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 захисту периметру корпоративної мережі на базі обладнання D-Link» _____.

Виконавець: _____ Роман САЛЕЙ.
(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

Салея Романа Петровича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Система захисту периметру корпоративної мережі на базі обладнання D-Link»
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: міжмережевого екрану D-Link, операційна система NetDefendOS
4. Зміст пояснювальної записки: вступ, актуальність проблеми захисту периметру корпоративної мережі, методи та засоби захисту периметра корпоративної мережі, система захисту периметру корпоративної мережі на базі обладнання D-Link, висновки, список використаних джерел
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди за тематикою роботи в програмному пакеті Microsoft PowerPoint

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	10.04.2023-12.04.2023	Виконано
2	Вступ	13.04.2023	Виконано
3	Актуальність проблеми захисту периметру корпоративної мережі	14.04.2023-01.05.2023	Виконано
4	Методи та засоби захисту периметра корпоративної мережі	02.05.2023-14.05.2023	Виконано
5	Система захисту периметру корпоративної мережі на базі обладнання D-Link	14.05.2023-29.05.2023	Виконано
6	Усунення недоліків та захист кваліфікаційної роботи	01.06.2023-10.06.2023	Виконано

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

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

Завдання прийняв до виконання _____ Роман САЛЕЙ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Система захисту периметру корпоративної мережі на базі обладнання D-Link» містить 62 сторінки, 7 рисунків, 1 таблиця, 6 використаних джерел.

КОМПЮТЕРНА МЕРЕЖА, КІБЕРБЕЗПЕКА, D-LINK, NETDEFENDOS

Об’єкт дослідження – операційна система NetDefendOS.

Предмет дослідження – міжмережевий екран D-Link DFL-1600.

Мета кваліфікаційної роботи – налаштування системи захисту периметру корпоративної мережі на базі обладнання D-Link.

Метод дослідження – опис, порівняння, аналіз, узагальнення.

Матеріали кваліфікаційної роботи рекомендується використовувати при вивченні принципів побудови систем захисту периметру мережі.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

IDS(Intrusion Detection System) – система виявлення вторгнень

IPS(Intrusion prevention system) – система профілактики вторгнення

WAN(Wide Area Network) – глобальна обчислювальна мережа

VPN(Virtual Private Network) – віртуальна приватна мережа

ALG(Application Layer Gateway) – шлюз прикладного рівня

SNMP(Simple Network Management Protocol) – простий протокол керування мережею

SMTP(Simple Mail Transfer Protocol) – простий протокол пересилання пошти

HTTP(HyperText Transfer Protocol) – протокол передачі гіпертекстових документів

CLI(Command line interface) – інтерфейс командного рядка

VLAN(Virtual Local Area Network) – віртуальна локальна комп'ютерна мережа

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

DMZ(Demilitarized Zone) – демілітаризована зона

ВСТУП

Актуальність теми. Наразі всі державні служби, середній бізнес, великі підприємці перейшли або переходять на електронний обмін та зберігання даних і потребують якісного та надійного захисту периметру корпоративної мережі.

D-Link є популярним брендом, який виробляє мережеве обладнання споживчого та корпоративного рівня. Брандмауери D-Link NetDefend забезпечують потужне рішення безпеки для захисту бізнес-мереж від різноманітних загроз.

Мета і завдання дослідження. Розробити систему захисту периметру корпоративної мережі на базі обладнання D-Link.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. обґрунтування необхідності захисту периметру корпоративної мережі;
2. огляд методів та засобів захисту периметра корпоративної мережі;
3. загальні налаштуваня операційної системи NetDefendOS;
4. забезпечення безпеки окремих елементів корпоративної мережі за допомогою ALG міжмережевого екрану.

Об’єктом дослідження – операційна система NetDefendOS.

Предметом дослідження – міжмережевий екран D-Link DFL-1600.

Методи дослідження. Опис, порівняння, аналіз, узагальнення.

Практичне значення отриманих результатів. Матеріали кваліфікаційної роботи рекомендується використовувати при вивченні принципів побудови систем захисту периметру мережі.

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
АКТУАЛЬНІСТЬ ПРОБЛЕМИ ЗАХИСТУ ПЕРИМЕТРУ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1. Необхідність захисту мережі

Мережева безпека охоплює всі кроки, зроблені для захисту цілісності комп'ютерної мережі та даних всередині неї. Безпека мережі важлива, оскільки вона захищає конфіденційні дані від кібератаків та забезпечує мережу, яка є корисною та надійною. Успішні стратегії безпеки мережі використовують декілька рішень безпеки для захисту користувачів та організацій від зловмисних та кібер-атак, таких як відмова в обслуговуванні.

Мережа складається з взаємопов'язаних пристроїв, таких як комп'ютери, сервери та бездротові мережі. Багато з цих пристроїв сприйнятливі до потенційних зловмисників. Мережева безпека передбачає використання різноманітних програмних та апаратних інструментів у мережі або як програмне забезпечення з послуг. Безпека стає важливішою, оскільки мережі зростають складнішими, а підприємства більше покладаються на їхні мережі та дані для ведення бізнесу. Методи безпеки повинні розвиватися, оскільки суб'єкти загрози створюють нові методи нападу на ці все складніші мережі.

Незалежно від конкретного методу або стратегії безпеки підприємства, безпека зазвичай обрамлена як відповідальність кожного, оскільки кожен користувач в мережі представляє можливу вразливість у цій мережі.

Безпека мережі є критичною, оскільки вона запобігає кіберзлочинцям отримати доступ до цінних даних та конфіденційної інформації. Коли хакери отримують такі дані, вони можуть спричинити різноманітні проблеми, включаючи крадіжку особи, викрадені активи та репутаційну шкоду.

Нижче наведено чотири найважливіші причини, через які є важливі захисні мережі та дані, які вони зберігають:

1. Оперативні ризики. Організація без адекватного зриву в мережевій безпеці. Підприємства та особисті мережі залежать від пристроїв та програмного забезпечення, які не можуть ефективно працювати, коли компрометували вірусами, зловмисними та кібер-атаками. Бізнес також покладається на мережі для більшості внутрішньої та зовнішньої комунікації.

2. Фінансові ризики для компрометованої особистої інформації. Порушення даних можуть бути дорогими як для людей, так і для підприємств. Організації, які обробляють PII, такі як номери соціального страхування та паролі, повинні захистити його. Експозиція може коштувати грошима жертвам штрафу, реституції та ремонту порушених пристроїв. Порушення даних та експозиція також можуть зруйнувати репутацію компанії та піддавати її судовам. "Вартість звіту про порушення даних 2022 року", який проводився Інститутом Понемона, повідомила, що середня вартість порушення даних зросла до 4,35 мільйонів доларів у 2022 році з 4,24 мільйона доларів у 2021 році.

3. Фінансовий ризик порушеного інтелектуальної власності. Організації також можуть викрадатися власну інтелектуальну власність, що дорого. Втрата ідей, винаходів та продуктів компанії може призвести до втрати бізнесу та конкурентних переваг.

4. Проблеми з регуляторами. Багато урядів вимагають від підприємств дотримуватися правил безпеки даних, які охоплюють аспекти безпеки мережі. Наприклад, медичні організації в Сполучених Штатах зобов’язані дотримуватися правил Закону про переносність та підзвітність медичного страхування (HIPAA), а організації в Європейському Союзі, які стосуються даних громадян, повинні дотримуватися загального регламенту захисту даних (GDPR) . Порушення цих правил можуть призвести до штрафів, заборон та можливого часу в'язниці.

Безпека мережі настільки важлива, що кілька організацій зосереджуються на створенні та обміні стратегіями, як адаптуватися до сучасних загроз. Miter ATT &

СК, Національний інститут стандартів та технологій та Центр безпеки в Інтернеті забезпечують безкоштовні, непропретаційні рамки безпеки та бази знань для обміну інформацією про кіберзагрози та допомоги бізнесу та іншим організаціям оцінювати їх методи безпеки мережі [1].

Безпека мережі застосовується за допомогою комбінації апаратних та програмних засобів. Основна мета безпеки мережі - запобігти несанкціонованому доступу до частин мережі або між ними.

Спеціаліст по безпеці або команда визначає стратегії та політику, які забезпечують безпеку мережі організації та допомагають їй дотримуватися стандартів безпеки та правил. Кожен в мережі повинен дотримуватися цих правил політики безпеки. Кожна точка в мережі, де авторизований користувач може отримати доступ до даних, також є моментом, коли дані можуть бути порушені або зловмисником, або через необережність користувача чи помилки.

Рис. 1.1. Елементи мережевої безпеки

Вибір політики та інструментів безпеки залежить від мережі до мережі та змінюється з часом. Сильна безпека часто передбачає використання декількох підходів, відомі як багатошарова безпека або захист глибоко, щоб надати організаціям якомога більше контролю безпеки. Нижче наведено деякі часто використовувані типи інструментів та програмного забезпечення мережевої безпеки:

• Управління доступом. Цей метод обмежує доступ до мережевих додатків та систем певній групі користувачів та пристроїв. Ці системи заперечують доступ до користувачів та пристроїв, які вже не санкціоновані.

• Антивірус та протидія зловмисного забезпечення. Антивірус та протидія зловмисного забезпечення - це програмне забезпечення, призначене для виявлення, вилучення або запобігання вірусам та зловмисним програмним забезпеченням, таких як троянські коні, шантажувальне програмне забезпечення та шпигунське програмне забезпечення, зараження комп'ютера та, отже, мережі.

• Безпека додатків. Важливо контролювати та захищати програми, які організації використовують для ведення свого бізнесу. Це правда, чи організація створює цю програму чи купує його, оскільки сучасні загрози зловмисного програмного забезпечення часто орієнтуються на з відкритим кодом та контейнерами, які організації використовують для створення програмного забезпечення та додатків.

• Поведінкова аналітика. Цей метод аналізує поведінку мережі та автоматично виявляє та сповіщає організації щодо ненормальної діяльності.

• Хмарна безпека. Хмарні постачальники часто продають додаткові засоби хмарної безпеки, які забезпечують можливості безпеки у своїй хмарі. Провайдер хмара керує безпекою своєї загальної інфраструктури та пропонує інструменти для користувача для захисту своїх екземплярів у загальній хмарній інфраструктурі. Наприклад, веб -сервіси Amazon надають групи безпеки, які контролюють вхідний та вихідний трафік, пов'язаний із додатком або ресурсом.

• Профілактика втрат даних (DLP). Ці інструменти контролюють дані, що використовуються, в русі та в спокої для виявлення та запобігання порушенням

даних. DLP часто класифікує найважливіші дані та ризики та навчає працівників у кращих практиках захисту цих даних. Наприклад, не надсилати важливі файли як вкладення в електронних листах - одна з таких найкращих практик.

• Безпека електронної пошти. Електронна пошта - одна з найбільш вразливих моментів у мережі. Співробітники стають жертвами фішингу та зловмисних програм, коли вони натискають на посилання електронною поштою, які таємно завантажують шкідливе програмне забезпечення. Електронна пошта - це також невпевнений метод надсилання файлів та конфіденційних даних, якими мимоволі займаються працівники.

• Брандмауер. Програмне забезпечення або прошивка перевіряє вхідний та вихідний трафік для запобігання несанкціонованого доступу до мережі. Брандмауери - одні з найбільш широко використовуваних інструментів безпеки. Вони розташовані в декількох областях в мережі. Брандмауери нового покоління пропонують підвищений захист від нападів на шарі та вдосконалену оборону зловмисного програмного забезпечення за допомогою вбудованої глибокої перевірки пакетів.

• Система виявлення вторгнень (IDS).Ідентифікатори виявляють несанкціоновані спроби доступу та позначають їх як потенційно небезпечні, але не видаляють їх. ІДС та система профілактики вторгнення (IPS) часто використовуються в поєднанні з брандмауером.

• Система профілактики вторгнень. IPS призначені для запобігання вторгнень, виявляючи та блокуючи несанкціоновані спроби отримати доступ до мережі.

• Захист мобільних пристроїв. Бізнес -додатки для смартфонів та інших мобільних пристроїв зробили ці пристрої важливою частиною мережевої безпеки. Моніторинг та контроль, які мобільні пристрої отримують доступ до мережі та те, що вони роблять колись підключення до мережі, має вирішальне значення для сучасної мережевої безпеки.

• Багатофакторна автентифікація (MFA).MFA-це просте для працевлаштування та все більш популярне рішення мережевої безпеки, яке вимагає

двох або більше факторів для перевірки ідентичності користувача. Прикладом цього є Google Authenticator, додаток, який генерує унікальні коди безпеки, які користувач вводить поряд із своїм паролем, щоб перевірити свою ідентичність.

• Сегментація мережі. Організації з великими мережами та мережевим трафіком часто використовують сегментацію мережі для розбиття мережі на менші, простіші для управління сегментами. Цей підхід надає організаціям більше контролю та підвищення видимості в потоці руху. Безпека промислової мережі - це підмножина сегментації мережі, що забезпечує підвищення видимості в системах промислового управління (ICS). ICS більше ризикує для кіберзагроз через посилення інтеграції з хмарою.

