Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Аналіз рівня безпеки мережевого протоколу IPv6

Виконав: студент IV курсу, групи СНзс-42
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

_____ Страмик В.В.
(підпис) (прізвище та ініціали)

Керівник _____ Фриз М.Є.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Стадник М.А.
(підпис) (прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«__» _____ 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Стрaмику Віталію Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз рівня безпеки мережевого протоколу IPv6

Керівник роботи Фриз Михайло Євгенович, к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «02» 03 2021 року № 4/7-170

2. Термін подання студентом завершеної роботи 14.06 2021р.

3. Вихідні дані до роботи Наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. Розділ 1. Аналіз предметної області. 1.1. Звернення до архітектури. 1.2 Заголовки Розширень 1.3. Link-Layer Security. 1.4 Висновок до першого розділу. Розділ 2. Огляд вразивостей протоколу IPV6. 2.1 Контроль площини безпеки. 2.2 Маршрутизація безпеки. 2.3 Протоколювання та моніторинг. 2.4. Перехідні технології та співіснування. 2.5. Особливості безпеки підприємств. 2.6 Огляд конфіденційності. 2.7 Висновок до другого розділу. Розділ 3. Безпека життєдіяльності, основи хорони праці. 3.1 Законодавство про охорону праці в галузі інформаційних технологій. 3.2 Аналіз шкідливих і небезпечних факторів. 3.3 Висновок до третього розділу. Висновки. Список літературних джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема, мета, завдання. 2.Сім показників адаптації до протоколу ipv6. 3.Статистичні дані компанії Google з використання ipv6. 4. Адресація 5. Приклад формування ідентифікатора інтерфейсу за форматом EUI-64. 6. Формат заголовку мережевого протоколу IPV6. 7. Огляд вразливостей протоколу IPV6. 8. Smurf атака. 9. Оцінки вразливостей. 10. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Гурик О.Я., доцент кафедри МТ		

7. Дата видачі завдання 17травня 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	17.05.2021	*Виконано*
2.	Аналіз літературних джерел	18.05.2021-19.05.2021	*Виконано*
3.	Виконання дослідження щодо дослідження протоколу IPv6	20.05.2021-21.05.2021	*Виконано*
4.	Оформлення розділу «Аналіз предметної області»	22.05.2021-28.05.2021	*Виконано*
5.	Оформлення розділу «Огляд вразивостей протоколу IPv6»	29.06.2021-01.06.2021	*Виконано*
6.	Виконання завдання до підрозділу «Безпека життєдіяльності»	2.06.2021	*Виконано*
7.	Виконання завдання до підрозділу «Основи хорони	2.06.2021	*Виконано*
	праці»		
8.	Оформлення кваліфікаційної роботи	6.06.2021	*Виконано*
9.	Нормоконтроль	7.06.2021	*Виконано*
10.	Перевірка на плагіат	7.06.2021	*Виконано*
11.	Попередній захист кваліфікаційної роботи	11.06.2021	*Виконано*
12.	Захист кваліфікаційної роботи	14.06.2021	

Студент _____ Страмик В.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Фриз М.Є.

АНОТАЦІЯ

Аналіз рівня безпеки мережевого протоколу IPv6 // Кваліфікаційна робота освітнього рівня «Бакалавр» // Страмик Віталій Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНзс-42 // Тернопіль, 2021 // С. – рисунок – , таблиці – кресл. – , додат. – , бібліогр. – .

Ключові слова: DoS, CVSS, NAT, ARP, MAC, IANA, CAM, TCAM

Розподіл адрес IPv6 та загальна архітектура є важливою частиною захисту IPv6. Початкові проекти, навіть якщо вони були тимчасовими, зазвичай тривають значно довше, ніж очікувалося. Хоча спочатку вважалося, що IPv6 полегшує перенумерацію, на практиці може бути надзвичайно важко перенумерувати без належної системи управління IP-адресами (IPAM).

Ключовим завданням перед початком розгортання IPv6, після отримання достатніх знань, є підготовка плану адресації. За достатку доступного адресного простору, план адресації може бути структурований навколо послуг разом з географічним розташуванням, що тоді може бути основою для більш структурованих політик безпеки, щоб дозволити або заборонити послуги між географічними регіонами.

ANNOTATION

Analysis of network protocol IPv6 safety level // Qualification work of educational level «Bachelor» // Stramyk Vitaliy Volodymyrovych // Ternopil’ Ivan Pul’uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science, group SNzs-42 // Ternopil', 2021 // P. , Fig. – , Tables – , References – Annexes. – .

