, пристрої моніторингу

мережі (монітори SNMP і зонди RMON), пристрої безпеки мережі (RADIUS і TACACS), системи електронної пошти, мережеві файлові сервери , сервери мережевого друку, сервери мережевих програм (DNS і DHCP), сервери програм даних, настільні комп’ютери та інші пристрої

Мережеве обладнання, таке як комутатори, маршрутизатори, DNS-сервери та DHCP-сервери, може дозволити подальший доступ до мережі, і тому є пристроями середнього або високого ризику. Також можливо, що пошкодження цього обладнання може призвести до збою самої мережі. Такий збій може бути дуже руйнівним для бізнесу.

1.6. Класифікація вторгнень

Вторгнення в мережу – це будь-яка несанкціонована діяльність у комп'ютерній мережі. Виявлення вторгнення залежить від захисників, які чітко розуміють, як працюють напади. У більшості випадків така небажана діяльність поглинає мережеві ресурси, призначені для інших застосувань, і майже завжди загрожує безпеці мережі або її даних.

Демонструю свою варіацію класифікації вторгнень:

- за умовами атаки:

Зовнішні атаки походять ззовні системи або мережі, на яку спрямована атака.

Внутрішні атаки ініціюються особами, які мають санкціонований доступ до системи або мережі, на яку спрямована атака.

Фізичні атаки передбачають прямий фізичний доступ до апаратного забезпечення або інфраструктури системи, на яку спрямована атака.

- за характером впливу:

Атаки на доступність спрямовані на порушення або відмову в доступі до системи або мережі, роблячи її недоступною для законних користувачів.

Атаки на цілісність спрямовані на модифікацію або зміну даних у системі чи мережі, що ставить під загрозу її цілісність.

Атаки на конфіденційність спрямовані на отримання несанкціонованого доступу до важливої або конфіденційної інформації, що зберігається в системі або мережі, на яку спрямована атака.

Рис. 1.8. Класифікація втогнень

- за метою атаки:

Фінансова вигода. Атаки мотивовані грошовою вигодою, наприклад, крадіжкою фінансової інформації або проведенням шахрайських транзакцій.

Політичні мотиви. Атаки, зумовлені політичними мотивами або ідеологією, які спрямовані на виведення з ладу або отримання контролю над критично важливими системами.

Шпигунство. Атаки, пов'язані з викраденням конфіденційної інформації, комерційної таємниці або інтелектуальної власності з метою отримання конкурентних або стратегічних переваг.

Вандалізм. Атаки здійснюються з наміром завдати шкоди, порушити роботу або знищити об'єкт без конкретної вигоди.

- за наявністю зворотного зв'язку:

Активні атаки полягають у безпосередній співпраці з цільовою системою або мережею, активно змінюючи або порушуючи її роботу.

Пасивні атаки зосередженні на прослуховуванні або перехопленні даних без зміни або впливу на систему, що атакується.

- за місцем розташування зловмисника:

Локальні атаки відбуваються з тієї ж локальної мережі або з фізичної близькості до системи чи мережі, на яку спрямована атака.

Віддалені атаки запускаються з іншого місця, як правило, через Інтернет, і націлені на віддалені системи або мережі.

1.7. Зразок політики корпоративної безпеки

Політика безпеки включає набір цілей для компанії, правила поведінки для користувачів та адміністраторів та вимоги до системи та управління, які спільно забезпечують безпеку мережевих та комп'ютерних систем в організації. Політика безпеки - це "живий документ", що означає, що документ ніколи не закінчується і постійно оновлюється в міру зміни технологій та вимог працівників.

Політика безпеки перекладає, роз'яснює та передає керівну позицію щодо безпеки, визначеної у принципах безпеки високого рівня. Політика безпеки діє як міст між цими цілями управління та конкретними вимогами безпеки. Він інформує користувачів, персоналу та менеджерів про їх обов'язкові вимоги щодо захисту технологій та інформаційних активів. Він повинен вказати механізми, які вам потрібно для задоволення цим вимогам. Він також забезпечує базову лінію, з якої можна придбати, налаштувати та аудит комп'ютерних систем та мереж для дотримання політики безпеки. Тому спроба використовувати набір інструментів безпеки за відсутності принаймні політичної політики безпеки безглуздо.

Зразок політики корпоративної безпеки:

Користувачам дозволяється використовувати лише ті мережеві адреси, призначені їм ІТ-відділом компанії.

Весь віддалений доступ до компанії буде через безпечне з'єднання VPN на пристрої, що належить компанії, який має сучасне антивірусне програмне забезпечення, або на затверджених мобільних пристроях.

Віддалені користувачі можуть підключатися до інформаційних систем компанії, використовуючи лише протоколи, затверджені ним. Користувачі всередині брандмауера компанії не можуть бути підключені до мережі компанії одночасно, для зовнішньої мережі використовується віддалене з'єднання.

Користувачі будь-яким чином не повинні розширювати або повторювати мережеві послуги. Це означає, що користувач не повинен встановлювати маршрутизатор, перемикач, центр або бездротову точку доступу до мережі компанії без затвердження компанії.

Користувачі не повинні встановлювати мережеве обладнання або програмне забезпечення, яке надає мережеві послуги без затвердження IT. Стороні комп'ютерні системи, які потребують підключення до мережі, повинні бути затверджені компанією IT.

Користувачі не повинні завантажувати, встановлювати або запускати програми безпеки або утиліти, які виявляють слабкі місця в безпеці системи. Наприклад, користувачі компанії не повинні запускати програми злому паролів, сніфферів пакетів, інструменти для відображення мережі або сканери портів під час будь-якого способу до мережевої інфраструктури компанії. Тільки IT-відділу дозволяється виконувати ці дії.

ВИСНОВКИ ДО РОЗДІЛУ 1

В першому розділі були розглянуті основні аспекти забезпечення безпеки мережі, з'ясовано що безпека мережі повинна поєднувати в собі кілька шарів захисних сил на кінцевих пристроях та в самій мережі. Кожен мережевий рівень безпеки реалізує політику та управління. Задача фахівці з кібербезпеки постійно захищати комп'ютерні системи від різних типів загроз. Загрози можуть походити від різних суб'єктів, включаючи корпоративних шпигунів, хакерів, терористичних груп,

ворожих національних держав, злочинних організацій та інших.

У більшості випадків така небажана діяльність поглинає мережеві ресурси, призначені для інших застосувань, і майже завжди загрожує безпеці мережі або її даних. Правильне проєктування та розгортання мережевої системи виявлення вторгнень допоможе блокувати зловмисників.

Політика безпеки мережі — це набір стандартизованих практик і процедур, які окреслюють правила доступу до мережі, архітектуру мережі та середовища безпеки, а також визначають, як політики застосовуються. Політика безпеки включає набір цілей для компанії, правила поведінки для користувачів та адміністраторів та вимоги до системи та управління, які спільно забезпечують безпеку мережевих та комп'ютерних систем в організації. Використання набору інструментів безпеки за відсутності принаймні політичної політики безпеки не є доцільним.

РОЗДІЛ 2
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА АПАРАТНІ ЗАСОБИ БРАНДМАУЕРІВ CISCO PIX

2.1. Міжмережевий екран Cisco Secure Private Internet Exchange Firewall

Правильно налаштований брандмауер PIX (Private Internet Exchange) допомагає запобігти неавторизованим підключенням однієї мережі до іншої. Мережа, яку захищає брандмауер PIX, називається внутрішньою мережею, а мережа, з якої контролюються підключення зовнішньою мережею. Брандмауер PIX додатково підтримує кілька зовнішніх мереж, які можна позначити як мережі периметра або демілітаризовані зони (DMZ). Підключенням між периметром, зовнішньою та внутрішньою мережами можна керувати брандмауером PIX.

Для ефективного використання брандмауера в організації необхідно розробити політику безпеки, що гарантуватиме, що весь трафік, що прямує зсередини назовні, буде проходити через брандмауер. Крім того, важливо визначити, хто має право отримувати доступ до мережевих ресурсів, які служби можна ефективно підтримувати, а також хто може мати доступ до внутрішньої та периметральної мережі ззовні.

На рис. 2.1 показано, як брандмауер PIX захищає мережу, надаючи вихідним з’єднанням безпечний доступ до Інтернету.

У цій архітектурі брандмауер PIX утворює межу між внутрішньою мережею та зовнішніми мережами. Весь трафік між внутрішньою та зовнішньою мережами має проходити через брандмауер для підтримки безпеки. Зовнішня мережа зазвичай доступна через Інтернет і містить системи, які надають послуги зовнішній мережі. Такі послуги можуть включати веб-сервер, FTP-сервер або сервер SMTP. Підключення до цих серверів, додатків можна контролювати за допомогою списків доступу в підключеному до Інтернету маршрутизаторі.

Рис. 2.1. Брандмауер PIX у мережі

Крім того, серверні системи можуть бути розташовані на периметрі мережі, як показано вище, а доступ до серверних систем можна контролювати та контролювати за допомогою брандмауера PIX. Брандмауер PIX також дозволяє запровадити ваші політики безпеки для підключення до внутрішньої мережі та з неї.

Зазвичай, внутрішня мережа – це власна внутрішня мережа організації, або інтранет, а зовнішня мережа – це Інтернет, але брандмауер PIX також можна використовувати в інтрамережі для ізоляції або захисту однієї групи внутрішніх обчислювальних систем і користувачів від іншої.

Мережа периметра може бути налаштована так само безпечно, як і внутрішня мережа, або з різними рівнями безпеки від найбільш безпечної внутрішньої мережі до найменш безпечної зовнішньої мережі. Периметральна та внутрішня мережі захищені алгоритмом адаптивної безпеки брандмауера PIX. Внутрішній, периметральний і зовнішній інтерфейси можуть дізнаватись про оновлення маршрутизації RIP, а внутрішній і периметральний інтерфейси можуть транслювати маршрут RIP за замовчуванням.

Коли вихідні пакети надходять до внутрішнього інтерфейсу брандмауера PIX, брандмауер PIX перевіряє, чи надійшли попередні пакети з внутрішнього хосту. Якщо ні, брандмауер PIX створює слот перекладу (також званий "xlate") у своїй таблиці стану для нового підключення. Слот містить внутрішню IP-адресу та

глобально унікальну IP-адресу, призначену трансляцією мережевих адрес (NAT), трансляцією адрес порту (PAT) або ідентифікацією (яка використовує внутрішню адресу як зовнішню). Потім брандмауер PIX змінює IP-адресу джерела пакета на глобально унікальну адресу, змінює контрольну суму та інші поля за потреби та пересилає пакет до відповідного зовнішнього інтерфейсу.

Коли вхідний пакет надходить до зовнішнього інтерфейсу, він спочатку повинен пройти критерії адаптивної безпеки брандмауера PIX. Якщо пакет проходить перевірку безпеки, брандмауер PIX видаляє IP-адресу призначення, а внутрішню IP-адресу вставляє на її місце. Пакет пересилається на внутрішній інтерфейс.