• Пісочниця. Цей підхід дозволяє організаціям сканувати зловмисне програмне забезпечення, відкривши файл в ізольованому середовищі, перш ніж надати йому доступ до мережі. Після відкриття в пісочниці організація може спостерігати, чи діє файл зловмисно, чи показує будь -які вказівки на зловмисне програмне забезпечення.

• Інформація про безпеку та управління подіями (SIEM). Ця техніка управління безпекою записує дані з додатків та мережевих апаратних засобів та монітори для підозрілої поведінки. Коли виявлена аномалія, система SIEM попереджає організацію та вживає інших відповідних дій.

• Визначений програмним визначеним периметром (SDP).SDP - це метод безпеки, який сидить на вершині мережі, яку він захищає, приховуючи його від зловмисників та несанкціонованих користувачів. Він використовує критерії ідентичності для обмеження доступу до ресурсів та формує віртуальну межу навколо мережевих ресурсів.

• Віртуальна приватна мережа (VPN).VPN забезпечує зв’язок від кінцевої точки до мережі організації. Він використовує протоколи тунелювання для шифрування інформації, яка надсилається по менш безпечній мережі. VPN з віддаленим доступом дозволяють працівникам віддалено отримувати доступ до мережі своєї компанії.

• Веб-безпека. Ця практика контролює використання веб -сайтів працівників у мережі та пристроях організації, включаючи блокування певних загроз та веб -сайтів, а також захищає цілісність самих веб-сайтів організації.

• Бездротова безпека. Бездротові мережі є однією з найризикованіших частин мережі та потребують жорсткого захисту та моніторингу. Важливо дотримуватися найкращих практик бездротової безпеки, таких як сегментація користувачів Wi-Fi за допомогою ідентифікаторів набору послуг або SSID, а також використання аутентифікації 802.1x. Для забезпечення безпеки бездротової мережі також потрібні хороші інструменти моніторингу та аудиту.

• Безпека навантаження. Коли організації врівноважують навантаження між декількома пристроями в хмарних та гібридних середовищах, вони збільшують потенційні атакові поверхні. Заходи безпеки робочого навантаження та безпечні балансири навантаження мають вирішальне значення для захисту даних, що містяться в цих навантаженнях.

• Доступ до мережі нульової дотепності. Подібно до контролю доступу до мережі, нульовий дотепний доступ до мережі надає лише користувачеві, який вони повинні мати свою роботу. Це блокує всі інші дозволи.

Основні переваги безпеки мережі:

• функціональність. Мережева безпека забезпечує постійну високу продуктивність мереж, на які покладаються підприємства та окремі користувачі.

• конфіденційність та безпека. Багато організацій обробляють дані користувачів і повинні забезпечити конфіденційність, цілісність та доступність даних у мережі, відомої як Тріада ЦРУ. Безпека мережі запобігає порушенням безпеки, які можуть викрити конфіденційну інформацію, пошкодити репутацію бізнесу та призвести до фінансових втрат.

• Захист інтелектуальної власності. Інтелектуальна власність є ключовою для здатності багатьох компаній конкурувати. Забезпечення доступу до інтелектуальної власності, пов'язаної з продуктами, послугами та бізнес -стратегіями, допомагає організаціям підтримувати свою конкурентоспроможну перевагу.

• Відповідність. Дотримання правил безпеки та конфіденційності даних, таких як HIPAA та GDPR, юридично вимагається у багатьох країнах. Безпечні мережі є ключовою частиною дотримання цих мандатів.

Мережі містять шари, представлені моделлю взаємозв'язку відкритих систем (OSI). Дані проходять через ці шари, коли вони подорожують серед пристроїв, а різні кіберзагрози орієнтуються на різні шари. Тому кожен шар у стеку повинен бути забезпечений для того, щоб мережа вважалася захищеною.

Таблиця 1.1 відповідає рівнем OSI до відповідного типу мережевої безпеки.

Таблиця 1.1

Відповідність рівня OSI до типу безпеки

Рівні (ISO 7498-1)	ISO 7498-2 Модель безпеки
Прикладний	Аутентифікація
Представлення	Контроль доступу
Сеансовий	Непудація (Nonrepudiaton)
Транспортний	Цілісність даних
Мережевий	Конфіденційність
Канальний	Запевнення та доступність
Фізичний	Нотарізація та підпис

Зауважте, що третій рівень знизу називається мережевий, але мережева безпека не стосується лише цього шару. Кожен пристрій в комп'ютерній мережі функціонує на декількох шарах під час обробки інформації. Враховуючи це, кожен шар повинен бути безпечним для того, щоб мережа вважалася захищеною. Іншими словами, мережа Word у цьому визначенні мережевої безпеки широко стосується корпоративної інфраструктури в цілому, а не лише до мережевого рівня.

Наприклад, деякі люди можуть розрізняти хмарну безпеку та мережеву

безпеку. Хмарна безпека включає безпеку додатків та безпеку контейнерів, які існують поза мережевим шаром моделі OSI. Однак ці хмарні функції все ще можуть вважатися частиною загальної корпоративної мережі, а їх забезпечення є частиною мережевої безпеки.

Роботи, пов'язані з мережевою безпекою, включають наступне:

• Головні співробітники інформаційної безпеки (CISO) – одна з найвищих оплачуваних позицій у мережевій безпеці. CISO відповідає за розробку та реалізацію загальної програми безпеки інформації.

• Тестери проникнення, або тестери для пера, наймаються на проникнення в корпоративну мережу для викриття вразливості. Це можна автоматизувати або виконувати вручну працівниками або сторонніми тестуваннями ручки як постачальники послуг.

• Інженери безпеки зосереджуються на контролі якості в IT-інфраструктурі.

• Архітектори безпеки планують, аналізують, розробляють та перевіряють IT - інфраструктуру організації.

• Аналітики безпеки аналізують та планують стратегію безпеки, а також проводять аудит безпеки.

1.2. Типи загроз для безпеки мережі

Базовими поняттями інформаційної безпеки є загроза та атака. Загроза – це набір обставин і дій, які потенційно можуть призвести до порушення безпеки системи (до порушення її конфіденційності, повноцінності та доступності). Атака – це реалізована загроза.

Цілком можлива ситуація, коли система має певну вразливість, але ця вразливість ще не стала відомою зловмисникам — у цьому випадку відповідної загрози немає, а значить, і атака не може бути проведена. Аналогічно, існування загальновідомої загрози не тягне за собою жодної небезпеки для системи, в якій немає відповідної вразливості. Наприклад, поява інформації про деяку помилку в

коді ОС Windows може спричинити загрозу, але атака не здійсниться, якщо ця вразливість буде швидко усунута.

Таким чином, будь-яка загроза спрямована на пошук та використання вразливостей системи. У деяких випадках зловмисник працює «на дотик», намагаючись виявити той чи інший дефект системи. Система реагує на такі загрози видачею повідомлень про дрібні, але дивні неполадки, а також флуктуації в статистичних характеристиках роботи системи, на підставі яких адміністратор мережі або спеціаліст з безпеки може запідозрити підготовку атаки.

Рис. 1.2. Джерела загроз

Інші загрози виражаються в чіткій послідовності дій і мають формалізоване втілення у вигляді експлойту (exploit) — програми або просто послідовності командних рядків, деякої порції даних та/або покроковому описі дій, які, будучи виконаними, дозволяють зловмиснику скористатися певною конкретною вразливістю інформаційної системи у своїх інтересах. Особлива небезпека експлойта полягає в тому, що маючи його у своєму розпорядженні, навіть малопідготовлений хакер здатний провести успішну атаку. Для цього йому достатньо зайти на один із численних сайтів, які постачають усіх бажаючих своєю «продукцією». Більш того, на додаток до інструкцій та програм в Інтернеті можна знайти навіть пропозиції про здачу в оренду цілих бот-мереж, готових до реалізації потужних кібератак. У той же час наявність у експлойтів фіксованих ознак, таких,

наприклад, як специфічні кодові послідовності, полегшує розпізнавання та відображення відповідних атак.

Загрози можуть походити як від легальних користувачів мережі, так і від зовнішніх зловмисників. В останні роки у статистиці порушень безпеки зафіксовано різке зрушення від зовнішніх до внутрішніх загроз. Приблизно дві третини від загальної кількості всіх найбільш серйозних інцидентів, пов'язаних з безпекою, становлять порушення або помилки легальних користувачів мереж: співробітників та клієнтів підприємств, студентів, які мають доступ до мережі навчального закладу та ін.

Загрози з боку легальних користувачів можуть бути як навмисними, так і ненавмисними. До умисних загроз належать, наприклад, доступ та викрадення конфіденційних даних, моніторинг системи з метою отримання інформації про її пристрій, відвідування заборонених веб-сайтів, винесення за межі підприємства знімних носіїв тощо.

Безпека може бути порушена і внаслідок ненавмисних порушень користувачів та обслуговуючого персоналу — помилок, що призводять до пошкодження мережевих пристроїв, даних, програмного забезпечення, ОС та додатків, безтурботності у забезпеченні секретності паролів та ін. Відомо, що правильне конфігурування пристроїв є одним із потужних засобів забезпечення безпеки. Але виконана з помилками, ця операція здатна обернутися своєю протилежністю — загрозою. Як з'ясувалося, деякі «атаки» на ІС були насправді не атаками, а помилками адміністраторів мереж під час конфігурування елементів системи. Наприклад, широко відомий випадок неправильного конфігурування протоколу маршрутизації BGP в мережі клієнта провайдера AS7007, який призвів до відмов роботи великої частини Інтернету [2].

Загрози зовнішніх зловмисників, які також називають хакерами, за визначенням є навмисними і зазвичай кваліфікуються як злочини. Серед зовнішніх порушників безпеки зустрічаються люди, котрі займаються цією діяльністю професійно або просто з хуліганських спонукань.

Атаки поділяють на активні та пасивні. Активні атаки включають явні на систему, що змінюють її стан. Це можуть бути шкідливий програмний код-вірус, впроваджений у програму, що виконується системою, спотворення даних на сторінках зламаного веб-сайту, блокування мережевого сервісу шляхом бомбардування його помилковими запитами або впроваджене в комунікаційний протокол помилкове повідомлення. Головною відмінністю активних атак є те, що після свого завершення вони, як правило, залишають сліди.

Багато активних кібератак відносять до типу зламування (breaking-in) за аналогією з побутовим пограбуванням зі зломом, коли господар заходить у свій будинок і відразу виявляє пошкоджені замки, спустошені ящики та розкидані на підлозі речі. У комп'ютерній системі після активного проникнення зловмисника теж залишаються сліди «зламування»: наприклад, змінюється вміст пам'яті, надходять дивні діагностичні повідомлення, програми починають виконуватися неправильно, уповільнено або взагалі зависають, в характеристиках мережного трафіку та інших статистичних даних про роботу системи з'являються незрозумілі сплески активності.

Іноді грабіжник так добре «замітає сліди», що постраждалий може відразу й не помітити злочину, особливо якщо він не має спостережливості Шерлока Холмса або Еркюля Пуаро. Так і в інформаційній системі ретельно підготовлена активна атака може пройти непоміченою, якщо фахівці, які відповідають за її безпеку, погано обізнані про можливі наслідки таких атак. [3]

Пасивні атаки не порушують нормальну роботу, вони пов'язані зі збором інформації про систему, наприклад прослуховуванням внутрішньомережевого трафіку або перехопленням повідомлень, що передаються по лініях зв'язку. У багатьох випадках пасивні атаки не залишають слідів, тому їх дуже складно виявити, часто вони проходять непоміченими. Якщо використовувати військову аналогію, це розвідка (але не боєм).

Протиставлення активної та пасивної форм атак є деякою ідеалізацією. На практиці ми рідко маємо справу з активною чи пасивною атакою «у чистому вигляді». Найчастіше атака включає підготовчий етап збору інформації про систему,

що атакується, а потім на основі зібраних даних здійснюється активне втручання в її роботу. До корисної для хакера інформації відносяться типи ОС та додатків, IP-адреси, номери портів, імена та паролі користувачів. Частина такої інформації може бути отримана при аналізі відкритої інформації або простому спілкуванні з персоналом (це називають соціальним інжинірингом), а частина — за допомогою тих чи інших програм. В останньому випадку ми стикаємося з іншою послідовністю етапів: спочатку виконується активна фаза впровадження на атакований комп'ютер підслухуючої програми, потім період пасивного збору інформації (наприклад, паролів користувачів), а потім активна фаза проникнення в комп'ютер.

ВИСНОВКИ ДО РОЗДІЛУ 1

Успіх у сфері інформаційної безпеки може принести лише системний підхід, у якому узгоджено застосовуються засоби захисту різних типів: законодавчі, адміністративні, процедурні та технічні. Важливим напрямом законодавства, крім переслідування порушників у сфері безпеки, є стандартизація та ліцензування. Основу адміністративного рівня засобів безпеки становить безпекова політика, яка визначає стратегічні напрями інформаційного захисту підприємства.