Keywords: DoS, CVSS, NAT, ARP, MAC, IANA, CAM, TCAM

IPv6 address allocation and overall architecture are important parts of IPv6 security. Initial projects, even if they were temporary, usually take much longer than expected. Although IPv6 was originally thought to facilitate renumbering, in practice it can be extremely difficult to renumber without a proper IP address management system (IPAM).

The key task before IPv6 deployment, after gaining sufficient knowledge, is to prepare an addressing plan. With sufficient address space available, the addressing plan can be structured around services along with geographic location, which can then be the basis for more structured security policies to allow or prohibit services between geographic regions.

ЗМІСТ

ВСТУП

Актуальність теми. Інтернет-протокол (IP) є основним засобом зв'язку Інтернету. Швидке його розширення призвело до нестачі адрес IPv4 і спричинило поточне перетворення процесу до оновленої версії IPv6. Незважаючи на те, що нова версія була оновлена кілька разів, основний дизайн безпеки та конфіденційності був зроблений в 1998. Однак повне розгортання в 2010-х роках виявило окремі вразливості системи безпеки. У 2011 році (IANA) було розподіллено останні IPv4-адреси. Таким чином, тривале перетворення на IPv6 набирає обертів. В іншому розумінні IPv6 - це лише новий транспортний рівень заголовку. Однак це супроводжується довгим списком модернізацій та перегляду супутніх технологій, які були тісно пов’язані з IPv4. Це включає нові типи записів для доменного імені Система (DNS), інтернет-протокол керуючих повідомлень (ICMP).

Мета і задачі дослідження. Провести аналіз рівня безпеки мережевогопротоколу IPv6 і вирішити такі завдання:

- розглянути специфікацію мережевого протоколу IPv6;
- розглянути питання розгортання протоколу IPv6;
- здійснити пошук можливих методів усунення небезпек та вразливостей.

Практичне значення одержаних результатів. Для успішного прийняття IPv6 у всьому світі, безпеки та аспектів конфіденційності в наборі протоколів були розглянуті ретельно за останні роки. Розглянуті результати були описані в різних наукових працях. Отже, це трудомістке завдання зібрати всі висновки та отримати всебічний розуміння цієї теми. Окрім наукової роботи, було описано ненаукові матеріали з хакерських блогів. Загальною метою даної роботи, це узагальнення та систематизація вразливості IPv6, а також опис відповідних контрзаходів. Надалі, ми описуємо вразливості IPv6 і оцінюємо відповідні контрзаходи.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Звернення до архітектури

Розподіл адрес IPv6 та загальна архітектура є важливою частиною захисту IPv6. Початкові проекти, навіть якщо вони були тимчасовими, зазвичай тривають значно довше, ніж очікувалося. Хоча спочатку вважалося, що IPv6 полегшує перенумерацію, на практиці може бути надзвичайно важко перенумерувати без належної системи управління IP-адресами (IPAM).

Ключовим завданням перед початком розгортання IPv6, після отримання достатніх знань, є підготовка плану адресації. За достатку доступного адресного простору, план адресації може бути структурований навколо послуг разом з географічним розташуванням, що тоді може бути основою для більш структурованих політик безпеки, щоб дозволити або заборонити послуги між географічними регіонами.

На рисунку 1.1 показаний графік використання протоколу IPv6 на початок 2018 року.

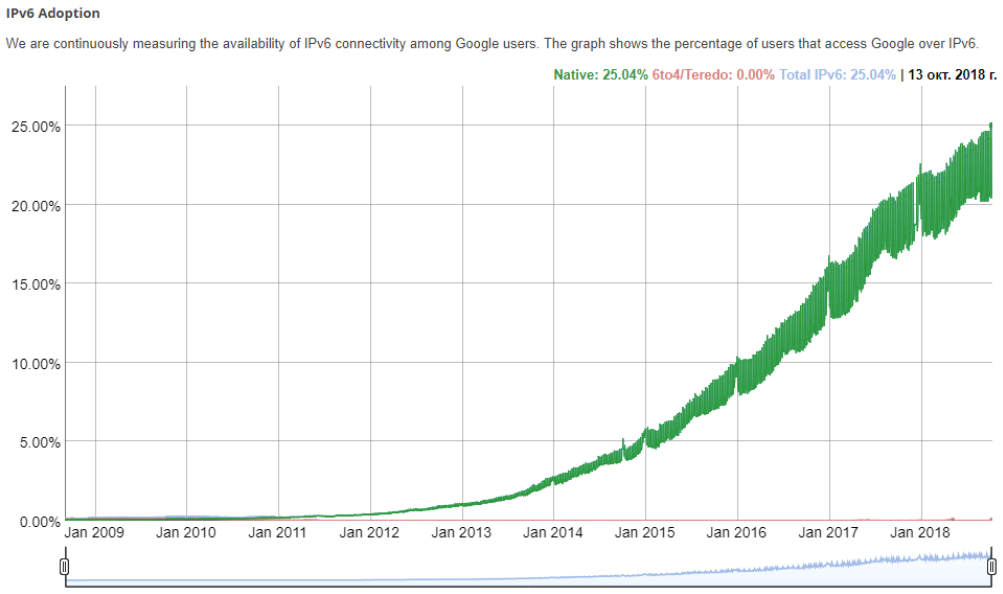

Рисунок 1.1 – Використання протоколу IPv6 (статистичні дані Google)