Слоти динамічної передачі корисні для настільних машин, яким не потрібні постійні адреси в Інтернеті. Внутрішні мережеві хости з IP-адресами, не зареєстрованими в NIC (Network Information Center), можуть отримати прямий доступ до Інтернету за допомогою стандартного програмного забезпечення TCP/IP на робочому столі, увімкнувши трансляцію адрес у брандмауері PIX. Ніякого спеціального клієнтського програмного забезпечення не потрібно. Брандмауер PIX підтримує трансляцію мережевих адрес (NAT), яка надає глобально унікальну адресу для кожного внутрішнього хоста, і трансляцію адреси порту (PAT), яка спільно використовує одну глобально унікальну адресу для багатьох внутрішніх хостів. Адреси NAT і PAT беруться з віртуальної мережі до 64K адрес хостів, налаштованих у брандмауері PIX.

Іншим класом трансляції адрес на брандмауері PIX є статична трансляція. Статичний переклад ефективно переміщує внутрішній незареєстрований хост у віртуальну мережу в брандмауері PIX. Це корисно для внутрішніх машин, до яких потрібно звертатися із зовнішніх шлюзів Інтернету; наприклад, сервер SMTP.

Після базової конфігурації брандмауер PIX дозволяє всі вихідні з’єднання з внутрішньої мережі до зовнішньої мережі та відхиляє будь-які вхідні з’єднання із зовнішньої мережі. Цю політику за замовчуванням можна змінити відповідно до вимог політики вашої організації.

Брандмауер PIX відокремлює деталі впровадження політики безпеки від

надання мережевих послуг, таких як Web, FTP, Telnet і SMTP.

Це забезпечує:

- Набагато краща масштабованість і продуктивність — брандмауер PIX призначений для виконання ролі безпеки та не потребує значних накладних витрат, необхідних для підключення до сервера.
- Підвищена безпека — якщо не налаштовано так, брандмауер PIX не приймає підключення із зовнішньої мережі (приватне посилання є винятком із цього) і реалізується за допомогою власної вбудованої системи, а не повної операційної системи, необхідної для підтримки серверних програм.
- Знижена складність — кожен пристрій виконує певну функцію.

Щоб ефективно використовувати брандмауер у вашій організації, вам потрібна політика безпеки для захисту ресурсів даних від вторгнення. Створивши або вдосконаливши політику безпеки, ви можете захистити себе від зловмисних атак сторонніх осіб і контролювати наслідки помилок і збоїв обладнання.

Ваша політика безпеки має гарантувати, що користувачі можуть виконувати лише ті завдання, на виконання яких вони мають повноваження, лише отримувати інформацію, яку вони мають, і не завдавати шкоди даним, програмам або операційному середовищу системи.

Перш ніж створювати будь-яку політику безпеки, скористайтеся цими вказівками:

Крок 1. Намалюйте карту вашої повної мережі, вказавши, які системи підключаються до Інтернету, які є серверами, і визначте, які IP-адреси є в кожній підмережі. Коли ваша карта буде готова, поширте її відповідним мережевим адміністраторам, регулярно оновлюйте її та отримайте паперові копії для вирішення проблем.

Крок 2. Визначте, які системи потрібно захистити від доступу до Інтернету, а які мають бути видимими у зовнішній мережі, наприклад IP-адреси, зареєстровані в мережевому адаптері.

Функція трансляції мережевих адрес (NAT) брандмауера PIX дозволяє

вказати, що IP-адреси, зареєстровані в мережевому адаптері, видимі зовні брандмауера або що IP-адреси внутрішньої мережі залежать виключно від глобального пулу для трансляції.

Крок 3. Визначте, які внутрішні сервери мають бути видимими в зовнішніх і периметральних мережах, а також який тип автентифікації та авторизації вам потрібні, щоб користувачі могли отримати доступ до серверів.

Крок 4. Визначте, які функції маршрутизатора вам потрібно буде налаштувати для розміщення брандмауера PIX у вашій мережі.

За правильного налаштування брандмауер PIX може захистити вашу мережу від зовнішніх загроз. Брандмауер PIX не є системою «під ключ». Ви повинні запрограмувати його, щоб визначити, які хости можуть отримати доступ до вашої внутрішньої мережі, а які ні.

IP-адреса хоста або мережі, яка може отримати доступ до консолі Telnet брандмауера PIX. Якщо ім’я інтерфейсу не вказано, припускається, що адреса знаходиться на внутрішньому інтерфейсі. Брандмауер PIX автоматично перевіряє IP-адресу на відповідність IP-адресам, указаним у командах ip-адреси, щоб переконатися, що вказана вами адреса знаходиться у внутрішньому інтерфейсі. Якщо вказано ім’я інтерфейсу, брандмауер PIX перевіряє хост лише на вказаний вами інтерфейс.

Брандмауер PIX не може захистити вашу мережу від внутрішніх зловмисників. Щоб належним чином захиститися від цих загроз, усім особам, які мають доступ до внутрішньої мережі, слід надати лише найменші привілеї та доступ, необхідні для виконання їхньої роботи.

Cisco PIX Firewall забезпечує повний захист брандмауером, який повністю приховує архітектуру внутрішньої мережі від зовнішнього світу. Брандмауер PIX забезпечує безпечний доступ до Інтернету з наявних приватних мереж і можливість розширення та переналаштування мереж TCP/IP, не переймаючись проблемою нестачі IP-адрес..

Функції брандмауера PIX, описані в таблиці 2.1.

Таблиця 2.1

Функції брандмауера PIX

Функція	Опис	Переваги	Вплив на безпеку
Адаптивний алгоритм безпеки (ASA)	Реалізує контроль за станом підключення через брандмауер	Дозволяє одностороннє (зсередини назовні) підключення без явної конфігурації для кожної внутрішньої системи та програми	Завжди в роботі відстежує повернення пакетів, щоб переконатися, що вони дійсні
Перетворення мережевої адреси (NAT)	Для внутрішніх систем перекладає вихідну IP-адресу вихідних пакетів на RFC 1631	Дозволяє присвоювати приватні адреси всередині (визначених у RFC 1918) або зберігати існуючі недійсні адреси	Приховує реальну мережеву ідентичність внутрішніх систем із зовнішньої мережі
Переклад адреси порту (PAT)	Використовуючи переробку порту, одна дійсна IP -адреса може підтримувати джерело	PAT мінімізує кількість глобально дійсних IP - адрес, необхідних для підтримки приватних або недійсних схем внутрішньої адресації.	Приховує реальну мережеву ідентичність внутрішніх систем із зовнішньої мережі
Кілька інтерфейсів	До брандмауера PIX можна додати додаткові мережеві інтерфейси.	Займає місце декількох брандмауерів PIX в одному шасі.	Забезпечує адаптивну безпеку для периметрових інтерфейсів.

Закінчення таблиці 2.1

Ідентифікація	Дозволяє відключити переклад адреси.	Функція ідентичності дозволяє NAT та PAT вибірково відключити для цих систем.	Робить внутрішні мережеві адреси видимими для зовнішньої мережі.
Захист від флуду	Захищає внутрішні системи від атак TCP SYN flood	Дозволяє захищати сервери у внутрішній мережі від атаки типу «відмова в обслуговуванні»	Захищає внутрішні системи від атак SYN
Сервер конфігурації TFTP	Забезпечує налаштування брандмауера PIX через TFTP	Дозволяє одному чи кільком брандмауерам отримати доступ до конфігурацій із центрального джерела	Невпевнений. Не використовуйте, якщо ваша політика безпеки забороняє обмін привілейованою інформацією у вигляді відкритого тексту

2.2. Типи брандмауерів

Брандмауери можна відрізнити різними способами: від розміру мережі, яку вони розроблені для роботи, до того, як вони забезпечують захист. У цій главі розглядається основна систематика брандмауерів та використовує конвенцію класифікації брандмауерів на основі "розміру" особистих або настільних брандмауерів, брандмауерів невеликого офісу/домашнього офісу (SOHO) та брандмауерів підприємства. Крім того, у цій главі обговорюються різні способи, як брандмауери захищають мережі, в яких вони розміщуються, від простих фільтрів пакетів до державних фільтрів пакетів до проксі-серверів. В цьому підрозділі наведено високий рівень огляду різних продуктів брандмауера компінії Cisco.

Брандмауери бувають різного розміру та призначення. Найбільш типовою ідеєю брандмауера є спеціалізована система або прилад, що сидить у мережі та сегментах "внутрішньої" мережі з "зовнішнього" Інтернету. Більшість домашніх або SoHo Networks використовують пристрій на основі приладу для широкосмугового підключення, який включає вбудований брандмауер. Загалом, брандмауери можна класифікувати за одним із двох загальних типів:

- Настільні або особисті брандмауери
- Мережеві брандмауери

Основна відмінність цих двох типів брандмауерів просто зводиться до кількість хостів, які захищає брандмауер. У межах мережевого типу брандмауера існують первинні класифікації пристроїв, включаючи наступне:

- Брандмауери-фільтрування пакетів (SPI та нестабільні)
- Шлюзи канального рівня
- Шлюзи прикладного рівня

У попередньому списку описані загальні класи брандмауерів, але, як обговорювалося пізніше, багато мережевих брандмауерів представляють гібриди попередніх класифікацій. Багато брандмауерів мають характеристики, які розміщують їх у більш ніж одній класифікації.

На рисунку 2.2 показано розбиття різних видів брандмауера.

Цей рисунок не дає повної картини можливостей у кожного типа брандмауера, а скоріше показує загальну систематику різних брандмауерів, доступних у двох первинних типах: особистих або настільних брандмауерів та мережевих брандмауерів.

Враховуючи різні типи брандмауерів, користувачам може бути важко визначитися, що саме їм потрібно. У багатьох випадках витрати є рушійним фактором придбання брандмауера, але знаючи, які типи брандмауерів доступні та які можливості вони надають, дасть змогу користувачам прийняти більш обґрунтоване остаточне рішення.