Засоби безпеки процедурного рівня, основним інструментом яких є людина, вирішують завдання, поставлені адміністративним рівнем вище, з використанням технічних засобів, що надаються нижчим технічним рівнем. Технічний рівень включає підсистеми аутентифікації, авторизації та аудиту ОС, системи виявлення та запобігання вторгненням, антивірусні засоби, аналізатори мережевого трафіку та фаєрволи, а також інші найрізноманітніші програмні та апаратні засоби; ще до нього належать математичні методи, зокрема методи криптографії.

Процес побудови системи захисту має відповідати наступним універсальним принципам:

- Проєктування системи захисту має йти зверху донизу;
- Захист повинен бути безперервним, циклічним, проактивним процесом;

- Ефективний захист забезпечується шляхом резервування засобів безпеки;

- Ступінь захищеності системи вимірюється захищеністю її найслабшої ланки;

- При створенні системи безпеки необхідний компроміс між витратами та ризиками.

РОЗДІЛ 2
МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ПЕРИМЕТРА КОРПОРАТИВНОЇ МЕРЕЖІ

2.1. Архітектура корпоративної мережі

Комп'ютерні мережі будуються для задоволення потреб своїх клієнтів. Нижче описано три поширені типи корпоративних мереж:

- Мережі доступу для університетських містечок і філій створені для залучення користувачів і інших речей, наприклад для підключення співробітників в офісній будівлі.

- Мережі для центрів обробки даних з’єднують сервери, на яких розміщені дані та програми, і роблять їх доступними для користувачів.

- Глобальні мережі (WAN) з’єднують користувачів із програмами, іноді на великих відстанях, наприклад, з’єднують працівників лікарень із програмами охорони здоров’я.

Ці та всі інші мережі стикаються з різними загрозами безпеці, від яких їм потрібно захищатися. Щоб задовольнити ці різноманітні вимоги, усі типи мереж мають унікальну архітектуру.

Сьогодні, щоб задовольнити гострі потреби, викликані технологічним прогресом та ініціативами цифрової трансформації, мережі покликані робити більше.

Мережі доступу мають розпізнавати, автентифікувати та авторизувати користувальницькі пристрої та інтелектуальні пристрої, перш ніж підключити їх. Мережі центрів обробки даних потребують підключення додатків у кількох центрах обробки даних і хмарах [4].

Глобальні мережі повинні мінімізувати витрати та покращити взаємодію з користувачами під час обслуговування розподілених програм для розподілених

користувачів.

Мережі також мають бути динамічними, гнучкими та відповідати потребам бізнесу. Традиційні, інтенсивні вручну методи керування комп'ютерними мережами виявляються нежиттєздатними. Потрібні нові підходи, які вимагають трансформаційних змін у архітектурі мереж.

Протягом багатьох років основним фокусом корпоративних мереж було підключення всіх і всього до локальних централізованих центрів обробки даних, де зберігалися дані та запускалися програми. Цей доступ забезпечувався шляхом підключення користувачів і пристроїв до локальної мережі в корпоративному офісі. Локальна мережа кожного офісу була з'єднана з іншими офісами через глобальну мережу великого підприємства, яка зазвичай створювалася за допомогою виділених маршрутів багатопротокольної комутації міток (MPLS).

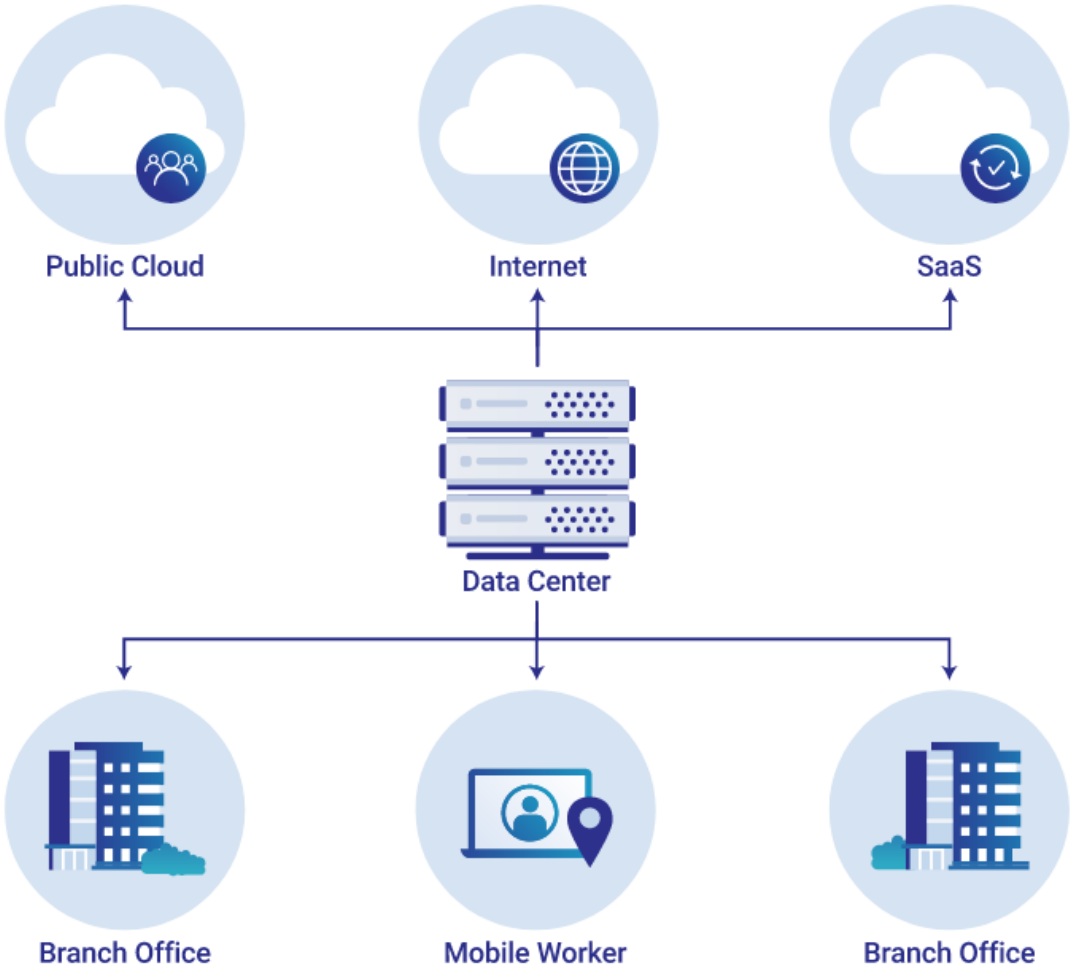

Рис. 2.2. Інфраструктура корпоративної мережі

Інфраструктура корпоративної мережі складається з фізичних пристроїв, підключених один до одного та до персональних комп'ютерів, принтерів і пристроїв Інтернету речей за допомогою комбінації кабелів Ethernet і сигналів WiFi. Пристрої, що можуть використовуватиьс для побудови мережі:

- Маршрутизатори надсилають дані з однієї мережі в іншу, забезпечуючи підключення між мережами та доступ до Інтернету.

- Комутатори пересилають дані в мережі на окремі пристрої.

- Шлюзи забезпечують з'єднання між різними мережами за допомогою кількох протоколів і на кількох рівнях моделі OSI.

- Брандмауери обробляють весь трафік, що надходить і виходить з мережі, щоб блокувати потенційні атаки.

- Балансувальники навантаження розподіляють мережевий трафік між декількома серверами в центрі обробки даних, щоб уникнути перевантаження сервера (балансувальники навантаження можуть робити те саме для веб-додатків).

- VPN-сервери встановлюють і припиняють VPN-з'єднання, щоб забезпечити безпечний доступ до внутрішньої мережі.

2.2. Проксі-сервери

Проксі-сервер (також відомий як «проксі» в IT-колах) є посередником між кінцевим користувачем/комп'ютером та Інтернетом. Проксі-сервер діє як провідник трафіку. Залежно від того, де у вашій мережі знаходиться проксі-сервер (докладніше про це пізніше), він перевірятиме та направлятиме інтернет-трафік до/від користувача та запитуваної веб-адреси.

Проксі-сервери еволюціонували протягом багатьох років і пропонують функції та функції, що виходять за межі стандартного веб-трафіку. Багато проксі-серверів, які використовуються сьогодні, виступатимуть як головна лінія захисту для користувачів Інтернету, вирішуватимуть ключові випадки використання та

проблеми відповідності, такі як політика безпеки мережі та конфіденційності, а також допомагатимуть регулювати інтернет-трафік і використання.

Сучасний ринок складається з різних типів проксі-серверів. Незважаючи на схожість, назви та функції часто плутають і міняють місцями. Нижче наведено розбивку кількох поширених типів:

Повний проксі: зазвичай проксі, який перехоплює весь веб-трафік.

Прямий проксі: коли веб-запити кінцевого користувача пересилаються на проксі-сервер перед виходом в Інтернет, а відповіді повертаються через проксі-сервер, а потім назад до користувача для забезпечення конфіденційності, кращої видимості, контролю вмісту та захисту від загроз.

Зворотний проксі: зазвичай контрольна точка, розташована ближче до веб-ресурсів, що допомагає безпечно та ефективно розповсюджувати вміст із веб-сайту назад до запитувача. В основному використовується популярними веб-сайтами та кількома рішеннями CASB.

Варіанти використання: три причини використовувати проксі-сервер

Безпека: проксі-сервери можуть діяти як перша лінія захисту від зловмисної діяльності. Багато проксі-серверів дозволяють налаштувати параметри, щоб блокувати відомі сайти, які містять зловмисне програмне забезпечення, і шифрувати ваші дані під час їх переміщення в Інтернеті. Загальною практикою для сучасних організацій є поєднання проксі-сервера з брандмауером наступного покоління (NGFW) і віртуальною приватною мережею (VPN), гарантуючи, що віддалені користувачі завжди отримають доступ до Інтернету через проксі-сервер своєї організації, допомагаючи дотримуватися правил і стандартів компанії.

Конфіденційність: одним із ключових атрибутів проксі-сервера є можливість забезпечувати окремим особам і організаціям підвищену конфіденційність під час перегляду Інтернету. Деякі проксі навіть мають можливість змінювати IP-адресу користувача, забезпечуючи повну анонімність під час перегляду веб-сторінок.

Моніторинг Інтернет-трафіку/використання: проксі також є чудовим способом для організацій керувати вмістом і контролювати його, а також забезпечувати захист

від загроз для своїх користувачів. Якщо організація не хоче, щоб її співробітники переглядали/відвідували певні веб-сайти через свою мережу, вони можуть налаштувати параметри свого проксі-сервера, щоб заборонити доступ до таких сайтів.

Організації також можуть використовувати проксі-сервери для моніторингу та реєстрації запитів веб-трафіку, забезпечуючи видимість не лише годин пікової активності мережі, але й сайтів, які найчастіше запитуються.

- VPN-сервери встановлюють і припиняють VPN-з'єднання, щоб забезпечити безпечний доступ до внутрішньої мережі.

2.3. Пакетні фільтри

Фільтрація пакетів — це контроль доступу до мережі шляхом аналізу вхідних і вихідних пакетів і пропуску або зупинки їх на основі IP-адреси джерела та призначення. Фільтрування пакетів є одним із багатьох методів для реалізації брандмауерів безпеки. Фільтрування пакетів є одночасно інструментом і технікою, яка є основним будівельним блоком безпеки мережі.

У контексті мережі TCP/IP фільтр пакетів спостерігає за кожною окремою IP-дейтаграмою, декодує інформацію заголовка вхідного та вихідного трафіку, а потім або блокує передачу датаграми, або дозволяє їй пройти на основі вмісту адресу джерела, адресу призначення, порт джерела, порт призначення та/або статус з'єднання. Це базується на певних критеріях, визначених інструментом фільтрації пакетів. Провідні IP-маршрутизатори, включаючи Cisco, Bay і Lucent, можна налаштувати для фільтрації IP-дейтаграм. Багато операційних систем можна налаштувати для фільтрації пакетів. Фільтрування пакетів можна додати до операційних систем *nix. Практично всі комерційні брандмауери підтримують фільтрацію пакетів. Деякі комерційні брандмауери також мають можливість фільтрації пакетів на основі стану попередніх пакетів (перевірка стану).

Фільтрування пакетів, як правило, недороге. Однак слід розуміти, що пристрій

фільтрації пакетів не забезпечує такий самий рівень безпеки, як брандмауер програм або проксі. Усі IP-мережі, крім найпростіших, складаються з IP-підмереж і містять маршрутизатори. Кожен маршрутизатор є потенційною точкою фільтрації. Оскільки вартість маршрутизатора вже поглинена, додаткові витрати на фільтрацію пакетів не потрібні. Фільтрування пакетів підходить там, де є скромні вимоги до безпеки. Внутрішні (приватні) мережі багатьох організацій не дуже сегментовані. Для ізоляції однієї частини організації від іншої не потрібні високоскладні брандмауери. Однак доцільно забезпечити певний захист виробничої мережі від лабораторії чи експериментальної мережі. Пристрій фільтрації пакетів є дуже відповідним заходом для забезпечення ізоляції однієї підмережі від іншої. Як працює фільтр пакетів? Усі фільтри пакетів функціонують однаково. Працюючи на мережевому та транспортному рівнях стеку протоколів TCP/IP, кожен пакет перевіряється, коли він надходить у стек протоколів. Мережні та транспортні заголовки ретельно перевіряються для отримання такої інформації:

• протокол (IP-заголовок, мережевий рівень) – у IP-заголовку байт 9 (кількість байтів починається з нуля) визначає протокол пакета. Більшість фільтруючих пристроїв мають можливість розрізняти TCP, UPD і ICMP.