Поширене питання полягає в тому, чи повинні компанії використовувати простір незалежний від постачальника (PI) проти розподіленого провайдером (PA) простір [RFC7381], але з точки зору безпеки мало різниці. Однак слід пам’ятати про один аспект: хто має адміністративну власність на адресний простір і хто несе технічну відповідальність, якщо/коли існує потреба в застосуванні обмежень щодо маршрутизації простору, наприклад, через зловмисну злочинну діяльність, що походить з нього.

У [RFC7934] рекомендується, щоб розгортання мережі IPv6 надавали декілька адрес IPv6 від кожного префікса до хостів загального призначення, і конкретно не рекомендується обмежувати хост лише однією адресою IPv6 на префікс. Він також рекомендує, щоб мережа надала хосту можливість використовувати нові адреси, не вимагаючи явних запитів (наприклад, за допомогою SLAAC).

Використання ULA

Унікальні локальні адреси (ULA) [RFC4193] призначені для сценаріїв, коли системи глобально недоступні, незважаючи на те, що формально мають загальний обсяг. ULA не схожі на адреси [RFC1918] і мають різні варіанти використання. Одне використання ULA описано в [RFC4864], а деякі міркування щодо використання ULA описані в проекті документа [ID.ietf-v6ops-ula-usage-obzir]; цей документ не мав консенсусу IETF і зараз вважається мертвим.

Точкові посилання

Деякі середовища також використовують локальну адресацію посилань для посилань точка-точка. Хоча така практика може додатково зменшити поверхню атаки на пристрої інфраструктури, оперативні недоліки також слід ретельно розглянути; див. також [RFC7404].

Loopback адреси

Багато операторів зарезервують блок/64 для всіх адрес зворотного зв'язку в своїй інфраструктурі та виділяють/128 із цього зарезервованого/64 префікса для кожного інтерфейсу зворотного зв'язку. Ця практика дозволяє

легко писати Список контролю доступу для забезпечення політики безпеки щодо цих адрес зворотного зв'язку.

Статично налаштовані адреси

Розглядаючи спосіб призначення статично налаштованих адрес, слід враховувати ефективність захисту периметра в даному середовищі. Існує компроміс між простотою експлуатації (де деякі частини адреси IPv6 можна легко впізнати для оперативної налагодження та усунення несправностей) та ризиком тривіального сканування, що використовується для розвідки. [SCANNING] показує, що існують науково обґрунтовані механізми, які роблять сканування доступних вузлів IPv6 більш здійсненним, ніж очікувалося. Використання загальновідомих (таких як ff02:: 1 для всіх локальних вузлів посилань) або використання часто повторюваних адрес може полегшити з'ясування, які пристрої є серверами імен, маршрутизаторами чи іншими критичними пристроями; навіть простий трасування маршруту відкриє більшість маршрутизаторів на шляху. Існує багато методів сканування, які можуть стати можливими, тому оператори не повинні покладатися на парадигму "неможливо знайти, тому що моя адреса випадкова", навіть якщо загальноприйнятою практикою є статично налаштовані адреси, хаотично розподілені по/64 підмережі та завжди використовувати DNS.

Хоча в деяких середовищах забруднення адрес може вважатися додатковою перевагою; це не виключає, що правила периметра активно застосовуються і що статично налаштовані адреси дотримуються певної логічної схеми розподілу для зручності роботи (оскільки простота завжди допомагає безпеці). Типові розгортання матимуть поєднання статичних та нестатичних адрес.

Тимчасові адреси - розширення конфіденційності для SLAAC

Історична автоконфігурація адрес без статусу (SLAAC) спиралася на автоматично згенерований 64-розрядний ідентифікатор інтерфейсу (IID) на основі MAC-адреси EUI-64, який разом з префіксом/64 складає глобально

унікальну адресу IPv6. Адреса EUI-64 генерується з 48-бітової стабільної MAC-адреси. [RFC8064] рекомендує забороняти використання адрес EUI-64, і слід зазначити, що більшість операційних систем хостів більше не використовують адреси EUI-64 і покладаються на [RFC4941] або [RFC8064].