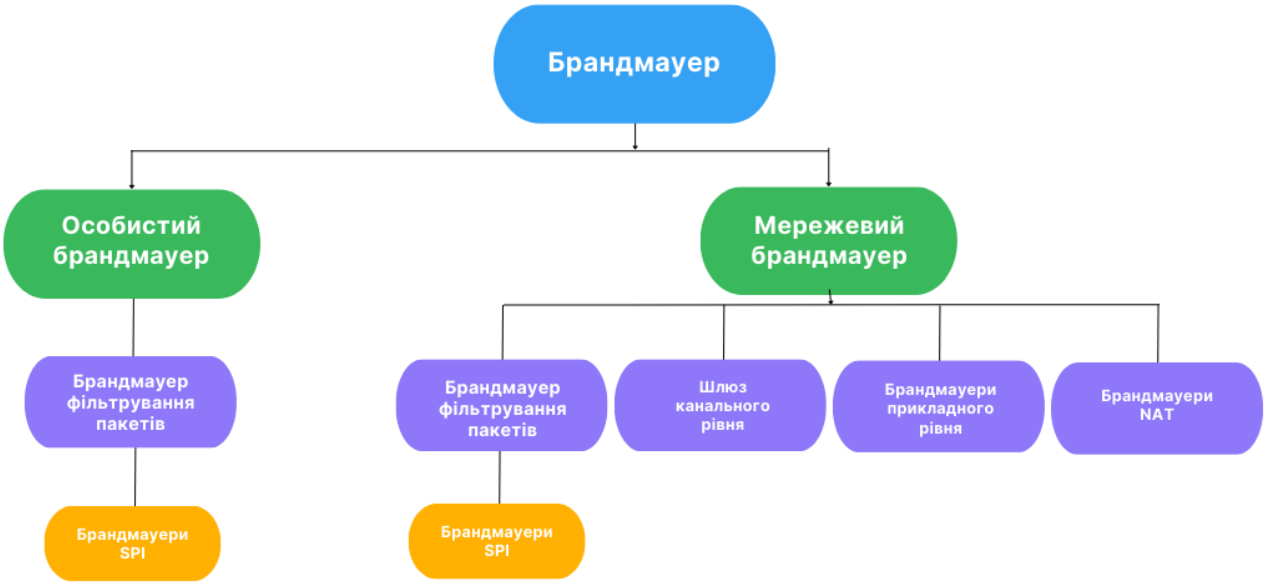

Рис. 2.2. Типи брандмауерів

Особисті брандмауери розроблені для захисту одного хоста від несанкціонованого доступу. Протягом багатьох років це розвивалося так, що сучасні особисті брандмауери зараз інтегрують додаткові можливості, такі як антивірусне моніторинг програмного забезпечення, а в деяких випадках аналіз поведінки та виявлення вторгнення для захисту пристрою.

Одним з важливих аспектів персональних брандмауерів є централізоване керування. Деякі виробники визначили, що значною перешкодою для розгортання персонального брандмауера на кожній кінцевій системі є необхідність централізованого управління, щоб політики могли розроблятися і застосовуватися віддалено до кінцевих систем, і розробили такі можливості в своїх продуктах. Великі підприємства не поспішають впроваджувати цю технологію персонального брандмауера для своїх систем через складність підтримки узгодженої політики брандмауера в масштабах всього підприємства.

Мережеві брандмауери призначені для захисту всієї мережі від атак. Мережеві брандмауери бувають двох основних форм: спеціальний пристрій або набір програмного забезпечення брандмауера, встановленого поверх операційної системи хоста. Приклади мережевих брандмауерів на основі пристроїв включають Cisco PIX, Cisco ASA, брандмауери NetScreen Juniper. До більш популярних брандмауерів на

основі програмного забезпечення належать брандмауери Check Point Firewall-1 NG або NGX.

Багато мережевих брандмауерів забезпечують корпоративним користувачам максимальну гнучкість і захист у системі брандмауерів. За останні кілька років ці брандмауери включили багато нових функцій, таких як вбудоване виявлення та запобігання вторгненням, а також можливості завершення віртуальної приватної мережі (VPN) як для мереж VPN між локальними мережами, так і для мереж VPN з віддаленим доступом користувачів.

Ще одна функція, яка була введена в мережеві брандмауери, це можливість глибокої перевірки пакетів. Брандмауер може визначати вимоги до трафіку не лише переглядаючи інформацію рівня 3 і рівня 4, але й заглиблюючись у дані програми, щоб брандмауер міг приймати рішення щодо того, як найкраще обробляти потік трафіку [5].

2.3. Логіка та види брандмауерів PIX

Брандмауери працюють на основі заздалегідь визначених правил або логіки, щоб контролювати потік мережевого трафіку між різними мережами або сегментами мережі. Основне призначення брандмауера - забезпечувати дотримання політики безпеки, перевіряючи мережеві пакети і визначаючи, чи дозволяти або блокувати їх на основі налаштованих правил. В свою чергу, серія пристроїв Cisco PIX Security Appliance забезпечує надійні інтегровані послуги мережевої безпеки корпоративного класу, включаючи міжмережеві екрани з перевіркою стану, перевірку протоколів і додатків, віртуальні приватні мережі (VPN), вбудований захист від вторгнень, а також захист мультимедійних і голосових даних - економічно ефективні і прості в розгортанні рішення. Ці інтегровані технології створюють потужний багаторівневий захист для сучасних мережевих середовищ, що постійно змінюються. Від компактних настільних брандмауерів "plug-and-play" для малих і домашніх офісів до модульних гігабітних брандмауерів операторського класу для найвимогливіших середовищ підприємств і постачальників послуг.

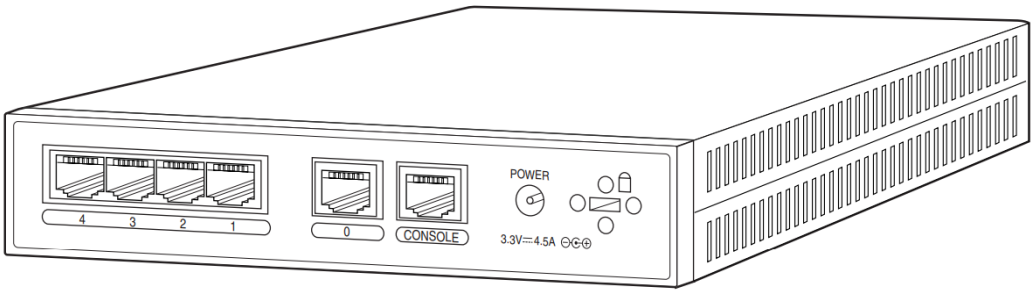

Рис. 2.3. Брандмауер Cisco PIX-501

Cisco PIX 501 Security Appliance забезпечує пропускну здатність міжмережевого екрану до 60 Мбіт/с, пропускну здатність 3DES VPN до 3 Мбіт/с і 4,5 Мбіт/с AES-128 VPN до 4,5 Мбіт/с. Інтерфейси:

Порт консолі: RS-232 (RJ-45) 9600 бод; зовні: інтегрований порт 10/100 Fast Ethernet, автоматичне узгодження (напів/повний дуплекс), RJ45; всередині: інтегрований 4-портовий комутатор 10/100 Fast Ethernet з автоматичним визначенням, авто-MDIX, RJ45.

ПРИМІТКА: 10/100 повнодуплексний з PIX OS 6.3, 10BaseT напівдуплексний з попередніми версіями. [6].

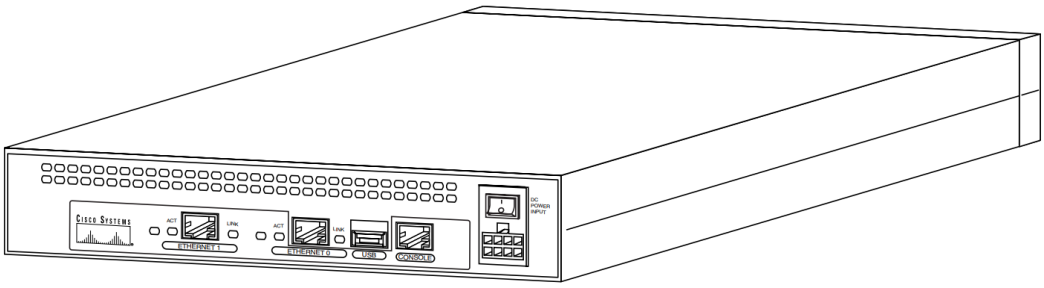

Рис. 2.4. Брандмауер Cisco PIX-506E

Пристрій безпеки Cisco PIX 506E забезпечує пропускну здатність міжмережевого екрану до 100 Мбіт/с, пропускну здатність 3DES VPN до 16 Мбіт/с і пропускну здатність AES-128 VPN до 30 Мбіт/с. Інтерфейси:

Порт консолі: RS-232 (RJ-45) 9600 бод; Зовнішній: інтегрований порт 10/100 Fast Ethernet, автоматичне узгодження (напів/повний дуплекс), RJ45; Внутрішній: інтегрований порт 10/100 Fast Ethernet, автоматичне узгодження (напів/повний дуплекс), RJ45.

ПРИМІТКА: 10/100 повнодуплексний з PIX OS 6.3, 10BaseT повнодуплексний з попередніми версіями [6].

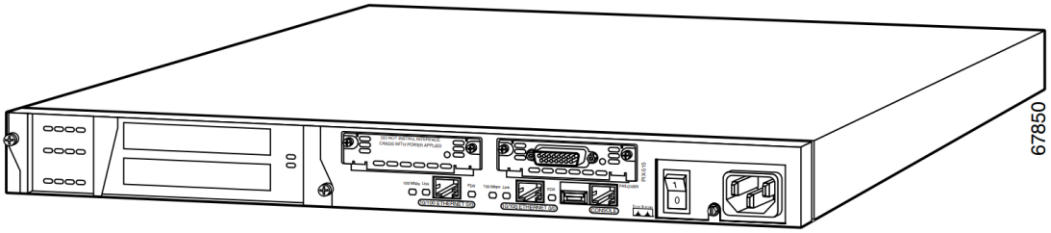

Рис. 2.5. Брандмауер Cisco PIX-515E

Пристрій безпеки Cisco PIX 515E має універсальну конструкцію в одну стійку (1RU) і підтримує до шести інтерфейсів 10/100 Fast Ethernet. Він забезпечує пропускну здатність брандмауера до 188 Мбіт/с з можливістю обробки понад 130 000 одночасних сеансів. Деякі моделі PIX 515E оснащені вбудованим апаратним прискоренням VPN, що забезпечує пропускну здатність до 140 Мбіт/с для 3DES VPN і 140 Мбіт/с для AES-256 VPN.

Розширення:

Два 32-розрядних/33-МГц слоти PCI; два 168-контактних слоти DIMM оперативної пам'яті, що підтримують до 64 МБ пам'яті.

Інтерфейси:

Порт консолі: RS-232 (RJ-45) 9600 бод; Відмовостійкий порт: RS-232 (DB-15) 115 Кбіт/с (потрібен кабель Cisco); Два інтегрованих порти 10/100 Fast Ethernet з автоматичним узгодженням (напів/повний дуплекс), RJ-45 [6].