• адреса джерела (IP-заголовок, мережевий рівень) – адреса джерела – це 32-розрядна IP-адреса хоста, який створив пакет.

• адреса призначення (IP-заголовок, мережевий рівень) – адреса призначення – це 32-розрядна IP-адреса хоста, для якого призначено пакет.

• вихідний порт (заголовок TCP або UDP, транспортний рівень) – кожен кінець мережевого підключення TCP або UDP прив’язаний до порту. Порти TCP є окремими та відмінними від портів UDP. Порти з номерами нижче 1024 зарезервовані – вони мають спеціально визначене використання. Порти з номерами вище 1024 (включно) відомі як ефемерні порти. Їх можна використовувати на вибір постачальника. Щоб отримати список «добре відомих» портів, зверніться до RFP1700. Вихідний порт — це псевдовипадково призначений ефемерний номер порту. Тому часто не дуже корисно фільтрувати вихідний порт.

• порт призначення (заголовок TCP або UDP, транспортний рівень) – номер порту призначення вказує на порт, на який надсилається пакет. Кожна служба на хості призначення прослуховує порт. Деякі добре відомі порти, які можуть бути відфільтровані, це 20/TCP і 21/TCP - ftp-з'єднання/дані, 23/TCP - telnet, 80/TCP - http і 53/TCP - передача зон DNS.

• статус з’єднання (заголовок TCP, транспортний рівень) – статус з’єднання вказує, чи є пакет першим пакетом мережевого сеансу. Біт ACK у заголовку TCP встановлюється на «false» або 0, якщо це перший пакет у сеансі. Дуже просто заборонити хосту встановлювати з’єднання, відхиляючи або відкидаючи будь-які пакети, у яких біт ACK встановлено на «false» або 0.

Фільтруючий пристрій порівнює значення цих полів з правилами, які були визначені, і на основі значень і правил пакет або пропускається, або відхиляється. Багато фільтрів також дозволяють визначити додаткові критерії з канального рівня, такі як мережевий інтерфейс, де має відбуватися фільтрація.

2.4. Шлюзи прикладного рівня

Шлюз прикладного рівня (ALG) — це програмний компонент, призначений для керування певними протоколами, такими як протокол ініціації сеансу (SIP) або FTP, наприклад на пристроях Juniper Networks під керуванням ОС Junos. Модуль ALG відповідає за обробку пакетів на комутаторах з урахуванням прикладного рівня.

Функціональність ALG може бути запущена службою або програмою, налаштованою в політиці безпеки:

• Служба — це об’єкт, який ідентифікує протокол програми за допомогою інформації рівня 4 (наприклад, стандартних і прийнятних номерів портів TCP і UDP) для служби програми (наприклад, Telnet, FTP і SMTP).

• Програма визначає програму рівня 7, яка відображається на службу рівня 4.

Попередньо визначена служба вже має відображення до програми рівня 7.

Однак для спеціальних служб ви повинні явно пов’язати службу з програмою, особливо якщо ви хочете, щоб політика застосовувала ALG.

ALG для пакетів, спрямованих на добре відомі порти, запускаються типом служби. ALG перехоплює та аналізує вказаний трафік, розподіляє ресурси та визначає динамічні політики, щоб дозволити трафіку безпечно проходити через пристрій:

1. Коли пакет надходить на пристрій, модуль потоку пересилає пакет відповідно до правила безпеки, встановленого в політиці.

2. Якщо виявлено, що політика дозволяє пакет, призначається пов’язаний тип служби або тип програми та створюється сеанс для цього типу трафіку.

3. Якщо для пакета знайдено сеанс, збіг правил політики не потрібен. Модуль ALG запускається, якщо ця конкретна служба або тип програми потребує підтримуваної обробки ALG.

“ALG також перевіряє пакет на наявність вбудованої IP-адреси та інформації про порт у корисному навантаженні пакета та, якщо необхідно, виконує обробку трансляції мережевих адрес (NAT). Буфер повідомлень виділяється лише тоді, коли пакет готовий до обробки. Буфер звільняється після того, як пакет завершує обробку ALG, зокрема змінює корисне навантаження, виконує NAT, відкриває пінхол для нового з’єднання між клієнтом і сервером і передає дані між клієнтом і сервером, розташованими на протилежних сторонах Juniper Networks.

Максимальний розмір jbuf становить 9 Кб. Якщо розмір буфера повідомлення перевищує 9 Кб, усе повідомлення не може бути передано до обробника пакетів ALG. Це змушує наступні пакети в сеансі обходити обробку ALG, що призводить до збою транзакції. Оптимізацію буфера повідомлень ALG покращено, щоб зменшити споживання пам’яті [5].

ALG також відкриває ворота для IP-адреси та номера порту, щоб дозволити обмін даними для сеансів керування та даних. Сеанс керування та сеанс даних можуть бути об’єднані, щоб мати однакове значення часу очікування, або вони можуть бути незалежними.

Попередньо визначена служба вже має відображення до програми рівня 7. Однак для спеціальних служб ви повинні явно пов’язати службу з програмою, особливо якщо ви хочете, щоб політика застосовувала ALG. Коли ви застосовуєте попередньо визначені служби до своєї політики, трафік, що відповідає службі, буде надіслано до відповідної ALG для подальшої обробки. Однак за деяких обставин може знадобитися визначити спеціальні служби, щоб досягти наступного:

• Використовуйте обробник ALG для обробки спеціального трафіку із зазначеними клієнтом протоколами, портами призначення тощо.

• Дозволяти трафік, але обходити обробку ALG, коли трафік відповідає попередньо визначеним службам, які зв’язуються з ALG.

• Додати більше програм до поточного набору програм ALG.

2.5. Міжмережевий екран

Брандмауер або міжмережевий екран може діяти як фільтр пакетів. Він може працювати як позитивний фільтр, дозволяючи пропускати лише пакети, які відповідають певним критеріям, або як негативний фільтр, відхиляючи будь-який пакет, який відповідає певним критеріям. Залежно від типу брандмауера, він може перевіряти один або кілька заголовків протоколу в кожному пакеті, корисне навантаження кожного пакета або шаблон, створений послідовністю пакетів.

Брандмауер із фільтрацією пакетів застосовує набір правил до кожного вхідного та вихідного IP-пакету, а потім пересилає або відхиляє пакет (Малюнок 22.1b). Брандмауер, як правило, налаштований на фільтрацію пакетів, що йдуть в обох напрямках (від внутрішньої мережі та до неї). Правила фільтрації базуються на інформації, що міститься в мережевому пакеті:

• Source IP-адреса: IP-адреса системи, яка створила IP-пакет (наприклад, 192.178.1.1)

• IP-адреса призначення: IP-адреса системи, до якої намагається отримати IP-пакет (наприклад, 192.168.1.2)

• Адреса транспортного рівня джерела та призначення: номер порту транспортного рівня (наприклад, TCP або UDP), який визначає такі програми, як SNMP або TELNET

• Поле протоколу IP: визначає транспортний протокол

• Інтерфейс: для брандмауера з трьома або більше портами, з якого інтерфейсу брандмауера надійшов пакет або для якого інтерфейсу брандмауера призначено пакет

Фільтр пакетів зазвичай налаштовується як список правил на основі збігів із полями в заголовку IP або TCP. Якщо є відповідність одному з правил, це правило викликається, щоб визначити, пересилати чи відхиляти пакет. Якщо немає відповідності жодному правилу, виконується дія за замовчуванням.

Можливі дві політики за умовчанням:

• За замовчуванням = відхилити: те, що прямо не дозволено, заборонено.

• За замовчуванням = вперед: те, що прямо не заборонено, дозволено.

2.6. Системи виявлення та запобігання вторгненням

Виявлення вторгнень — це процес моніторингу подій, що відбуваються в комп'ютерній системі чи мережі, та аналізу їх на наявність ознак можливих інцидентів, які є порушеннями або неминучою загрозою порушення політик комп'ютерної безпеки, політик прийнятного використання або стандартних практик безпеки.

Система виявлення вторгнень (IDS) — це програмне забезпечення, яке автоматизує процес виявлення вторгнень. Система запобігання вторгненням (IPS) — це програмне забезпечення, яке має всі можливості системи виявлення вторгнень і може також намагатися зупинити можливі інциденти.

Технології IDS і IPS пропонують багато однакових можливостей, і адміністратори зазвичай можуть вимкнути функції запобігання в продуктах IPS, змушуючи їх функціонувати як IDS. Відповідно, для стислості термін системи

виявлення та запобігання вторгненням (IDPS) використовується для позначення технологій IDS і IPS. Будь-які винятки окремо зазначаються. Він пояснює ключові функції, які виконують технології IDPS, і методології виявлення, які вони використовують. Далі висвітлюються найважливіші характеристики кожного з основних класів технологій IDPS.

IDPS в першу чергу зосереджені на виявленні можливих інцидентів. Наприклад, IDPS може виявити, коли зловмисник успішно скомпрометував систему, використовуючи вразливість у системі. IDPS буде реєструвати інформацію про діяльність і повідомляти про інцидент адміністраторам безпеки, щоб вони могли ініціювати дії реагування на інцидент, щоб мінімізувати шкоду. Багато IDPS також можуть бути налаштовані на розпізнавання порушень політики прийнятного використання та інших політик безпеки — наприклад, використання заборонених програм однорангового обміну файлами та передача великих файлів бази даних на знімні носії або мобільні пристрої. Крім того, багато IDPS можуть ідентифікувати розвідувальну діяльність, яка може вказувати на неминучість атаки або на те, що певна система чи характеристика системи становить особливий інтерес для зловмисників. Інше використання IDPS полягає в тому, щоб краще зрозуміти загрози, які вони виявляють, зокрема частоту та характеристики атак, щоб можна було визначити відповідні заходи безпеки. Деякі IDPS також можуть змінювати свій профіль безпеки, коли виявляється нова загроза. Наприклад, IDPS може збирати більш детальну інформацію для певного сеансу після виявлення зловмисної активності в цьому сеансі.

Технології IPS відрізняються від технологій IDS однією ознакою:

Технології IPS можуть реагувати на виявлену загрозу, намагаючись запобігти її успіху. Вони використовують кілька прийомів реагування, які можна розділити на такі групи:

• IPS сама зупиняє атаку. Приклади того, як це можна зробити, включають IPS, що розриває мережеве з’єднання, яке використовується для атаки, і IPS, що блокує доступ до цілі з облікового запису користувача, IP-адреси чи іншого атрибута

зловмисника.

• IPS змінює середовище безпеки. IPS може змінити конфігурацію інших засобів захисту, щоб перешкодити атаці. Типовими прикладами є перенастроювання IPS мережевого брандмауера для блокування доступу зловмисника або цілі, а IPS змінює брандмауер на основі 2 хостів на цілі для блокування вхідних атак. Деякі IPS можуть навіть спричинити застосування патчів до хосту, якщо IPS виявляє, що хост має вразливі місця.

• IPS змінює зміст атаки. Деякі технології IPS можуть видалити або замінити шкідливі частини атаки, щоб зробити її доброякісною. Простим прикладом є IPS, який видаляє заражений вкладений файл із електронного листа, а потім дозволяє очищеному електронному листу дістатися до одержувача.

Більш складним прикладом є IPS, який діє як проксі та нормалізує вхідні запити, що означає, що проксі перепаковує корисні навантаження запитів, відкидаючи інформацію заголовка. Це може спричинити відхилення певних атак в рамках процесу нормалізації.

2.7. Віртуальні приватні мережі

Віртуальні приватні мережі визначаються широко як спосіб розширення приватної мережі через загальнодоступну мережу, таку як Інтернет. Приватна мережа – це мережа, яка існує в локальній мережі (LAN). Розширення приватної мережі, яке здійснюється за допомогою технології VPN, можна використовувати для віддаленого доступу до інших приватних мереж за допомогою тунелю VPN. Тунель у мережі — це спосіб надсилання даних, які зазвичай не підтримуються мережевим протоколом, шляхом перепакування даних у пакет до іншого протоколу. Якщо на двох маршрутизаторах налаштовано тунелювання, можна інкапсулювати дані для безпосереднього надсилання один одному через Інтернет, а потім декапсулювати корисне навантаження, надіслане через тунель, щоб надіслати його далі до місця призначення.

VPN можна використовувати для зберігання конфіденційних даних у приватній мережі та забезпечення їх незмінності під час транспортування. Це додає додатковий рівень безпеки, не відкриваючи приватну мережу для публічного Інтернету, але водночас дає змогу отримати доступ до приватної мережі віддалено.

На рис. 2.7 наведено перший приклад типу VPN, він називається хост-мережа або віддалений доступ. Як випливає з назви, він використовується для підключення одного комп'ютера до приватної мережі, наприклад, віддаленого працівника, якому потрібен доступ до приватних файлів компанії в мережі компанії.

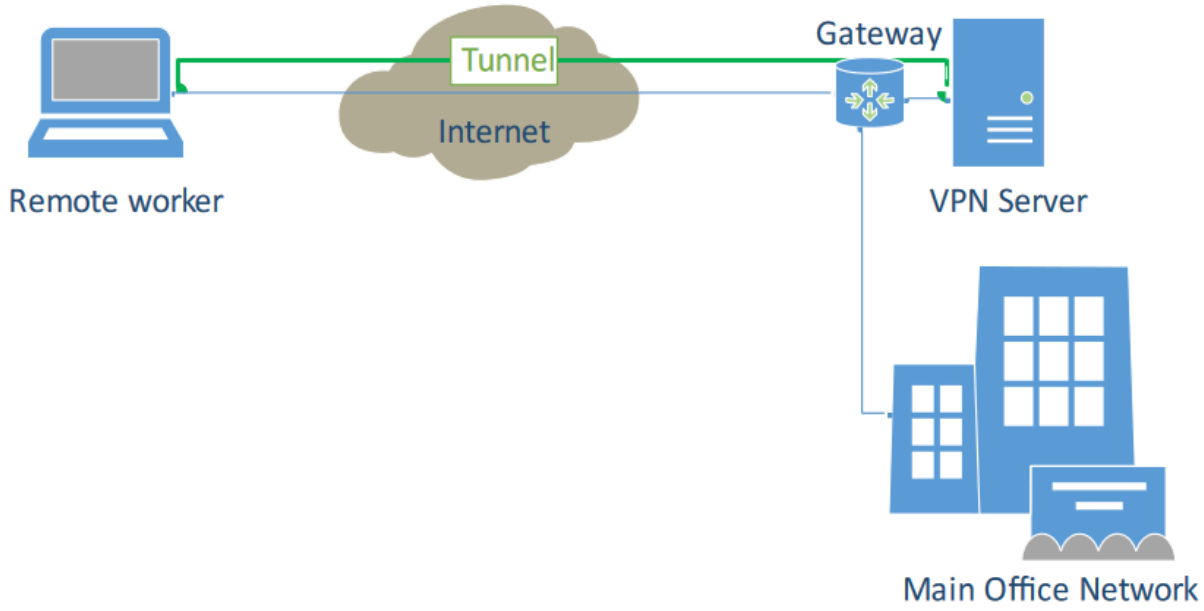

Рис. 2.7. Тип VPN віддаленого доступу

На рис. 2.8 показано мережу типу «сайт-сайт», яка використовується для з'єднання приватних мереж двох філій однієї компанії для спільного використання їхньої локальної приватної мережі та даних. Також можна використовувати цей тип VPN між двома різними компаніями чи організаціями для співпраці.

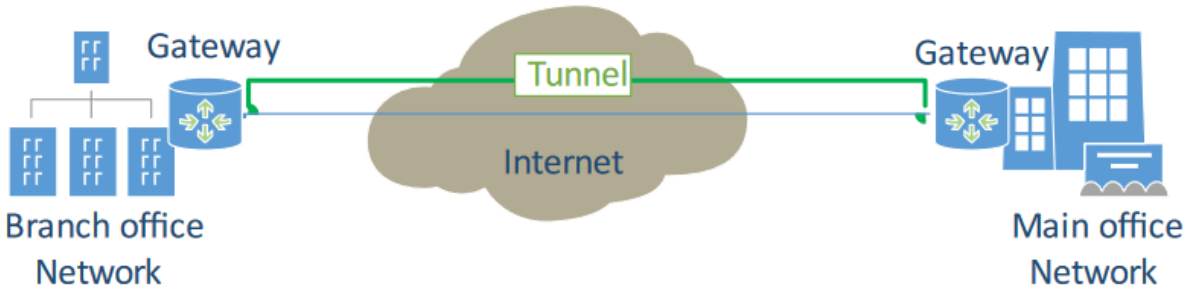

Рис. 2.8. Тип VPN типу "сайт-сайт"

Одна з причин використання VPN полягає в тому, що вона додає аспекти безпеки до мережевого з’єднання. Безпека в даному випадку означає захист мережевого трафіку щодо конфіденційності, цілісності та автентифікації. Конфіденційність досягається за допомогою шифрування. Якщо хтось отримає доступ до зашифрованих пакетів, надісланих через тунель VPN, він побачить лише зашифровані дані, які неможливо прочитати. Залежно від того, який тип шифрування використовується, його може бути дуже важко розшифрувати. Цілісність досягається за допомогою механізмів, які виявляють будь-які пакети підроблених. VPN використовують низку криптографічних алгоритмів і протоколів, щоб додати, наприклад, механізми автентифікації, щоб обмежити, хто може ними користуватися. Існує багато різних рівнів безпеки, які можна забезпечити різними програмами VPN. Іншою причиною використання VPN є віддалений доступ до інших приватних мереж, як показано на рисунках 2.7 і 2.8.

ВИСНОВКИ ДО РОЗДІЛУ 2

В другому розділі кваліфікаційної роботи були розібрані методи та засоби захисту периметра корпоративної мережі. Комп'ютерні мережі будуються для задоволення потреб своїх клієнтів. Мережі доступу мають розпізнавати, автентифікувати та авторизувати користувальницькі пристрої та інтелектуальні пристрої, перш ніж підключити їх.

Організації використовують проксі-сервери для моніторингу та реєстрації запитів веб-трафіку, забезпечуючи видимість не лише годин пікової активності мережі, але й сайтів, які найчастіше запитуються. У контексті мережі TCP/IP фільтр пакетів спостерігає за кожною окремою IP-дейтаграмою, декодує інформацію заголовка вхідного та вихідного трафіку, а потім або блокує передачу датаграми, або дозволяє їй пройти на основі вмісту адресу джерела, адресу призначення, порт джерела, порт призначення та/або статус з’єднання. Фільтруючий пристрій порівнює значення цих полів з правилами, які були визначені, і на основі значень і правил пакет або пропускається, або відхиляється.

Шлюз прикладного рівня — це програмний компонент, призначений для керування певними протоколами, такими як протокол ініціації сеансу або FTP. Брандмауер із фільтрацією пакетів застосовує набір правил до кожного вхідного та вихідного IP-пакету, а потім пересилає або відхиляє пакет. Фільтр пакетів зазвичай налаштовується як список правил на основі збігів із полями в заголовку IP або TCP. Якщо є відповідність одному з правил, це правило викликається, щоб визначити, пересилати чи відхиляти пакет.

Система виявлення вторгнень автоматизує процес виявлення вторгнень, а система запобігання вторгненням має всі можливості системи виявлення вторгнень і може також намагатися зупинити можливі інциденти. IDPS в першу чергу зосереджені на виявленні можливих інцидентів. Крім того, багато IDPS можуть ідентифікувати розвідувальну діяльність, яка може вказувати на неминучість атаки або на те, що певна система чи характеристика системи становить особливий інтерес

для зловмисників. Одна з причин використання VPN полягає в тому, що вона додає аспекти безпеки до мережевого з’єднання. Безпека в даному випадку означає захист мережевого трафіку щодо конфіденційності, цілісності та автентифікації. Конфіденційність досягається за допомогою шифрування, бо VPN використовують низку криптографічних алгоритмів і протоколів, щоб додати, наприклад, механізми автентифікації, щоб обмежити, хто може ними користуватися.

РОЗДІЛ 3
СИСТЕМА ЗАХИСТУ ПЕРИМЕТРУ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ D-LINK

3.1. Операційна система D-Link NetDefendOS

Оскільки можливості міжмережевого екрану D-Link DFL-1600 дуже великі, надано короткі описи основних функцій і більш поглиблені тим функціям та протоколам, які використовувалися при написанні цієї кваліфікаційної роботи.

Операційна система D-Link NetDefendOS (далі NetDOS) є базовим програмним забезпеченням, яке необхідне управління міжмережевими екранами D-Link з розширеними можливостями.

NetDOS розроблена як мережева операційна система, забезпечує широку смугу пропускання з гарною надійністю та малим кроком зміни смуги. На відміну від продуктів, що використовують іншу операційну систему, наприклад Unix або Microsoft Windows, NetDOS дає можливість вільної інтеграції підсистем, докладний контроль над усіма можливостями та зниження загрози атаки.

Об'єкти NetDOS з погляду системного адміністратора, сучасний підхід NetDOS дозволяє візуалізувати операції використанням низки логічних блоків чи об'єктів, які дозволяють налаштовувати пристрій майже нескінченним числом образів. Маленький крок керування дозволяє системному адміністратору виставити необхідні налаштування у різних мережах.

Основні можливості NetDOS - мережна операційна система із широким вибором функцій. Нижче представлені основні з них:

IP Routing NetDOS - забезпечує такі опції IP-маршрутизації як статична маршрутизація, динамічна маршрутизація, а також можливість маршрутизації

multicast. Крім цього, NetDOS підтримує наступне, Virtual LAN, моніторинг маршрутів, Proxy ARP та Transparency.

Firewalling Policies NetDOS – надає перевірку пакетів SPI для широкого набору протоколів, включаючи TCP, UDP та ICMP. Адміністратор визначає докладні алгоритми комутатора на основі джерела/призначення мережі/інтерфейсу, протоколу, портів, атрибутів користувача (user credentials), часу дня і т.д.

Address Translation – для забезпечення функціоналу, а також безпеки, NetDOS підтримує передачу адрес на основі алгоритмів. Підтримується два види трансляцій: динамічна трансляція адрес (NAT) та статична трансляція адрес (SAT), що дозволяє здійснювати роботу в різних типах мереж.

VPN NetDOS – підтримує всі можливі варіанти реалізації Virtual Private Network (VPN). NetDefendOS підтримує VPN на основі протоколів IPsec, L2TP і PPTP і може працювати як сервер, так і клієнт для всіх типів VPN, і дає можливість абсолютно будь-якому алгоритму безпеки для кожного VPN-тунелю.

TLS Termination NetDOS – підтримує TLS Termination. Це дозволяє міжмережевим екранам D-Link здійснювати роботу як кінцева точка для хостів Web-браузера HTTP (ця функція іноді називається SSL termination).

Anti-Virus Scanning NetDOS – вбудований антивірус. Трафік, що проходить через комутатор D-Link, може піддаватися детальній перевірці на віруси, і адреси, що розсилають віруси, будуть заноситися до чорного списку і блокуватися.

Intrusion Detection and Prevention – дозволяє захистити від вторгнень і запобігає атакам рівня додатків. IDP engine працює за заданим алгоритмом і дозволяє виконувати повне сканування та виявити атаки. Що дозволяє блокувати і внести в чорний список атакуючі хости.

Web Content Filtering NetDOS – дає можливість різним механізмам фільтрації вмісту, який не відповідає алгоритму використання Web. Даний вміст блокується за категоріями, невідповідні об'єкти можуть бути видалені, а Web-сайти можуть бути додані до певного списку кількох алгоритмів.

Traffic Management NetDOS - надає зручні можливості для управління трафіком завдяки функціям таким, як Формування трафіку (Traffic Shaping), Правила порогів (Тільки для деяких моделей) і Балансування навантаження сервера (Server Load Balancing). Traffic Shaping надає обмеження та розподіл смуги пропускання; Threshold Rules надає специфікацію порогів для надсилання повідомлень про мережний трафік; Server Load Balancing дозволяє пристрою з NetDOS розподіляти навантаження в мережі.

Operations and Maintenance - управління NetDOS проводитися через інтерфейс командного рядка (CLI). NetDOS також дозволяє детально спостерігати за подіями та реєстрацією, а також можлива підтримка моніторингу через SNMP.

ZoneDefense NetDOS – також використовується в управлінні комутаторами D-Link завдяки функції ZoneDefense. Ця функція дозволяє NetDOS блокувати ділянки мережі, в яких є джерело зараженого трафіку.

3.2. Структурні елементи NetDefendOS

Основними складовими елементами в NetDOS є інтерфейси, логічні об'єкти та правила.

Інтерфейси виконують роль "входів" для вихідного та вхідного трафіку, що проходить через NetDOS. За відсутності даних інтерфейсів у системи NetDOS немає можливості отримувати чи надсилати дані.

Типи інтерфейсів:

- Фізичні інтерфейси - актуальний фізичний Ethernet-порт.

- Під-інтерфейси (sub-interfaces) – інтерфейси VLAN та PPPoE.

- Інтерфейси тунелювання – відправлення та отримання даних через VPN-тунелі.

Симетричний інтерфейс. Дизайн інтерфейсу NetDOS симетричний, і виходить, що інтерфейси пристрою нестійкі і є незахищеними зовні або захищеними всередині і залежать тільки від адміністратора.