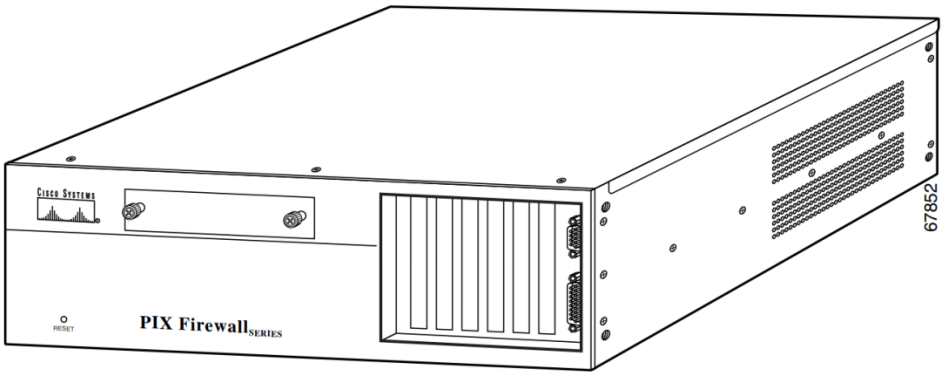

Рис. 2.6. Брандмауер Cisco PIX-520

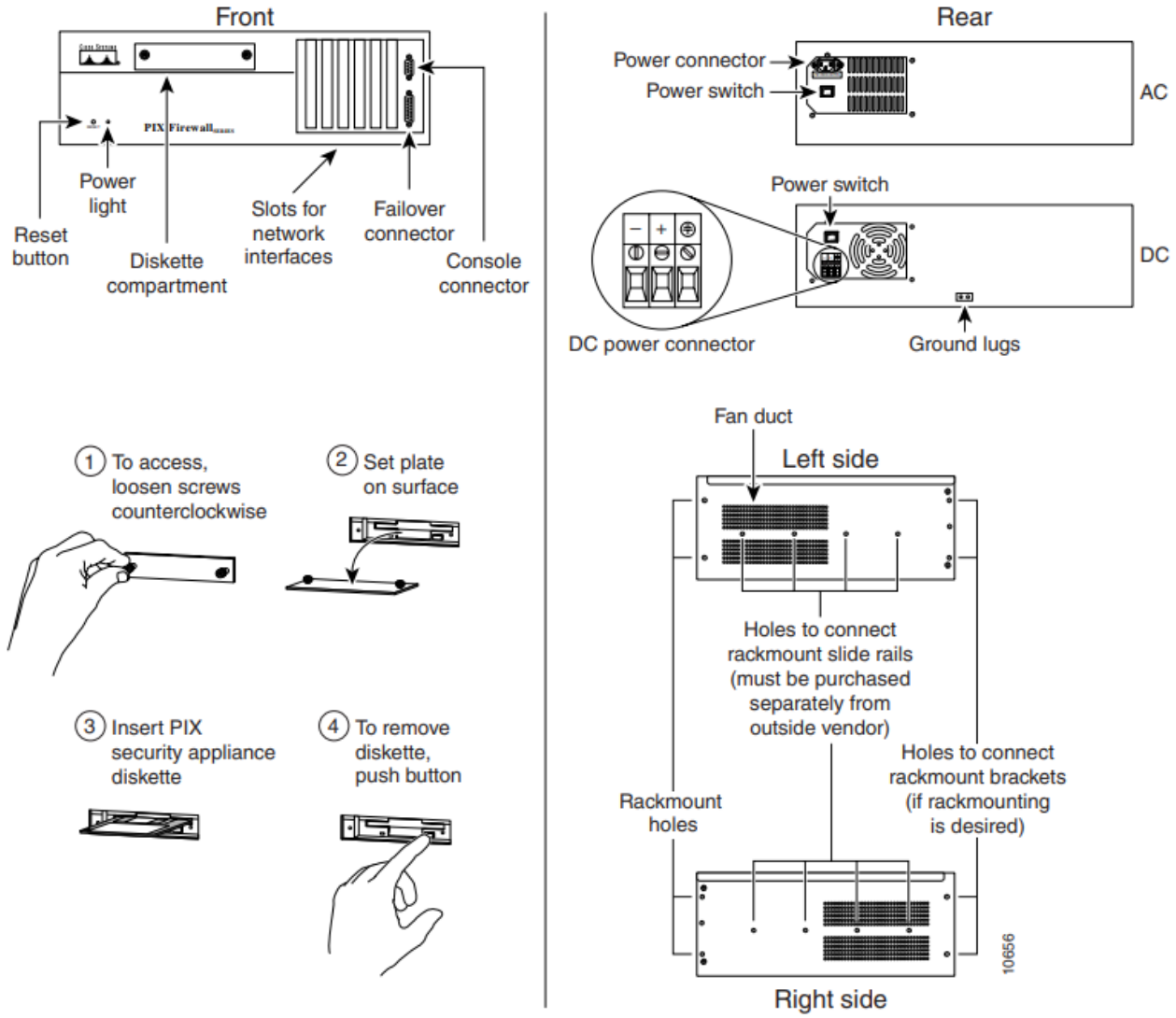

Рис. 2.7. Брандмауер Cisco PIX-520

Пристрій безпеки Cisco PIX 520 підтримує до 6 інтерфейсів.

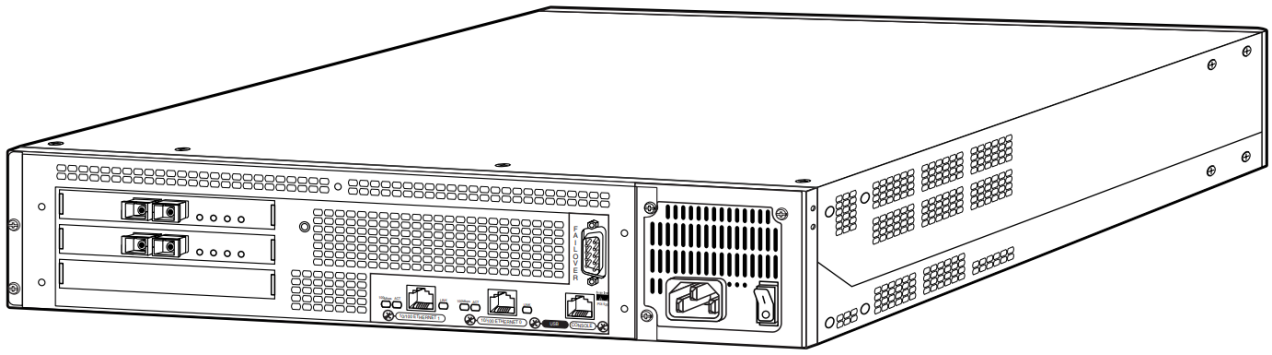

Рис. 2.8. Брандмауер Cisco PIX-525

Пристрій безпеки Cisco PIX 525 має модульну конструкцію в дві стійки (2RU) і підтримує до восьми інтерфейсів 10/100 Fast Ethernet або трьох інтерфейсів Gigabit Ethernet. Він забезпечує пропускну здатність брандмауера понад 330 Мбіт/с з можливістю обробки понад 280 000 одночасних сеансів. Деякі моделі PIX 525 оснащені вбудованим апаратним прискоренням VPN, що забезпечує пропускну здатність до 155 Мбіт/с при використанні 3DES VPN і 170 Мбіт/с при використанні AES-256 VPN.

Розширення:

Три 32-розрядні/33-МГц слоти PCI; два 168-контактні слоти оперативної пам'яті DIMM, що підтримують до 256 МБ пам'яті.

Інтерфейси:

Порт консолі: RS-232 (RJ-45) 9600 бод; Відмовостійкий порт: RS-232 (DB-15) 115 Кбіт/с (необхідний кабель Cisco); Два інтегрованих порти 10/100 Fast Ethernet, автоматичне узгодження (напів/повний дуплекс), RJ-45 [6].

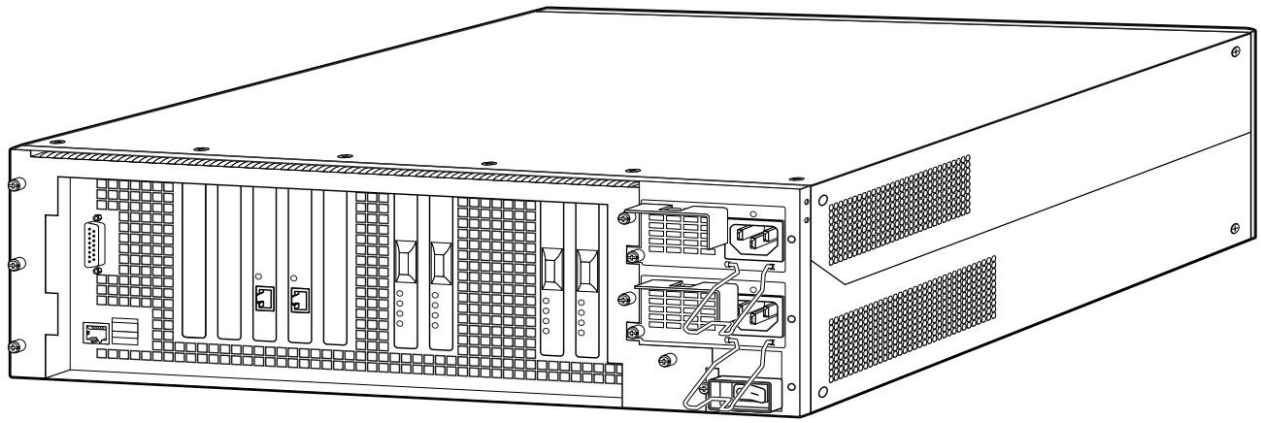

Рис. 2.9. Брандмауер Cisco PIX-535

Пристрій безпеки Cisco PIX 535 має високомодульну конструкцію в три стійки (3RU) і підтримує до десяти інтерфейсів 10/100 Fast Ethernet або дев'ять інтерфейсів Gigabit Ethernet, а також резервні джерела живлення. Він забезпечує пропускну здатність брандмауера до 1,7 Гбіт/с з можливістю обробки понад 500 000 одночасних сеансів. Деякі моделі PIX 535 оснащені вбудованим апаратним

прискоренням VPN, що забезпечує пропускну здатність до 440 Мбіт/с для 3DES VPN і 440 Мбіт/с для AES-256 VPN.

Розширення:

Чотири 64-розрядні/66-МГц слоти PCI; п'ять 32-розрядних/33-МГц слотів PCI; шість 168-контактних слотів оперативної пам'яті DIMM, що підтримують до 1 ГБ PC133 DRAM.

Інтерфейси:

Порт консолі: RS-232 (RJ-45) 9600 бод; Відмовостійкий порт: RS-232 (DB-15) 115 Кбіт/с (потрібен кабель Cisco); два інтегрованих порти 10/100 Fast Ethernet, автоузгодження (напів/повний дуплекс), RJ-45. [6].