Логічні об'єкти. Логічні об'єкти - це певні елементи, які у наборах правил. Адреса, наприклад, містить призначені об'єкти, такі як хост і мережні адреси. Іншим прикладом логічних об'єктів виступають послуги, які надають певні протоколи та порти. Крім цього, у важливій ролі виступають об'єкти Application Layer Gateway (ALG), необхідні визначення додаткових параметрів у певних протоколах, як-от HTTP, FTP, SMTP і H.323.

Набори правил NetDefendOS:

Зрештою, правила, задані адміністратором у різні комплекти правил (rule sets) необхідні фактичного застосування алгоритмів безпеки NetDOS. Основним комплектом правил є IP-правила (IP Rules), які використовуються для визначення алгоритмів IP-фільтрації рівня 3, а також для перенаправлення та балансування навантаження сервера. Правила створення трафіку (Traffic Shaping Rules) визначають алгоритм керування смугою пропускання, правила IDP дозволяють захистити мережу від вторгнення тощо.

Основні принципи використання NetDOS:

1) Ethernet-фрейм видається одному з Ethernet-интерфейсов системи. Проводиться перевірка базового Ethernet-фрейму і, якщо кадр не допускається, пакет буде відкинуто.

2) Пакет порівнюється з інтерфейсом джерела. Інтерфейс джерела ідентифікується так:

- Якщо Ethernet-фрейм містить ідентифікатор VLAN ID (Virtual LAN identifier) (ідентифікатор віртуальної локальної мережі), порівнюється конфігурація VLAN-інтерфейсу з відповідним VLAN ID. У разі відповідності VLAN інтерфейс стає інтерфейсом пакета. Якщо відповідності немає, пакет не допускається, а подія заноситься до журналу.

- Якщо Ethernet-фрейм містить дані PPP, система виконується перевірка відповідності з PPPoE-інтерфейсом. Якщо відповідність має місце, інтерфейс стає інтерфейсом джерела пакета. В іншому випадку пакет не допускається, а подія реєструється.

- Якщо нічого з перерахованого вище не відбувається, то інтерфейсом джерела пакету стає Ethernet-інтерфейс.

3) IP-датаграма з пакета передається на пристрій, що перевіряє NetDOS, який виконує перевірку пакета на помилки, включаючи перевірку контрольної суми, прапорів протоколу, довжини пакета і т.д. Якщо помилка є, пакет відкидається і заноситься до журналу.

4) NetDOS здійснює пошук існуючого з'єднання, порівнюючи параметри вхідного пакета, включаючи інтерфейс джерела, IP-адреси джерела та призначення та IP-протокол. Якщо відповідності немає, відбувається процес встановлення з'єднання. Якщо є відповідність, процес відбувається з кроку 10.

5) Правила доступу (Access Rules) визначають, чи дозволена IP-адреса джерела. Якщо дозволено, у таблиці маршрутизації відбувається пошук зворотного маршруту (reverse route lookup). Інакше, спочатку, інтерфейс прийматиме лише IP-адреса джерела, що належить мережі даного інтерфейсу. Пошук зворотного маршруту (reverse lookup) виконується з метою підтвердити існування маршруту використання інтерфейсу, якщо мережа є мережею призначення. У тому випадку, коли пошук правила доступу або зворотний пошук маршруту визначають, що IP джерела є помилковим, пакет не допускається і реєструється в журналі.

6) Пошук маршруту відбувається у відповідній таблиці маршрутизації. Інтерфейс призначення визначено заздалегідь.

7) Визначаються IP-правила, яким відповідають характеристики пакета. Використовуються такі характеристики:

-інтерфейси джерела та призначення;

-Мережа джерела та призначення;

-IP-протокол (наприклад, TCP, UDP, ICMP);

-TCP/UDP-порти;

-Типи ICMP-пакетів;

-Час дії правила за розкладом.

Якщо відповідності немає, пакет не допускається.

Якщо правило знайдено, що відповідає новому з'єднанню, параметр правила Action призначає дії системи NetDOS по відношенню до з'єднання. Якщо призначено дію Drop (Відхилити), пакет не допускається, а подія заноситься до журналу. Якщо призначено дію Allow (Дозволити), пакет проходить через систему. Відповідний стан буде занесено в таблицю з'єднань для порівняння з наступними пакетами, що належать до того ж з'єднання. Також об'єкт служби, пов'язані одним або декількома IP-протоколами з відповідними номерами портів, може бути пов'язаний з об'єктом Application Layer Gateway (ALG). Ці дані застосовуються для того, щоб система NetDOS керувала відповідними додатками для забезпечення обміну інформацією. В результаті, нове з'єднання буде занесено до журналу.

Існують також додаткові дії, наприклад, переадресація та балансування навантаження сервера.

8) Правила виявлення та запобігання вторгненням (Intrusion Detection and Prevention (IDP) Rules) оцінюються за аналогією з IP-правилами. Якщо знайдено відповідність, дані реєструються. Таким чином, система NetDOS знатиме про виконання сканування всіх пакетів, що належать до цього з'єднання.

9) Аналізується Формування трафіку (Traffic Shaping) та Правило обмеження порога (Threshold Limit rule). Якщо є відповідність, то інформація реєструється. Отже, здійснюється управління трафіком.

10) За наявності інформації система NetDOS вирішує, яку дію використовувати до пакету:

- За наявності даних ALG та виконання IDP-сканування дані пакета перевіряються підсистемою псевдоскладання TCP, яка у свою чергу використовує різні ALG, механізми зчитування вмісту на 7 рівні тощо.

- Якщо вміст пакета закодований (за допомогою протоколу IPsec, PPTP/L2TP або іншого типу протоколу тунелювання), здійснюється перевірка списків інтерфейсів на відповідність.

- Якщо виявлено відповідність, пакет декодується і дані (незашифрований текст) відправляються назад у NetDOS, але з інтерфейсом джерела, що відповідає

інтерфейсу тунелювання.

- За наявності інформації про керування трафіком, пакет визначаться в чергу або виконується дія згідно з заданими налаштуваннями.

11) У результаті пакет буде відправлено на інтерфейс призначення відповідно до його стану. Якщо інтерфейс призначення є інтерфейсом тунелювання або фізичним підінтерфейсом, виконується додаткова обробка даних, наприклад, кодування або інкапсуляція.

3.3. Управління NetDefendOS

Система NetDOS виконує керування доступом на основі набору IP-правил, в якому діапазон захищених LAN-адрес розглядається як довірені хости. При цьому потік трафіку з неперевірених ресурсів довірені хости обмежується. Перед перевіркою нового з'єднання на відповідність набору IP-правил, система NetDOS здійснює перевірку джерела з'єднання на відповідність «Правилам доступу». «Правила доступу» використовуються для того, щоб визначити джерело трафіку на певному інтерфейсі та для автоматичної заборони пакетів з певних джерел. Правила доступу забезпечують ефективну та спрямовану фільтрацію нових спроб з'єднання.

IP Spoofing. Зловмисник змінює IP-адресу пакетів, що йдуть із довіреного хоста, з метою обману системи безпеки міжмережевого екрану. Така атака називається Spoofing. IP spoofing – одна з найпоширеніших атак spoofing. Зловмисники використовують IP-адреси дозволених хостів, щоб «обійти» фільтрацію. У заголовку IP-пакета вказується адреса джерела пакета, змінена зловмисником і використовується як адреса локального хоста. Міжмережевий екран сприймає цей пакет як пакет довіреного джерела. Хоча джерело пакета не має можливості відреагувати правильно, виникає загроза перевантаження мережі та створення всього необхідного для атак Denial of Service (DoS). Міжмережевий екран з підтримкою VPN дозволяє захиститись від атак spoofing, але у випадку, коли VPN не підходить, використовуються «Правила доступу», які забезпечують захист від

атак spoofing за рахунок ще одного фільтра, що використовується для перевірки адреси джерела. За допомогою «Правила доступу» можна переконатися, що пакети, що надійдуть на відповідний інтерфейс, не мають адреси джерела, пов'язаного з мережею іншого інтерфейсу. Іншими словами:

- Будь-який вхідний трафік з IP-адреси джерела, що належить локальному довіреному хосту, БЛОКУЄТЬСЯ.

- Будь-який вихідний трафік з IP-адреси джерела, що належить зовнішньої невідомої мережі, БЛОКУЄТЬСЯ.

Перше правило не дозволяє невизначеним особам використовувати адресу локального хоста як адресу джерела.

Друге правило, у свою чергу, захищає будь-який локальний хост від атак spoof.

Антивірусне сканування. Антивірусний модуль NetDOS дозволяє захиститись від шкідливого коду, що переноситься завантажувальними файлами. Файли можуть бути завантажені як частина Web-сторінки в передачі HTTP, завантаження FTP, або у вигляді вкладень в електронну пошту, що доставляють через SMTP. Шкідливий код у таких завантаженнях призначений для різних цілей, як і програми подразнюючого впливу до більш зловмисних дій, наприклад, отримання паролів, номерів кредитних карток та іншої особистої інформації. Термін "Вірус" використовується як загальний опис для всіх видів шкідливого коду, що переноситься файлами.

На відміну від функції виявлення та запобігання вторгненням (IDP), яка, в основному, застосовується при нападі на сервери, антивірусне сканування сконцентровано на завантаженнях, що виконуються клієнтами. Антивірус NetDOS розроблений як доповнення до стандартного антивірусу, яке зазвичай виконується локально спеціалізованим програмним забезпеченням, встановленим на клієнтських комп'ютерах. Функція IDP не призначена для повної заміни локального сканування, а є додатковою функцією для підвищення безпеки. Найголовніше, вона також може виступати як додаткова функція, за відсутності антивіруса у локального клієнта.

Вразливі сервери мають можливість стати жертвою таких атак як «хробаки», «трояни» та «backdoor», які отримують контроль над сервером. Загальний термін, який використовується для опису таких атак на сервер - intrusions (вторгнення).

Відмінність вторгнення від вірусів у цьому, що вірус, зазвичай, міститься у одному файлі, завантажуваним у систему клієнта. Вторгнення є шкідливими Інтернет-даними, завданням яких є «обійти» механізми безпеки сервера. Вторгнення не є рідкістю і може змінюватися, оскільки вони автоматично створюється атакуючим. NetDOS IDP дозволяє захиститися від подібних загроз. Виявлення та запобігання вторгненням (IDP) є підсистемою NetDOS, яка спрямована на захист від спроб вторгнення. Система діє шляхом моніторингу мережного трафіку, що проходить через міжмережевий екран NetDOS, пошуку шаблонів, які показують спробу вторгнення. Після виявлення вторгнення, NetDOS IDP виконує кроки з нейтралізації вторгнення та його джерела.

Запобігання атакам DoS. Використовуючи мережу Інтернет, підприємства набувають нових можливостей для бізнесу та зростання. Мережа підприємства та мережеві програми є необхідними для бізнесу.

3.4. Захист FTP-сервера за допомогою FTP ALG

File Transfer Protocol (FTP) – це протокол на основі TCP/IP, який використовується для обміну файлами між клієнтом та сервером. Клієнт запускає з'єднання, підключаючись до FTP-сервера. Для початку клієнт надає особисті дані, вводячи логін і пароль. Після проведення аутентифікації сервер виводить клієнту список файлів/папок, можливих для завантаження/завантаження (залежно від прав доступу). FTP ALG використовується для керування FTP-з'єднаннями через міжмережевий екран NetDefend.

Протокол FTP використовує два канали зв'язку: канал для розподілу команд і канал для розподілу даних. Для відкриття FTP-сесії FTP-клієнт повинен налаштувати TCP-з'єднання (канал управління) з портом 21 (за замовчуванням) на

сервері FTP. Далі проводиться налаштування режиму FTP.

FTP працює у двох режимах: активному та пасивному. За допомогою режиму визначається роль сервера при відкритті каналів для обміну даними між клієнтом і сервером.

В активному режимі FTP-клієнт відправляє команду на FTP-сервер, вказуючи IP-адресу та порт, до якого слід підключитися. FTP-сервер встановлює канал передачі даних назад до FTP-клієнту, використовуючи отриману інформацію.

У пасивному режимі FTP-клієнт відкриває з'єднання з FTP-сервером передачі команд. Для FTP-клієнтів рекомендується стандартний режим, хоча деякі рекомендації можуть бути протилежними. Активний та пасивний режими FTP не є безпечними для міжмережевих екранів NetDefend.

Якщо FTP-клієнт у внутрішній мережі підключається через міжмережевий екран до FTP-сервера в Інтернеті. Далі слід додавати IP-правило, щоб дозволити проходження пакетів FTP-клієнта на порт 21 FTP-сервера.

Коли використовується активний режим, система NetDefendOS не обізнана, що FTP-сервером здійснюється встановлення нового з'єднання назад до FTP-клієнта. Тому запит на вхідне з'єднання для встановлення каналу обміну даними буде відхилено. Через те, що номер порту, який використовується для каналу передачі даних, є динамічним, є лише одне рішення – дозволити трафік з усіх портів FTP-сервера на всі порти FTP-клієнта, що буде небезпечним.

Коли використовується пасивний режим міжмережевого екрану, не потрібний дозвіл на з'єднання з FTP - сервером. З іншого боку, система NetDefendOS, як і раніше, залишається необізнаною про те, який порт FTP-клієнт спробує використовувати для встановлення каналу передачі даних. Це означає, що потрібно дозволити трафік з усіх портів FTP-клієнта на всі порти FTP-сервера. Хоча це і не так небезпечно як при використанні активного режиму, потенційна загроза безпеці все ж таки існує. Тим більше, що не всі клієнти FTP підтримують пасивний режим.

Система FTP ALG NetDefendOS стосується питань безпеки при відновленні каналу TCP-потоку для передачі FTP-команд та перевірки його вмісту. У цьому

випадку система NetDefendOS знає лише про те, який порт відкритий для каналу передачі даних. Крім того, FTP ALG також надає набір функцій для фільтрації певних команд керування та забезпечення захисту від переповнення буфера.

На рисунку 3.2, FTP-сервер підключений до міжмережевого екрану NetDefend у зоні DMZ з приватними IP-адресами:

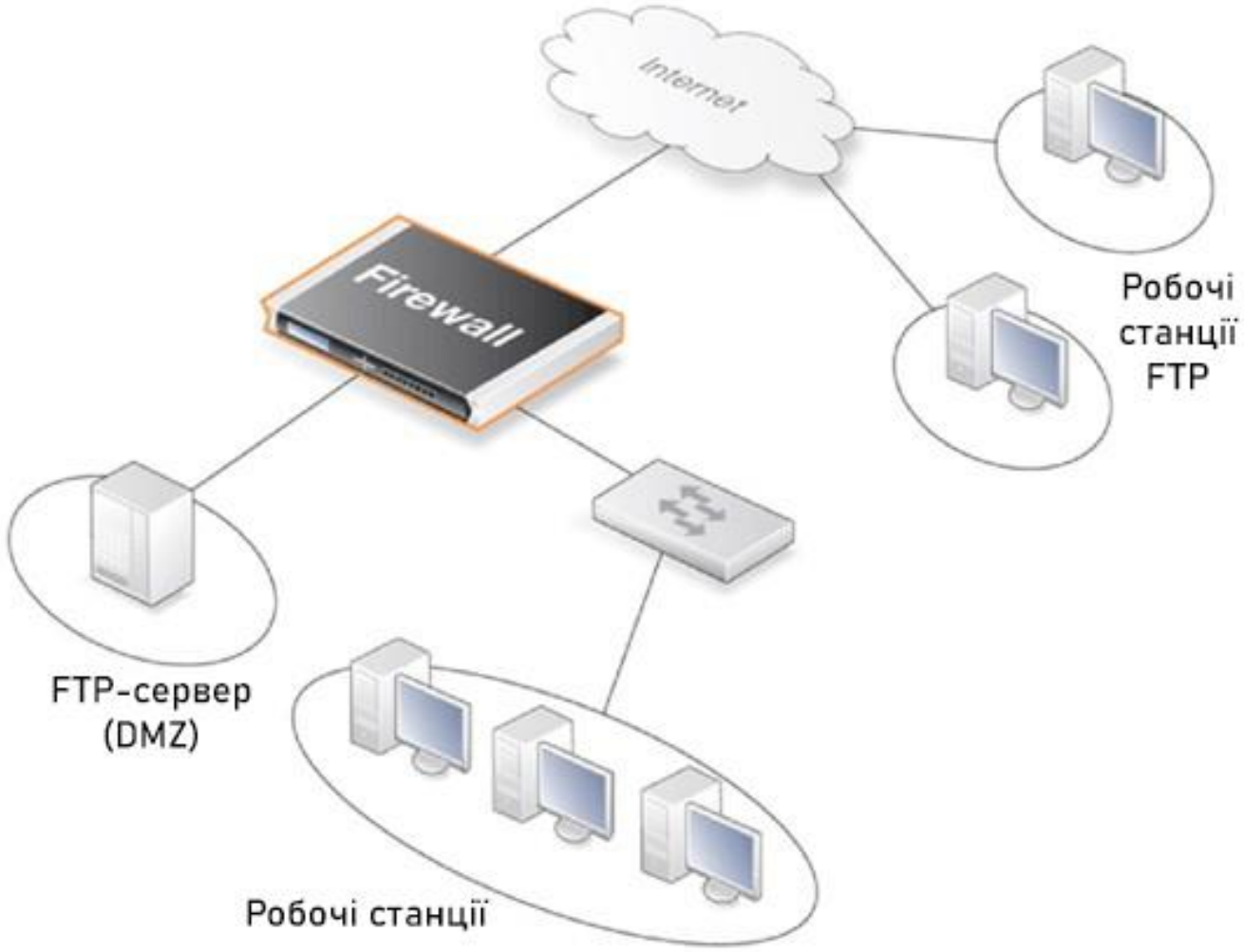

Рис. 3.2. Захист FTP-сервера міжмережевим екраном

У цьому випадку призначаються наступні обмеження FTP ALG.

• Увімкнено FTP ALG опцію Allow client to use active mode, таким чином, клієнти можуть використовувати як

активний, і пасивний режими.

• Вимкнено FTP ALG опцію Allow server для використання passive mode. Це забезпечує серверу вищий рівень безпеки, оскільки сервер не отримуватиме дані в

пасивному режимі. FTP ALG виконає переключення при підключенні клієнта, який використовує пасивний режим.

Налаштування виконується таким чином:

Web-інтерфейс

А. Визначено ALG:

1. Необхідно перейти до Objects > ALG > Add > FTP ALG

2. Введено Name: ftp-inbound

3. Вибрано поле Allow client to use active mode

4. Скасовано вибір поля Allow server to use passive mode

5. Підтвердження OK

Б. Визначено Service:

1. Необхідно перейти до Objects > Services > Add > TCP/UDP Service

2. Введено таке:

• Name: ftp-inbound-service

• Type: Вибрано TCP зі списку

• Destination: 21 (порт FTP-сервера)

• ALG: Вибрано ftp-inbound, створене вище

3. Підтвердження OK

Дозвіл з'єднання з публічною IP-адресою на порту 21 і перенаправлння на внутрішній FTP-сервер:

1. Необхідно перейти до Rules > IP Rules > Add > IPRule

2. Введено:

• Name: SAT-ftp-inbound

• Action: SAT

• Service: ftp-inbound-service

3. Для Address Filter введено:

• Source Interface: будь-який

• Destination Interface: core

• Source Network: all-nets

• Destination Network: wan_ip

4. Для SAT вибрано Translate the Destination IP Address

5. Введено To: New IP Address: ftp-internal (імовірно, ця внутрішня IP-адреса для FTP-сервера було визначено в об'єкті «Адресна книга»)

6. New Port: 21

7. Підтвердження OK

Г. Необхідно «натувати» трафік із внутрішнього інтерфейсу через одну публічну IP-адресу:

1. Необхідно перейти до Rules > IP Rules > Add > IPRule

2. Введено:

• Назви: NAT-ftp

• Action: NAT

• Service: ftp-inbound-service

3. Для Address Filter Введено:

• Source Interface: dmz

• Destination Interface: core

• Source Network: dmznet

• Destination Network: wan_ip

4. Для NAT Вибрано Use Interface Address

5. Підтвердження OK

Д. Дозвіл вхідних з'єднань (SAT потребує відповідного правила Allow):

1. Необхідно перейти до Rules > IP Rules > Add > IPRule

2. Введено:

• Назви: Allow-ftp

• Action: Allow

• Service: ftp-inbound-service

3. Для Address Filter Введено:

• Source Interface: будь-який

• Destination Interface: core

• Source Network: all-nets

• Destination Network: wan_ip

4. Підтвердження OK

3.5. Захист Web-сервера за допомогою HTTP ALG

Web-трафік є одним із найбільших джерел порушення безпеки та неправомірного використання мережі Інтернет. Перегляд веб-сторінок може спричинити загрозу безпеці мережі. Продуктивність та пропускна спроможність Інтернет-каналів також може бути порушена.

За допомогою HTTP ALG система NetDefendOS застосовує такі механізми фільтрації сумнівного Web-вмісту:

• Функція Active Content Handling може використовуватися для фільтрації Web-сторінок із вмістом, що розглядається адміністратором як потенційна загроза, наприклад, об'єкти ActiveX та Java Applets.

• За допомогою функції Static Content Filtering (Фільтрування статичного вмісту) можна вручну класифікувати веб-сайти на дозволені та заборонені. Ця функція також відома як «білий/чорний список» URL-адрес.

• Dynamic Content Filtering (Фільтрування динамічного вмісту) – це ефективна функція, яка дозволяє адміністратору дозволяти або блокувати доступ до Web-сайтів в залежності від категорії їх класифікації, виконаної службою автоматичної класифікації. Фільтрування динамічного вмісту вимагає мінімум зусиль адміністратора та забезпечує високу точність.

Web-вміст може містити шкідливий код, призначений для завдання шкоди робочої станції або мережі. Як правило, такий код вбудований у різні типи об'єктів або файли, які вбудовані на веб-сторінки.

Система NetDefendOS підтримує можливість видалення таких типів об'єктів з вмісту Web-сторінок:

• Об'єкти ActiveX (включаючи Flash)

• Java applets

• Код Javascript/VBScript

• Cookies

• Некоректне відображення символів при використанні кодування UTF-8 (некоректне відображення URL-адрес може використовуватися для атаки на Web-сервери) Типи об'єктів, які слід видалити, можуть бути обрані індивідуально шляхом налаштування відповідного HTTP Application Layer Gateway.

Налаштування HTTP Application Layer Gateway на вимкнення ActiveX та Java applets. В данному випадку використовується об'єкт content_filtering ALG та передбачається виконання користувачам одного із попередніх прикладів.

CLI

gw-world:/> set ALG ALG_HTTP content_filtering

RemoveActiveX=Yes RemoveApplets=Yes

Web-інтерфейс

1. Необхідно перейти до Objects > ALG

2. У таблиці Підтвердження об'єкт HTTP ALG, content_filtering

3. Вибрано керування Strip ActiveX objects (включаючи flash)

4. Вибрано керування Strip Java applets

5. Підтвердження OK

Використання функції фільтрації статичного вмісту, за допомогою якої система NetDefendOS може блокувати або дозволяти доступ на певні веб-сторінки на основі «чорних та білих списків».

У цьому невеликому сценарії користувачам заборонено завантаження .exe-файлів. Проте, веб-сайт D-Link надає необхідні програмні файли, які мають бути дозволені для завантаження.

CLI

Почніть з додавання HTTP ALG для фільтрації HTTP-трафіку:

gw-world:/> add ALG ALG_HTTP content_filtering

Потім створіть HTTP ALG URL для налаштування “чорного списку”:

gw-world:/> cc ALG ALG_HTTP content_filtering

gw-world:/content_filtering> add ALG_HTTP_URL

URL=*/*.exe

Action=Blacklist

На додачу до всього, створіть «білий список»:

gw-world:/content_filtering> add ALG_HTTP_URL

URL=www.D-Link.com/*.exe

Action=Blacklist

Web-інтерфейс

Почніть з додавання HTTP ALG для фільтрації HTTP-трафіку:

1. Необхідно перейти до Objects > ALG > Add > HTTP ALG

2. Введено відповідне ім'я для ALG, наприклад, content_filtering

3. Підтвердження OK

Потім створіть HTTP ALG URL для налаштування «чорного списку»:

1. Необхідно перейти до Objects > ALG

2. У таблиці оберано нещодавно створений HTTP ALG для перегляду його властивостей

3. Підтвердження вкладки HTTP URL

4. Підтвердження Add і вибрано меню HTTP ALG URL

5. Вибрано Blacklist як Action

6. Введено */*.exe у текстовому полі URL

7. Підтвердження OK

На додачу до всього створіть «білий список»:

1. Необхідно перейти до Objects > ALG

2. У таблиці обрано нещодавно створений HTTP ALG для перегляду його властивостей

3. Підтвердження вкладку HTTP URL

4. Підтвердження Add вибрано меню HTTP ALG URL

5. Вибрано Whitelist як Action

6. У текстовому полі URL Введено www.D-Link.com/*.exe

3.6. Захист поштового сервера за допомогою SMTP ALG

Для отримання повідомлень електронною поштою про події IDP необхідно налаштувати SMTP Log receiver. Це повідомлення електронної пошти міститиме огляд подій IDP, які відбулися в період, встановлений користувачем.

Після того, як відбулася подія IDP, NetDefendOS очікує кілька секунд (Hold Time), перш ніж надіслати повідомлення електронною поштою. Тим не менш, повідомлення буде надіслано тільки в тому випадку, якщо кількість подій, що відбулися в цей період часу, дорівнює або більше значення Log Threshold. Після надсилання повідомлення, NetDefendOS очікує кілька секунд (Minimum Repeat Time), перш ніж надіслати нове повідомлення.

IP-адреса SMTP Log Receivers

При визначенні SMTP log receiver необхідно вказати IP-адресу одержувача. Ім'я домену, таке як dns: smtp.domain.com, не може використовуватися.