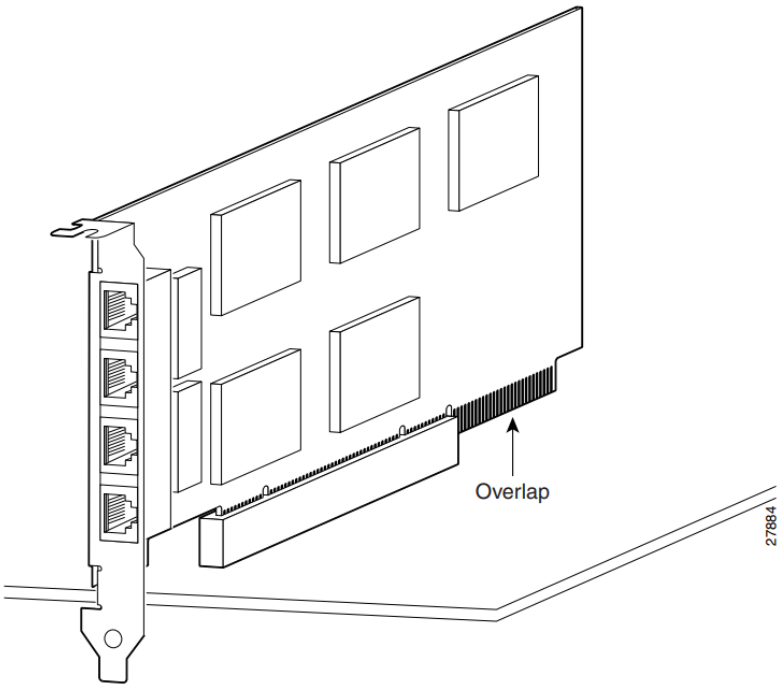

Рис. 2.10. Брандмауер Cisco PIX-4FE

PIX-1FE: інтерфейсна карта PIX 10/100 Fast Ethernet, RJ45.

PIX-4FE-66: Cisco Systems представила інтерфейсну карту Fast Ethernet 100BASE-TX для пристроїв Cisco PIX Security Appliances на базі високопродуктивної шини PCI 64-біт/66-МГц. Плата має чотири порти 100BASE-TX, підвищену продуктивність і гнучкість розгортання на модульних пристроях

Cisco PIX Security Appliances. Вона підтримується останніми випусками всіх поточних версій ОС Cisco PIX. [6].

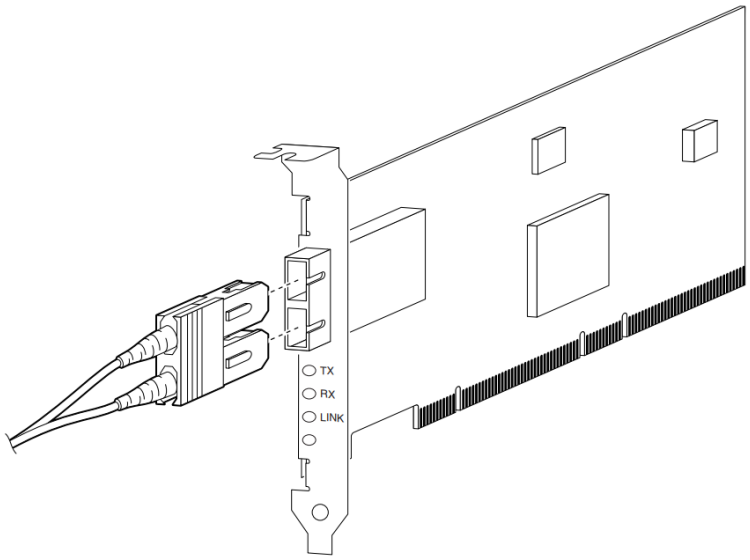

Рис. 2.11. Брандмауер Cisco PIX-1GE

Single Gigabit Ethernet interface для Cisco PIX 52X, 535 Firewall. Рекомендованим шляхом оновлення для карти Gigabit Ethernet 33 МГц є карта Gigabit Ethernet 66 МГц. Ці інтерфейси пропонують більшу продуктивність за порівнянну ціну. 64-розрядні, 66-МГц інтерфейси Gigabit Ethernet підтримуються в брандмауерах Cisco PIX 520, 525 і 535 [6].

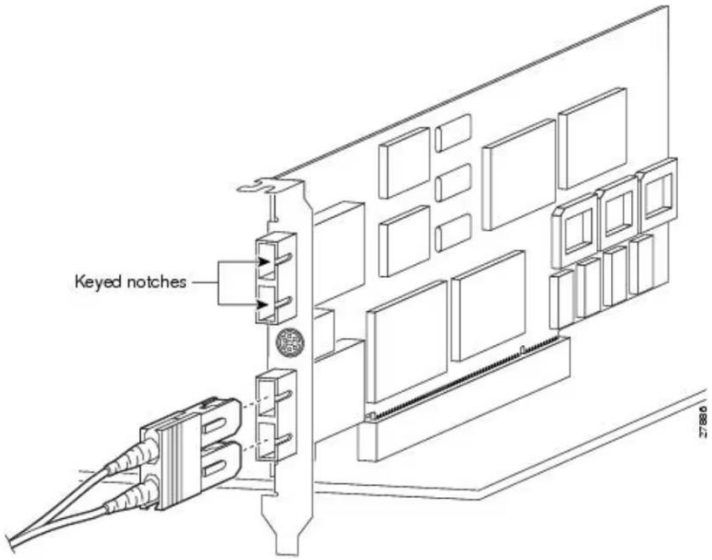

Рис. 2.12. Брандмауер Cisco PIX-FDDI

Fiber Distributed Data Interface для PIX - це EOS/EOL. Рекомендований шлях оновлення для FDDI - Gigabit Ethernet. Ці інтерфейси забезпечують більшу продуктивність при порівнянній ціні. 32-розрядні, 33-МГц інтерфейси Gigabit Ethernet підтримуються в PIX 520 і 525 так само, як і FDDI. Крім того, PIX 535 використовує більш продуктивний 64-розрядний інтерфейс Gigabit Ethernet 66 МГц, що забезпечує пропускну здатність до 1 Гбіт/с. [6].

ВИСНОВКИ ДО РОЗДІЛУ 2

В другому розділі було детально розглянуто функції та можливості Cisco PIX Firewall, який використовується для створення межі між внутрішньою мережею та зовнішніми мережами (що можуть включати одну або більше мереж периметра). Весь трафік між внутрішньою та зовнішньою мережами має проходити через брандмауер для підтримки безпеки. Зовнішня мережа зазвичай доступна через Інтернет і містить системи, які надають послуги зовнішній мережі.

Зі збільшенням кількості брандмауерів, розгорнутих в організації, адміністратор мережі повинен належним чином налаштувати конфігурації та моніторити кожного з цих брандмауерів. Тому надзвичайно важливо, щоб зі збільшенням кількості брандмауерів здатність їх вводити не була надто обтяжливо.

Мережеві брандмауери бувають двох основних форм: спеціальний пристрій або набір програмного забезпечення брандмауера, встановленого поверх операційної системи хоста. Найбільш типовою ідеєю брандмауера є спеціалізована система або прилад, що сидить у мережі та сегментах "внутрішньої" мережі з "зовнішнього" Інтернету. Приклади мережевих брандмауерів на основі пристроїв включають Cisco PIX, Cisco ASA, брандмауери NetScreen Juniper.

РОЗДІЛ 3
СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO PIX FIREWALL

3.1. Розробка структурної схеми проєкту мережі

В схемі проєкту використовується брандмауер Cisco PIX 515 для створення та захисту внутрішньої корпоративної мережі від зовнішніх зловмисників, одночасно дозволяючи внутрішнім хостам доступ до Інтернету. PIX створює три інтерфейси безпеки: зовнішній, внутрішній і DMZ. Він забезпечує зовнішнім користувачам обмежений доступ до DMZ і відсутність доступу до внутрішніх ресурсів. Внутрішні користувачі можуть отримати доступ до DMZ і зовнішніх ресурсів.

Виконання третього розділу зосереджене на конфігурації PIX як базового брандмауера. Для налаштувань використовується PIX CLI, який схожий на IOS CLI, для налаштування основних пристроїв і параметрів безпеки.

В мережі компанія має одне місце, підключене до Інтернет-провайдера. R1 представляє пристрій CPE, керований ISP. R2 являє собою проміжний Інтернет-маршрутизатор. R3 представляє провайдера, який підключає адміністратора компанії, що керує мережею, найнятого для дистанційного керування вашою мережею. PIX — це периферійний пристрій безпеки, який підключає внутрішню корпоративну мережу та DMZ до Інтернет-провайдера, надаючи послуги NAT і DHCP внутрішнім хостам.

PIX налаштовано для керування адміністратором внутрішньої мережі та віддаленим адміністратором. Інтерфейси VLAN рівня 3 забезпечують доступ до трьох областей: внутрішньої, зовнішньої та DMZ. Інтернет-провайдер призначив загальнодоступний простір IP-адрес 209.165.200.224/29, який використовуватиметься для трансляції адрес на PIX.

PIX, який використовується в даній схемі, — модель PIX 515 підтримує до шести інтерфейсів 10/100 Fast Ethernet, що робить його чудовим вибором для

підприємств, яким потрібне економічне, надійне рішення безпеки з підтримкою DMZ. Пристрій безпеки Cisco PIX 515, який є частиною провідної на ринку серії пристроїв безпеки Cisco PIX, забезпечує надійне застосування політики для користувачів і додатків, захист від багатовекторних атак і безпечні послуги підключення за допомогою широкого спектру різноманітних служб безпеки та мережевих служб

Необхідні ресурси:

- 3 маршрутизатори (Cisco 1941 із Cisco IOS Release 15.4(3)M2 образ з ліцензією Security Technology Package)
- 3 комутатори (Cisco 2960 із криптографічним образом IOS для підтримки SSH – випуск 15.0(2)SE7 або аналогічний)
- Мережевий екран Cisco PIX 515
- 3 ПК (Windows 7 або Windows 8 з клієнтським програмним забезпеченням SSH)
- Кабелі послідовного порту та Ethernet, як показано на топології
- Консольні кабелі для налаштування мережевих пристроїв Cisco

Перед тим як налаштовувати Cisco PIX Firewall була проведена основна конфігурація маршрутизаторів, комутаторів та ПК в схемі проєкту:

A. Підключення мережі та очищення попередніх налаштування пристроїв. Приєднання пристроїв, як показано на структурній схемі.
B. Налаштування основних параметрів для маршрутизаторів і комутаторів.

В схемі налаштована тактова частота для маршрутизаторів із послідовним кабелем DCE, під’єднаним до послідовного інтерфейсу. R1 показано тут як приклад.

R1(config)# interface S0/0/0

R1(config-if)# clock rate 64000

C. Налаштування статичної маршрутизацію на маршрутизаторах.

Налаштована статична маршрутизація на маршрутизаторах. Статичний маршрут за замовчуванням від R1 до R2 і від R3 до R2.

R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0

R3(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1

Налаштовано статичний маршрут від R2 до підмережі R1 G0/0 (підключеної до інтерфейсу PIX E0/0) і статичний маршрут від R2 до локальної мережі R3.

R2(config)# ip route 209.165.200.224 255.255.255.248 Serial0/0/0

R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/1

D. Увімкнення HTTP-серверу і налаштування облікового запису користувача, шифрування паролів та криптографічні ключі для SSH.

a) Увімкнено HTTP-доступ до R1 за допомогою команди ip http server у режимі глобальної конфігурації.

R1(config)# ip http server

b) Налаштовано мінімальну довжину пароля 10 символів за допомогою команди security passwords.

R1(config)# security passwords min-length 10

c) Налаштовано домене ім’я.

R1(config)# ip domain-name companysecurity.com

d) Налаштовано криптографічні ключі для SSH.

R1(config)# crypto key generate rsa general-keys modulus 1024

e) Налаштовано обліковий запис користувача admin01 за допомогою алгоритму scrypt для шифрування та пароля “Q1w0*9yu!pK”.

R1(config)# username admin01 algorithm-type scrypt secret Q1w0*9yu!pK

f) Налаштовано лінійну консоль 0 для використання локальної бази даних користувачів для входу. Для додаткової безпеки команда exec-timeout призводить до виходу лінії після п’яти хвилин бездіяльності. Синхронна команда logging запобігає перериванню введення команди повідомленнями консолі.

R1(config)# line console 0

R1(config-line)# login local

R1(config-line)# exec-timeout 5 0

R1(config-line)# logging synchronous

g) Налаштована строка vty 0 4, щоб використовувати локальну базу даних користувачів для входу та обмежити доступ лише до з’єднань SSH.

R1(config)# line vty 0 4

R1(config-line)# login local

R1(config-line)# transport input ssh

R1(config-line)# exec-timeout 5 0

h) Налаштовано пароль увімкненням надійним шифруванням.

R1(config)# enable algorithm-type scrypt secret K1q3t9*!ad

E. Налаштування параметрів IP хоста ПК.

Налаштовано статичну IP-адресу, маску підмережі та шлюз за замовчуванням для PC-A, PC-B і PC-C, як показано в табл. 3.1.

F. Перевірка підключення

Оскільки PIX є центральною точкою для мережевих зон, і її ще не налаштовано, підключення між пристроями, підключеними до неї, не буде. Однак PC-C повинен мати можливість перевіряти інтерфейс R1. З PC-C виконано пінг на IP-адресу R1 G0/0 (209.165.200.225).

G. Збереження базової робочої конфігурації для кожного маршрутизатора та комутатора.

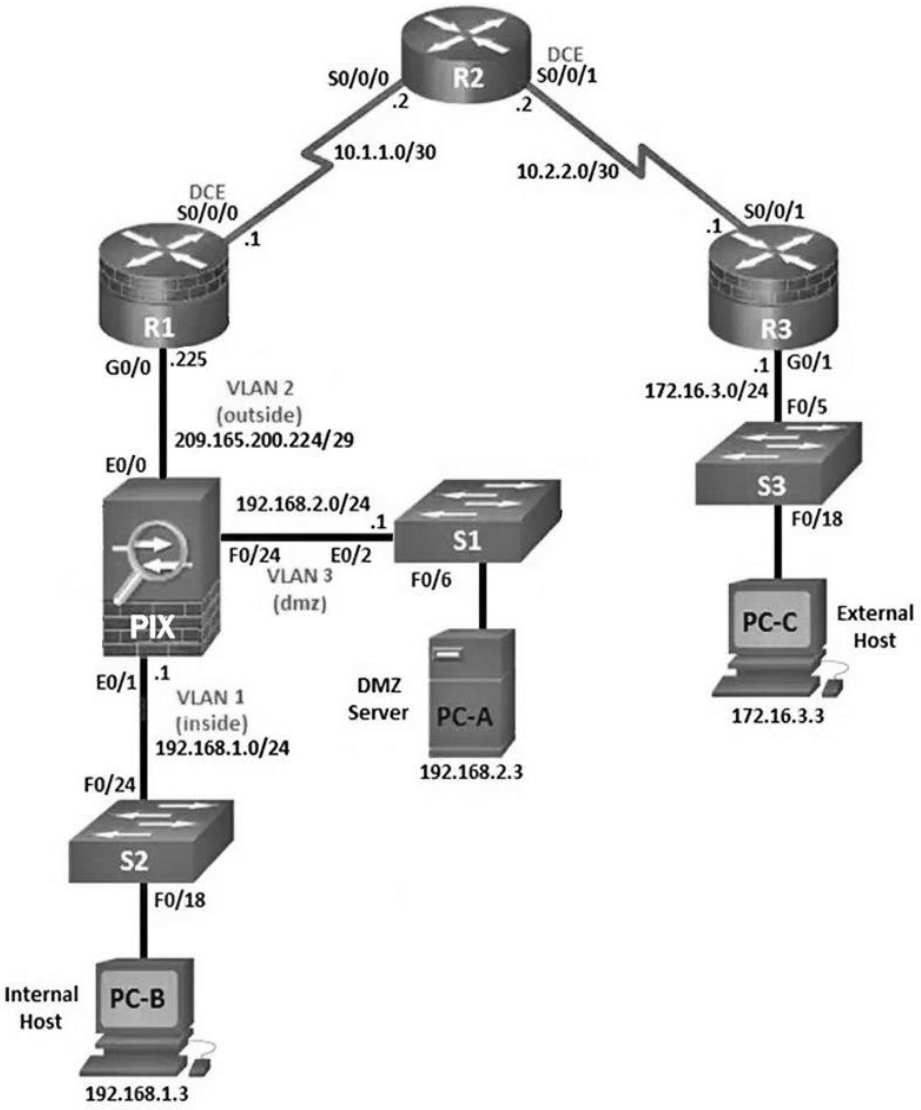

Рис. 3.1. Структурна схема проєкту мережі

Таблиця 3.1

Таблиця IP-адресації

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	209.165.200.225	255.255.255.248	N/A	PIX E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A

Завершення таблиці 3.1

R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PIX	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	N/A	S2 F0/24
PIX	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	N/A	R1 G0/0
PIX	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	N/A	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

3.2. Налаштування брандмауера Cisco PIX Firewall

Доступ до PIX через порт консолі такий самий, як і через маршрутизатор абокомутатор Cisco. Підключення до консольного порту PIX здійснюється за допомогою кабелю.

Для доступу до CLI можна використати програму емуляції терміналу, наприклад TeraTerm або PuTTy. Потім використовувати параметри послідовного порту 9600 бод, вісім бітів даних, без паритету, один стоп-біт і без керування потоком.

Вхід у привілейований режим здійснюється за допомогою команди enable та пароля (якщо пароль було встановлено). За замовчуванням пароль порожній. Ім’я хоста PIX за замовчуванням і запит — pixfirewall>.

pixfirewall> enable

Password: class (or press Enter if none set)

Визначимо поточну запущену конфігурацію:

Cisco PIX 515 зазвичай використовується як периферійний пристрій безпеки, який підключає малий бізнес або дистанційного працівника до пристрою Інтернет-провайдера, такого як DSL або кабельний модем, для доступу до Інтернету. Стандартна заводська конфігурація для PIX 515 включає наступне:

Налаштовано внутрішній інтерфейс VLAN 1, який включає порти комутатора Ethernet 0/1–0/7. IP-адреса та маска VLAN 1: 192.168.1.1 і 255.255.255.0.

Налаштовано зовнішній інтерфейс VLAN 2, який включає порт комутатора Ethernet 0/0. VLAN 2 за замовчуванням отримує свою IP-адресу від провайдера за допомогою DHCP.

Маршрут за замовчуванням походить від стандартного шлюзу DHCP.

Усі внутрішні IP-адреси транслюються під час зовнішнього доступу за допомогою інтерфейсу PAT на інтерфейсі VLAN 2.

За замовчуванням внутрішні користувачі можуть отримати доступ до зовнішнього за допомогою списку доступу, а зовнішні користувачі не мають доступу до внутрішнього.

Сервер DHCP увімкнуто на пристрої безпеки, тому ПК, який підключається до інтерфейсу VLAN 1, отримує адресу між 192.168.1.5 і 192.168.1.36 (базова ліцензія), хоча фактичний діапазон може відрізнятися.

Сервер HTTP увімкнено для ASDM і доступний для користувачів у мережі 192.168.1.0/24.

Паролі для консолі чи ввімкнення не потрібні, ім’я хоста за замовчуванням – pixfirewall.

a. Налаштовано логічний інтерфейс VLAN 1 для внутрішньої мережі (192.168.1.0/24) і встановлено рівень безпеки на найвище значення 100.

pixfirewall(config)# interface vlan 1

pixfirewall(config-if)# nameif inside

pixfirewall(config-if)# ip address 192.168.1.1 255.255.255.0

pixfirewall(config-if)# security-level 100

b. Створено логічний інтерфейс VLAN 2 для зовнішньої мережі (209.165.200.224/29), встановлено рівень безпеки на найнижче значення 0 і отримано доступ до інтерфейсу VLAN 2.

```
pixfirewall(config-if)# interface vlan 2
pixfirewall(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
pixfirewall(config-if)# ip address 209.165.200.226 255.255.255.248
pixfirewall(config-if)# no shutdown
```

За замовчуванням PIX застосовує політику, згідно з якою трафік від інтерфейсу з вищим рівнем безпеки до інтерфейсу з нижчим рівнем дозволено, а трафік від інтерфейсу з нижчим рівнем безпеки до інтерфейсу з вищим рівнем безпеки заборонено. Стандартна політика безпеки PIX дозволяє вихідний трафік, який перевіряється за умовчанням. Зворотний трафік дозволено завдяки перевірці пакетів із визначенням стану. Така типова поведінка брандмауера в режимі маршрутизації PIX дозволяє маршрутизувати пакети з внутрішньої мережі до зовнішньої мережі, але не навпаки.

c. Призначено порт E0/1 PIX рівня 2 для VLAN 1 і порт E0/0 для VLAN Використовано команду no shutdown, щоб переконатися, що вони працюють.

```
pixfirewall(config)# interface e0/1
pixfirewall(config-if)# switchport access vlan 1
pixfirewall(config-if)# no shutdown
pixfirewall(config-if)# interface e0/0
pixfirewall(config-if)# switchport access vlan 2
pixfirewall(config-if)# no shutdown
```

Для перевірки прикладного рівня, а також для інших розширених опцій Cisco MPF доступний на PIX. Cisco MPF використовує три об’єкти конфігурації для визначення модульних, об’єктно-орієнтованих та ієрархічних політик:

- Карти класів – визначення критерія відповідності.
- Карти політики – зв’язок дії з критеріями відповідності.

Політики обслуговування – приєднана карта політики до інтерфейсу або глобально до всіх інтерфейсів пристрою.

a. Відображення карти політики MPF за замовчуванням, яка виконує перевірку внутрішнього трафіку. Лише трафік, який було ініційовано зсередини, дозволено повертатися до зовнішнього інтерфейсу.

b. Додано перевірку трафіку ICMP до списку карти політики за допомогою таких команд:

pixfirewall(config)# policy-map global_policy

pixfirewall(config-pmap)# class inspection_default

pixfirewall(config-pmap-c)# inspect icmp

У цій частині підрозділу створено DMZ на PIX, налаштовано статичний NAT на сервер DMZ і застосовано ACL для контролю доступу до сервера.