Правило IDP налаштовано із SMTP Log Receiver. Якщо відбувається подія IDP, спрацьовує Правило. Як мінімум одна нова подія відбувається протягом періоду Hold Time, який триває 120 секунд, таким чином досягнувши рівня порога журналу (відбулося не менше 2). В результаті електронною поштою буде надіслано повідомлення, що містить коротку інформацію про події IDP. Після цього може статися ще кілька подій IDP, але для запобігання "повені" поштового сервера, перед відправкою нових повідомлень NetDefendOS очікує 600 секунд (10 хвилин). Передбачається, що сервер SMTP налаштований в адресній книзі з ім'ям smtp-сервер.

CLI

Додавання SMTP log receiver:

```
gw-world:/> add LogReceiver LogReceiverSMTP smt4IDP IPAddress=smtp-server
Receiver1=youremail@yourcompany.com
```

Правила IDP:

gw-world:/> cc IDPRule examplerule

gw-world:/examplerule> set IDPRuleAction 1 LogEnabled=Yes

Web-інтерфейс

Додавання SMTP log receiver:

1. Необхідно перейти до System > Log and Event Receivers > Add > SMTP Event Receiver

2. Введено:

• Name: smtp4IDP

• SMTP Server: smtp-server

• Server Port: 25

• Визначено альтернативні адреси електронної пошти (до 3)

• Sender: hostmaster

• Subject: Log event from NetDefendOS

• Minimum Repeat Delay: 600

• Hold Time: 120

• Log Threshold: 2

• Підтвердження OK

Правила IDP:

1. Необхідно перейти до IDP > IDP Rules

2. Вибрано правило та Підтвердження Edit

3. Вибрано дію, яку потрібно зареєструвати, та Підтвердження Edit

4. Вибрано Enable logging у вкладці Log Settings

5. Підтвердження OK

Встановлення IDP у простому сценарії, в якому поштовий сервер знаходиться в мережі Інтернет в зоні DMZ з публічною IP-адресою. З'єднання з публічною мережею Інтернет встановлено через WAN-інтерфейс міжмережевого екрану, як показано нижче.

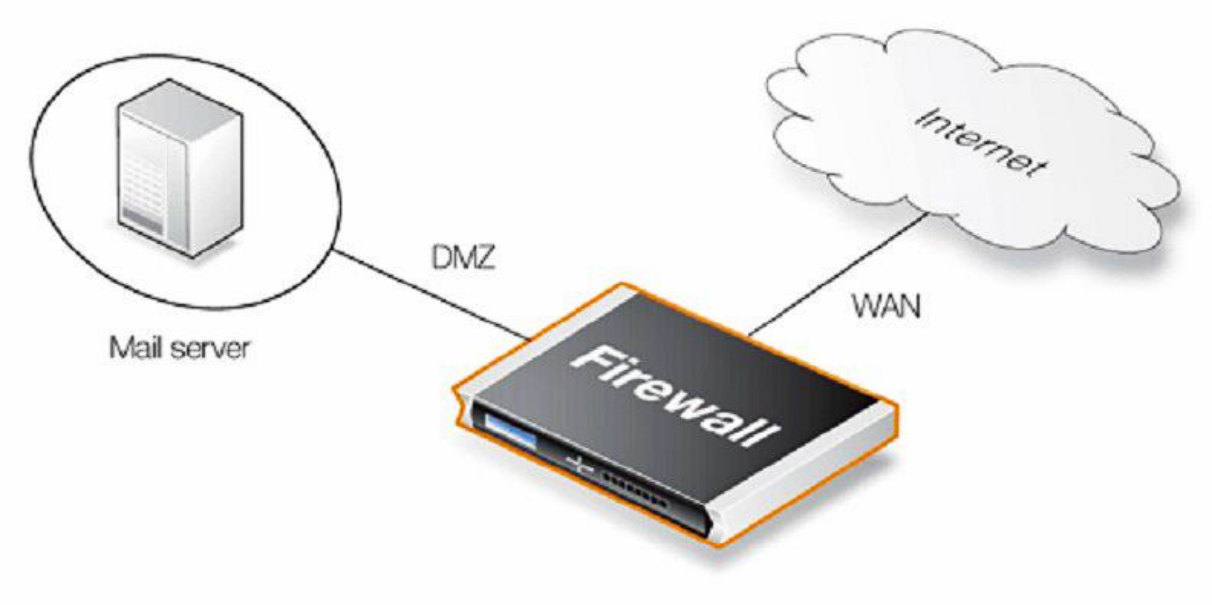

Рис. 3.3. Захист поштового сервера міжмережевим екраном

Створено правило IDP під назвою IDPMailSrvRule та Service для використання сервісу SMTP. Інтерфейс джерела та Мережа джерела визначають, звідки виходить трафік у цьому прикладі із зовнішньої мережі. Інтерфейс призначення та Мережа призначення визначають, куди спрямовано трафік, у разі на поштовий сервер. Тому слід встановлно Мережу призначення на об'єкті, що визначає поштовий сервер.

CLI

Додавання правила IDP:

gw-world:/> add IDPRule Service=smtp SourceInterface=wan

SourceNetwork=wannet

DestinationInterface=dmz

DestinationNetwork=ip_mailserver

Name=IDPMailSrvRule

Визначення дії правила:

gw-world:/> cc IDPRule IDPMailSrvRule

gw-world:/IDPMailSrvRule> add IDPRuleAction Action=Protect

IDPServity=All Signatures=IPS_MAIL_SMTP

Web-інтерфейс

Додавання правила IDP:

Це правило IDP називається IDPMailSrvRule та застосовується до сервісу SMPT. Інтерфейс джерела та Мережа джерела визначають, звідки виходить трафік у цьому прикладі із зовнішньої мережі. Інтерфейс призначення та Мережа призначення визначають, куди спрямовано трафік, у разі на поштовий сервер. Тому слід встановити Мережу призначення на об'єкті, що визначає поштовий сервер.

1. Необхідно перейти до IDP > IDP Rules > Add > IDP Rule

2. Введено:

• Name: IDPMailSrvRule

• Service: smtp

• Перевірено відкинуті пакети: весь трафік, що відповідає даному правилу, повинен бути просканований (це також означає, що трафік, що основний набір правил буде відкинутий), необхідно встановити прапорець у полі Protect against insertion/evasion attacks.

• Source Interface: wan

• Source Network: wannet

• Destination Interface: dmz

• Destination Network: ip_mailserver

• Підтвердження OK

Визначено дію:

Визначено дію, яка вказує, які сигнатури IDP використовувати при відповідності сканованих даних правилу, а також дії NetDefendOS, якщо виявлено можливе вторгнення, таким чином спроби вторгнення будуть причиною відхилення з'єднання, таким чином, встановлено Дію Protect. Для функції Сигнатури встановлено IPS_MAIL_SMTP, щоб використовувати сигнатури, які описують атаки із зовнішньої мережі, засновані на SMTP-протоколі.

1. Вибрано вкладку Rule Action для правила IDP

2. Введено:

• Action: Protect

• Signatures: IPS_MAIL_SMTP

• Click OK

Якщо потрібно зареєструвати спроби вторгнення, це можна виконати, натиснувши "Rule Actions" під час створення правила IDP та увімкнення реєстрації. Для Severity слід встановити значення All, щоб забезпечити збіг всіх SMTP-атак.

Таким чином, відбудеться таке: якщо трафік йде із зовнішньої мережі на поштовий сервер, функцію IDP буде активовано. Якщо трафік відповідає будь-якій із сигнатур у групі сигнатур IPS_MAIL_SMTP, з'єднання буде відкинуто, таким чином, здійснюється захист поштового сервера.

ВИСНОВКИ ДО РОЗДІЛУ 3

В третьому розділі описано основні функції та протоколи міжмережевого екрану D-Link DFL-1600. Основними складовими елементами в NetDOS є інтерфейси, логічні об'єкти та правила. Інтерфейси виконують роль "входів" для вихідного та вхідного трафіку, що проходить через NetDOS. За відсутності даних інтерфейсів у системи NetDOS немає можливості отримувати чи надсилати дані.

Система NetDOS виконує керування доступом на основі набору IP-правил, в якому діапазон захищених LAN-адрес розглядається як довірені хости. При цьому потік трафіку з неперевірених ресурсів довірені хости обмежується. Перед перевіркою нового з'єднання на відповідність набору IP-правил, система NetDOS здійснює перевірку джерела з'єднання на відповідність «Правилам доступу».

За допомогою системи FTP ALG NetDefendOS забезпечена безпека FTP-серверу при відновленні каналу TCP-потоку для передачі FTP-команд та перевірки його вмісту.

Після налаштувань HTTP ALG система NetDefendOS застосовує такі механізми фільтрації сумнівного Web-вмісту:

• Функція Active Content Handling може використовуватися для фільтрації Web-сторінок із вмістом, що розглядається адміністратором як потенційна загроза, наприклад, об'єкти ActiveX та Java Applets.

• Функції Static Content Filtering (Фільтрування статичного вмісту) можна вручну класифікувати веб-сайти на дозволені та заборонені. Ця функція також відома як «білий/чорний список» URL-адрес.

• Dynamic Content Filtering (Фільтрування динамічного вмісту) – це ефективна функція, яка дозволяє адміністратору дозволяти або блокувати доступ до Web-сайтів в залежності від категорії їх класифікації, виконаної службою автоматичної класифікації.

Створено правило IDP під назвою IDPMailSrvRule та Service для використання сервісу SMTP. Визначено дію, яка вказує, які сигнатури IDP використовувати при відповідності сканованих даних правилу, а також дії NetDefendOS, якщо виявлено можливе вторгнення, таким чином спроби вторгнення будуть причиною відхилення з'єднання, таким чином, встановлено дію Protect. Для функції Сигнатури встановлено IPS_MAIL_SMTP, щоб використовувати сигнатури, які описують атаки із зовнішньої мережі, засновані на SMTP-протоколі.

ВИСНОВКИ

В результаті налаштувань NetDefendOS виконує керування доступом на основі набору IP-правил, в якому діапазон захищених LAN-адрес розглядається як довірені хости. При цьому потік трафіку з неперевірених ресурсів довірені хости обмежується. Перед перевіркою нового з'єднання на відповідність набору IP-правил, система NetDOS здійснює перевірку джерела з'єднання на відповідність «Правилам доступу». «Правила доступу» використовуються для того, щоб визначити джерело трафіку на певному інтерфейсі та для автоматичної заборони пакетів з певних джерел. Правила доступу забезпечують ефективну та спрямовану фільтрацію нових спроб з'єднання.

Система NetDOS виконує керування доступом на основі набору IP-правил, в якому діапазон захищених LAN-адрес розглядається як довірені хости. При цьому потік трафіку з неперевірених ресурсів довірені хости обмежується. Перед перевіркою нового з'єднання на відповідність набору IP-правил, система NetDOS здійснює перевірку джерела з'єднання на відповідність «Правилам доступу».

За допомогою системи FTP ALG NetDefendOS забезпечена безпека FTP-серверу при відновленні каналу TCP-потоку для передачі FTP-команд та перевірки його вмісту.

Після налаштувань HTTP ALG система NetDefendOS застосовує такі механізми фільтрації сумнівного Web-вмісту:

• Функція Active Content Handling фільтрує Web-сторінки із вмістом, що розглядається адміністратором як потенційна загроза, наприклад, об'єкти ActiveX та Java Applets.

• Функції Static Content Filtering (Фільтрування статичного вмісту) класифікує веб-сайти на дозволені та заборонені. Ця функція також відома як «білий/чорний список» URL-адрес.

• Dynamic Content Filtering (Фільтрування динамічного вмісту) – це ефективна функція, яка дозволяє або блокує доступ до Web-сайтів в залежності від категорії їх

класифікації, виконаної службою автоматичної класифікації.

Створено правило IDP під назвою IDPMailSrvRule та Service для використання сервісу SMTP. Визначено дію, яка вказує, які сигнатури IDP використовувати при відповідності сканованих даних правилу, а також дії NetDefendOS, якщо виявлено можливе вторгнення, таким чином спроби вторгнення будуть причиною відхилення з'єднання, таким чином, встановлено дію Protect. Для функції Сигнатури встановлено IPS_MAIL_SMTP, щоб використовувати сигнатури, які описують атаки із зовнішньої мережі, засновані на SMTP-протоколі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Microsoft Official Academic Course: Networking Fundamentals, John Wiley & Sons, Inc., 2017. 228 p.
2. Computer Networks, 6th Edition, Andrew S. Tanenbaum, Nick Feamster, David Wetherall, published by Pearson Education, 2020. 946 p.
3. TSI, TS 103 533-3, v 1.1.1, CYBER: Middlebox Security Protocol; Part 3: Profile for enterprise network and data center access control, Oct. 2018
4. Офіційний сайт Cloudflare [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/network-layer/enterprise-networking/
5. Juniper Networks, Inc.: Application Layer Gateways User Guide, 1133 Innovation Way Sunnyvale California 94089 USA, 2023. 657 p.
6. Anderson, B. and McGrew, D., 2019, October. TLS Beyond the Browser: Combining End Host and Network Data to Understand Application Behavior. In Proceedings of the Internet Measurement Conference (pp. 379-392). ACM.