Для додавання DMZ і веб-сервера використовано іншу адресу з діапазону ISP, призначеного 209.165.200.224/29 (.224-.231). Маршрутизатор R1 G0/0 і зовнішній інтерфейс PIX вже використовують 209.165.200.225 і .226. Використано публічну адресу 209.165.200.227 і статичний NAT, щоб надати серверу доступ до перекладу адреси.

Налаштування інтерфейсу DMZ VLAN 3 на PIX.

Налаштовано DMZ VLAN 3, де буде розміщено веб-сервер загального доступу. Призначено IP-адресу VLAN 3 192.168.2.1/24, названо її dmz і призначено рівень безпеки 70.

pixfirewall(config)# interface vlan 3

pixfirewall(config-if)# ip address 192.168.2.1 255.255.255.0

pixfirewall(config-if)# nameif dmz

ERROR: This license does not allow configuring more than 2 interfaces with nameif and without a "no forward" command on this interface or on 1 interface(s) with nameif already configured.

pixfirewall(config-if)# no forward interface vlan 1

pixfirewall(config-if)# nameif dmz

INFO: Security level for "dmz" set to 0 by default.

pixfirewall(config-if)# security-level 70

pixfirewall(config-if)# no shut

с. Призначено фізичний інтерфейс PIX E0/2 до DMZ VLAN 3 і увімкнено інтерфейс.

pixfirewall(config-if)# interface Ethernet0/2

pixfirewall(config-if)# switchport access vlan 3

pixfirewall(config-if)# no shut

Налаштування статичного NAT на сервер DMZ за допомогою мережевого об’єкта.

Налаштовано мережевий об’єкт під назвою dmz-сервер і призначено йому статичну IP-адресу сервера DMZ (192.168.2.3). Перебуваючи в режимі визначення об’єкта, використовано команду nat, щоб вказати, що цей об’єкт використовується для перетворення адреси DMZ на зовнішню адресу за допомогою статичного NAT, і вказано загальнодоступну перекладену адресу 209.165.200.227.

pixfirewall(config)# object network dmz-server

pixfirewall(config-network-object)# host 192.168.2.3

pixfirewall(config-network-object)# nat (dmz,outside)

Налаштовано іменований список доступу (OUTSIDE-DMZ), який дозволяє використовувати будь-який протокол IP від будь-якого зовнішнього хоста до внутрішньої IP-адреси сервера DMZ. Застосовано список доступу до зовнішнього інтерфейсу PIX в напрямку IN.

pixfirewall(config)# access-list OUTSIDE-DMZ permit ip any host 192.168.2.3

pixfirewall(config)# access-group OUTSIDE-DMZ in interface outside

Зовнішні хости отримують доступ до сервера, використовуючи його загальнодоступну статичну адресу NAT, PIX перетворює її на внутрішню IP-адресу хоста, а потім застосовує ACL.

Тепер доступ до сервера DMZ можна отримати із хоста у внутрішній мережі, оскільки для внутрішнього інтерфейсу PIX (VLAN 1) встановлено рівень безпеки 100 (найвищий), а для інтерфейсу DMZ (VLAN 3) встановлено 70. PIX діє як маршрутизатор між двома мережами. Список доступу може бути застосований до

внутрішнього інтерфейсу, щоб керувати типом дозволеного чи забороненого доступу до сервера DMZ із внутрішніх хостів.

3.3. Політика корпоративной безпеки

Метою цієї політики є встановлення технічних вказівок щодо IT-безпеки та передача засобів контролю, необхідних для безпечної мережевої інфраструктури. Політика безпеки мережі забезпечить практичні механізми підтримки комплексного набору політик безпеки компанії.

Політика поширюється на всі IT-системи та пристрої, які входять до корпоративної мережі або які іншим чином контролюються компанією.

А. Паролі мережевих пристроїв

Зламаний пароль на мережевому пристрої може мати руйнівні наслідки для всієї мережі. Паролі, які використовуються для захисту цих пристроїв, як-от маршрутизаторів, комутаторів і серверів, мають відповідати вищим стандартам, ніж стандартні паролі на рівні користувача чи настільних системних паролів.

а) Пароль

Побудова Наступні твердження застосовуються до побудови паролів для мережевих пристроїв:

• Паролі повинні містити не менше 6 символів

• Паролі мають складатися з комбінації літер, цифр і спеціальних символів (знаків пунктуації та символів)

• Паролі повинні складатися з комбінації символів верхнього та нижнього регістру

• Паролі не повинні складатися зі слів, які можна знайти в словнику, або іншим чином використовувати їх

• Паролі не повинні складатися з очевидної послідовності клавіатури (наприклад, qwerty)

• Паролі не повинні містити дані, які можна вгадати, наприклад особисту інформацію, як-от дні народження, адреси, номери телефонів, місцезнаходження тощо.

b) Помилка входу в систему

Повторні помилки входу можуть означати спробу «зламати» пароль і приховано отримати доступ до мережевого облікового запису. Щоб захиститися від підбору пароля та спроб грубої сили, компанія повинна заблокувати обліковий запис користувача після 3 невдалих входів. Це може бути реалізовано як блокування на основі часу або вимагає ручного скидання на розсуд IT-менеджера. З метою захисту від вгадування облікового запису, коли виникають помилки входу, повідомлення про помилку, передане користувачеві, не повинно конкретно вказувати, чи ім’я облікового запису чи пароль були неправильними. Помилка може бути такою простою, як «ім’я користувача та/або пароль, які ви надали, були неправильними».

c) Вимоги до змін

Паролі повинні бути змінені відповідно до Політики паролів компанії. Крім того, наступні вимоги застосовуються до зміни паролів мережевих пристроїв: • Якщо існує підозра, що пароль будь-якого мережевого пристрою було зламано, потрібно негайно змінити паролі всіх мережевих пристроїв.

• Якщо мережевий або системний адміністратор компанії залишає компанію, усі паролі, до яких адміністратор міг мати доступ, необхідно негайно змінити. Ця заява також стосується будь-якого консультанта чи підрядника, який має доступ до адміністративних паролів.

• Під час введення в експлуатацію нових пристроїв необхідно змінити паролі за замовчуванням від виробника.

d) Застосування політики паролів

Там, де використовуються паролі, має бути реалізовано програму, яка забезпечує дотримання політики паролів компанії щодо створення, зміни, повторного використання, блокування тощо.

e) Пароль адміністратора

Рекомендації Як правило, адміністративний (також відомий як "кореневий") доступ до систем має бути обмежений лише тими особами, які мають законну бізнес-потребу в цьому типі доступу. Це особливо важливо для мережевих пристроїв, оскільки адміністративні зміни можуть мати серйозний вплив на мережу та, як такі, на безпеку мережі. Крім того, слід реєструвати адміністративний доступ до мережевих пристроїв.

B. Ведення журналу

Реєстрація певних подій є важливою складовою належної практики керування мережею. Потреби в журналі залежать від типу мережевої системи та типу даних, які система зберігає. У наступних розділах детально описано вимоги компанії щодо реєстрації та перегляду журналів.

a) Сервери додатків

Журнали із серверів додатків представляють інтерес, оскільки ці сервери часто дозволяють з'єднання з великої кількості внутрішніх та/або зовнішніх джерел. Ці пристрої часто є невід'ємною частиною безперебійної роботи бізнесу. Приклади: Інтернет, електронна пошта, сервери баз даних. Вимога: як мінімум потрібно реєструвати помилки, збої та помилки входу. За потреби рекомендується проводити додаткове журналювання. Жодні паролі не повинні міститися в журналах.

b) Мережеві пристрої

Журнали мережевих пристроїв представляють інтерес, оскільки ці пристрої контролюють увесь мережевий трафік і можуть мати величезний вплив на безпеку компанії.

Приклади: брандмауери, мережеві комутатори, маршрутизатори

Вимога: як мінімум потрібно реєструвати помилки, несправності та невдалі входи. За потреби рекомендується проводити додаткове журналювання. Жодні паролі не повинні міститися в журналах.

c) Критичні пристрої

Критичні пристрої – це будь-які системи, критично важливі для бізнес-операцій. Ці системи також можуть підпадати під інші категорії, наведені вище - у будь-якому випадку, коли це станеться, цей розділ замінить собою.

Приклади: файлові сервери, лабораторні чи виробничі машини, системи зберігання інтелектуальної власності

Вимоги. Потрібна як мінімум реєстрація помилок, несправностей і невдалих входів. За потреби рекомендується проводити додаткове журналювання. Жодні паролі не повинні міститися в журналах.

d) Керування журналами

Журнали слід зберігати відповідно до Політики зберігання компанії. Якщо інше не визначено IT-менеджером, журнали слід вважати робочими даними.

C. Брандмауери

Брандмауери є, мабуть, найважливішим компонентом надійної стратегії безпеки. Підключення до Інтернету та інші незахищені мережі мають бути відокремлені від мережі компанії за допомогою брандмауера.

a) Конфігурація

Наступні твердження стосуються впровадження компанією технології брандмауера:

• Брандмауери повинні забезпечувати безпечний адміністративний доступ (за допомогою шифрування) з доступом до керування, обмеженим, якщо це можливо, лише мережами, з яких очікується вихід керуючих з'єднань.

• На брандмауерах не можна вмикати непотрібні служби чи програми. Компанія повинна використовувати «захищені» системи для платформ брандмауера або пристроїв.

• Годинники брандмауерів повинні бути синхронізовані з іншим мережевим обладнанням компанії за допомогою NTP або іншим способом. Серед інших переваг це допоможе у вирішенні проблем і розслідуванні інцидентів безпеки.

• Набір правил брандмауера необхідно документувати та щоквартально перевіряти. Перевірки повинні охоплювати кожне правило, для чого воно потрібне, чи все ще є необхідним і чи можна його вдосконалити.

• Для власного захисту набір правил брандмауера повинен включати «правило прихованої дії», яке забороняє підключення до самого брандмауера.

• Брандмауер повинен реєструвати скинуті або відхилені пакети.

b) Фільтрація вихідного трафіку

Брандмауери часто налаштовані на блокування лише вхідних з’єднань із зовнішніх джерел; однак, фільтруючи вихідні з’єднання з мережі, безпеку можна значно покращити. Ця практика також називається «фільтрацією вихідного трафіку».

Блокування вихідного трафіку запобігає доступу користувачів до непотрібних і часто небезпечних служб. Якщо точно вказати, який вихідний трафік дозволити, увесь інший вихідний трафік блокується. Цей тип фільтрації блокуватиме руткити, віруси та інші шкідливі інструменти, якщо хост буде скомпрометовано. Це також запобігатиме доступу віддалених робочих столів до внутрішньої мережі.

Компанія заохочує вихідну фільтрацію, якщо це можливо, але це не обов’язково. Якщо фільтрування вважається можливим, лише такі відомі «хороші» служби повинні бути дозволені на вихід із мережі: 21, 22, 23, 25, 53, 80, 110, 443 і 995.

D. Мережеве обладнання

Мережеве обладнання, таке як маршрутизатори, комутатори, концентратори, мости та точки доступу, має бути реалізовано послідовним чином. Наступні твердження стосуються впровадження компанією мережевого обладнання:

• Мережеве обладнання повинне забезпечувати безпечний адміністративний доступ (за допомогою шифрування) з доступом до керування, обмеженим, якщо це можливо, лише мережами, з яких очікується вихід керуючих з’єднань.

• Годинники на всьому мережевому обладнанні мають бути синхронізовані за допомогою NTP або іншим способом. Серед інших переваг це допоможе у вирішенні проблем і розслідуванні інцидентів безпеки.

• Якщо це можливо для програми, перевагу надають комутаторам, ніж концентраторам. Під час використання комутаторів компанія повинна використовувати VLAN для розділення мереж, якщо це розумно та можливо.

• На мережевих пристроях, які забороняють пряме з’єднання з пристроями, мають бути реалізовані списки контролю доступу. Винятком є підключення до керування, які можуть бути обмежені відомими джерелами.

• Невикористовувані служби та порти мають бути відключені на мережевому обладнанні.

• Доступ до адміністративних портів на мережевому обладнанні має бути обмежено відомими хостами керування та іншим чином заблоковано брандмауером або списком контролю доступу.

E. Мережеві сервери

Сервери зазвичай приймають з’єднання з кількох джерел, як внутрішніх, так і зовнішніх. Як правило, чим більше джерел підключається до системи, тим більший ризик пов’язаний із цією системою, тому особливо важливо захищати мережеві сервери. Наступні твердження стосуються використання компанією мережевих серверів:

• Непотрібні файли, служби та порти слід видалити або заблокувати. Якщо можливо, дотримуйтеся посібника з посилення безпеки сервера, який можна отримати від провідних виробників операційних систем.

• Мережеві сервери, навіть ті, які призначені для прийому публічних з'єднань, повинні бути захищені брандмауером або списком контролю доступу.

• Якщо можливо, слід розробити стандартний процес встановлення для мережевих серверів компанії. Це забезпечить узгодженість між серверами незалежно від того, який співробітник або підрядник займається встановленням.

• Годинники мережевих серверів мають бути синхронізовані з іншим мережевим обладнанням компанії за допомогою NTP або іншим способом. Серед інших переваг це допоможе у вирішенні проблем і розслідуванні інцидентів безпеки.

F. Виявлення/запобігання вторгненням

Технології системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) можуть бути корисними для моніторингу та безпеки мережі. Інструменти відрізняються тим, що IDS попереджає про підозрілу активність, тоді як IPS блокує цю активність. При правильному налаштуванні IDS корисні, але можуть генерувати велику кількість даних, які необхідно оцінити, щоб система була корисною. IPS автоматично вживають заходів, коли бачать підозрілі події, що може

бути як добре, так і погано, оскільки законний мережевий трафік може блокуватися разом із зловмисним.

Компанія не вимагає і не забороняє використання систем IDS або IPS. Рішення про використання систем IDS/IPS залишається на розсуд IT-менеджера.

G. Тестування безпеки

Тестування безпеки, також відоме як оцінка вразливості, аудит безпеки або тестування на проникнення, є важливою частиною підтримки безпеки мережі компанії. Тестування безпеки може здійснюватися співробітниками IT-спеціалістів, але часто ефективніше, якщо виконується третьою стороною, яка не має зв'язку з повсякденною діяльністю компанії в галузі інформаційних технологій. У наступних розділах детально описано вимоги компанії щодо тестування безпеки.

a) Тестування внутрішньої безпеки

Тестування внутрішньої безпеки не обов'язково стосується тестування внутрішньої мережі, а скоріше тестування, яке виконують члени IT-команди компанії. Внутрішнє тестування не повинно замінювати зовнішнє тестування; однак, коли зовнішнє тестування з будь-якої причини не є доцільним або як доповнення до зовнішнього тестування, внутрішнє тестування може бути корисним для оцінки безпеки мережі. Внутрішнє тестування безпеки допускається, але тільки працівниками, службовими функціями яких є оцінка безпеки, і лише з дозволу IT-менеджера. Внутрішнє тестування не повинно мати вимірного негативного впливу на системи компанії або продуктивність мережі.

b) Зовнішнє тестування безпеки

Зовнішнє тестування безпеки, яке проводиться сторонньою організацією, є чудовим способом аудиту засобів контролю безпеки компанії. IT-менеджер повинен визначити, якою мірою слід проводити це тестування та які системи/програми воно має охоплювати.

Зовнішнє тестування не повинно негативно впливати на продуктивність мережі в робочий час або безпеку мережі в будь-який час.

Як правило, слід не заохочувати «тестування на проникнення», яке є активним використанням вразливостей компанії. Якщо проводиться тестування на проникнення, воно не повинно негативно впливати на системи чи дані компанії.

Компанія заохочує зовнішнє тестування безпеки, але не надає жорстких вказівок щодо того, з якою періодичністю має відбуватися тестування. Тестування слід проводити так часто, як це необхідно, як це визначає IT-менеджер.

H. Антивірус/Anti-Malware

Комп'ютерні віруси та зловмисне програмне забезпечення викликають нагальне занепокоєння в сучасному середовищі загроз. Якщо машина або мережа не захищені належним чином, спалах вірусу може мати руйнівні наслідки для машини, мережі та всієї компанії. Компанія надає такі вказівки щодо використання антивірусного програмного забезпечення та програмного забезпечення для захисту від шкідливих програм:

• На всіх наданих компанією робочих станціях користувачів має бути встановлено програмне забезпечення для захисту від вірусів/шкідливих програм.

• Програмне забезпечення робочої станції має підтримувати поточну «підписку» на отримання виправлень і оновлень файлів сигнатур/визначення вірусів.

• Патчі, оновлення та оновлення файлів антивірусних сигнатур необхідно встановлювати своєчасно, автоматично або вручну.

ВИСНОВКИ ДО РОЗДІЛУ 3

В третьому розділі була спроектована схема проєкту мережі, брандмауер Cisco PIX 515 використовується для створення та захисту внутрішньої корпоративної мережі від зовнішніх зловмисників, одночасно дозволяючи внутрішнім хостам доступ до Інтернету. PIX створює три інтерфейси безпеки: зовнішній, внутрішній і DMZ. Він забезпечує зовнішнім користувачам обмежений доступ до DMZ і відсутність доступу до внутрішніх ресурсів. Внутрішні користувачі можуть отримати доступ до DMZ і зовнішніх ресурсів. Виконання третього розділу

зосереджене на конфігурації PIX як базового брандмауера. Для налаштувань використовується PIX CLI, який схожий на IOS CLI, для налаштування основних пристроїв і параметрів безпеки.

В мережі компанія має одне місце, підключене до Інтернет-провайдера. R1 представляє пристрій CPE, керований ISP. R2 являє собою проміжний Інтернет-маршрутизатор. R3 представляє провайдера, який підключає адміністратора компанії, що керує мережею, найнятого для дистанційного керування вашою мережею. PIX — це периферійний пристрій безпеки, який підключає внутрішню корпоративну мережу та DMZ до Інтернет-провайдера, надаючи послуги NAT і DHCP внутрішнім хостам. PIX налаштовано для керування адміністратором внутрішньої мережі та віддаленим адміністратором. Інтерфейси VLAN рівня 3 забезпечують доступ до трьох областей: внутрішньої, зовнішньої та DMZ.

Політика корпоративної безпеки встановлює технічні вказівки щодо IT-безпеки та передачі засобів контролю, необхідних для безпечної мережевої інфраструктури.

ВИСНОВКИ

Під час виконання даної кваліфікаційної роботи було створено проєкт системи інформаційної безпеки на базі обладнання Cisco Secure Private Internet Exchange Firewall та розроблено поради для впровадження та застосування політики корпоративної безпеки, які включають в собі основні правила та тенденції для створення системи мережевої безпеки підприємства.

В першому розділі були розглянуті основні аспекти забезпечення безпеки мережі, з'ясовано що безпека мережі повинна поєднувати в собі кілька шарів захисних сил на кінцевих пристроях та в самій мережі. Кожен мережевий рівень безпеки реалізує політику та управління. Загрози можуть походити від різних суб'єктів, включаючи корпоративних шпигунів, хакерів, терористичних груп, ворожих національних держав, злочинних організацій та інших. Було проаналізовано категорії загроз, види мережевих вторгнень, варіанти протидії мережевим атакам. Також було оглянуто причини, які спричиняли мережеві вторгнення.

В другому було розглянуто функції та можливості Cisco PIX Firewall, який використовується для створення межі між внутрішньою мережею та зовнішніми. Аналізувалися типи брандмауерів та види міжмережевих екранів PIX.

Третій розділ представляє собою реалізацію самого проєкту системи інформаційної безпеки на базі обладнання на базі обладнання Cisco PIX Firewall. Отже в даному розділі була спроектована та налаштована певна приватна мережа. Було сформульовані приклади правил корпоративної безпеки. Спроектована система може використовуватись для домашніх потреб, так і невеликими підприємствами.

Політика безпеки мережі проєкту забезпечує практичні механізми підтримки комплексного набору політик безпеки компанії. Політика безпеки поширюється на всі IT-системи та пристрої, які входять до проєкту корпоративної мережі.

Дана система інформаційної безпеки мережі здатна забезпечити прийнятний рівень безпеки від більшості існуючих загроз. А при дотримані правил, своєчасній

модерації, діагностиці та відмінному адмініструванні система має потенціал бути стабільно захищеною, добре працювати, мати задатки на гарну майбутню експлуатацію та модернізацію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is Network Security?. *Forcepoint*. URL: https://www.forcepoint.com/cyber-edu/network-security (дата звернення: 11.06.2023).
2. Інформаційна безпека - Wise IT Ukraine. *Wise IT Ukraine*. URL: https://wiseit.com.ua/services/rishennya-ta-servisy/informaczijna-bezpeka/ (дата звернення: 11.06.2023).
3. What is a Data Breach? | IBM. *IBM - Deutschland | IBM*. URL: https://www.ibm.com/topics/data-breach (дата звернення: 11.06.2023).
4. Number of data breaches and victims U.S. 2022 | Statista. *Statista*. URL: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (дата звернення: 11.06.2023).
5. What Is Network Security?. *Cisco*. URL: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html (дата звернення: 11.06.2023).
6. *Networking, Cloud, and Cybersecurity Solutions - Cisco*. URL: https://www.cisco.com/web/ANZ/cpp/refguide/hview/security/pix.html (дата звернення: 11.06.2023).