Випадкове створення ідентифікатора інтерфейсу, як описано в [RFC4941], є частиною SLAAC з так званими адресами розширення конфіденційності та використовується для вирішення деяких проблем конфіденційності. Адреси розширення конфіденційності, відомі як тимчасові адреси, можуть допомогти пом'якшити взаємозв'язок діяльності вузла в тій самій мережі, а також можуть якось зменшити вікно впливу атак.

Використання адрес розширення конфіденційності [RFC4941] може перешкодити оператору створювати списки контролю доступу (ACL) для конкретного хосту. Оскільки адреси розширення конфіденційності [RFC4941] також можуть бути використані для приховування деяких зловмисних дій (незалежно від того, чи це було спеціально чи ні), слід запровадити конкретні процедури приписування/звітності користувачів.

[RFC8064] визначає інший спосіб генерування адреси, зберігаючи однаковий IID для кожного префіксу мережі; це дозволяє вузлам SLAAC завжди мати однакову стабільну адресу IPv6 у певній мережі, маючи при цьому різні адреси IPv6 у різних мережах.

У деяких випадках екстремального використання, коли підзвітність користувачів важливіша за конфіденційність користувачів, мережеві оператори можуть розглянути можливість відключити SLAAC і покладатися лише на DHCPv6; але, не всі операційні системи підтримують DHCPv6, тому деякі хости не отримуватимуть підключення IPv6. Вимкнення адрес SLAAC та розширень конфіденційності можна зробити для більшості ОС та не хакерських користувачів, надіславши RA-повідомлення з підказкою для отримання адрес через DHCPv6, встановивши M-біт, а також відключивши SLAAC, скинувши всі A-біти у всій інформації про префікс. варіанти. Однак

зловмисники все ще можуть знайти способи обійти цей механізм, якщо він не застосовується на рівні комутатора/маршрутизатора.

Однак у сценаріях, коли анонімність є сильним бажанням (захист конфіденційності користувачів важливіший за атрибуцію користувача), слід використовувати адреси розширення конфіденційності. Коли доступний [RFC8064], стабільна адреса конфіденційності, мабуть, є гарним балансом між конфіденційністю (між різними мережами) та безпекою/атрибуцією користувачів (усередині мережі).

Міркування щодо DHCP/DNS

Багато середовищ використовують DHCPv6 для надання адрес та інших параметрів, щоб забезпечити можливість перевірки та відстеження. Основною проблемою безпеки є можливість виявлення та протидії неправдивим DHCP-серверам. Слід зазначити, що на відміну від DHCPv4, DHCPv6 може орендувати кілька адрес IPv6 на кожного клієнта, і оренда не пов'язана з адресою рівня зв'язку клієнта, а з унікальним ідентифікатором DHCP (DUID) клієнта, який не завжди пов'язаний на адресу клієнтського рівня посилання.

Незважаючи на те, що принципових відмінностей у питаннях безпеки DNS щодо IPv4 та IPv6 немає, є особливий розгляд у середовищах DNS64 [RFC6147], які слід розуміти. Зокрема, слід розуміти взаємодію та потенціал перешкод у впровадженні DNSSEC - вони детальніше вказані в Розділі 2.7.3.2.

Цікавим підходом є використання/64 на хоста, як запропоновано в [RFC8273]. Це дозволяє полегшити атрибуцію користувача (як правило, на основі MAC-адреси хосту), оскільки його префікс/64 стабільний, навіть якщо додатки, контейнери всередині хоста можуть змінювати адресу IPv6 у цьому/64.

1.2 Заголовки розширень

Заголовки розширень є важливою відмінністю між IPv4 та IPv6. Структура пакетів має велике значення. Наприклад, тривіально знайти (у пакетах на основі IPv4) тип протоколу верхнього рівня та заголовок протоколу, тоді як в IPv6 це насправді не так, оскільки ланцюжок заголовків розширення повинен бути повністю проаналізований. IANA закрила існуючий порожній реєстр "Наступні типи заголовків" для нових записів і перенаправляє своїх користувачів до нового реєстру «Типи заголовків розширень IPv6» відповідно до [RFC7045].

Повна IPv6 адреса	2001:0db8:0000:0000:1100:AA00:0011:00AA
Запис адреси без початкових нулів	2001:db8:0:0:1100:AA00:11:AA
Запис адреси з подвійною двокрапкою замість послідовних нулів	2001:db8::1100:AA00:11:AA

Рисунок 1.2 – IPv6-адреси

На рисунку 1.2 зображено формат запису протоколу IPv6.

Вони також стали дуже суперечливою темою, оскільки, як відомо, вузли переадресації, які відкидають пакети, що містять заголовки розширень, спричиняють збої в підключенні та проблеми розгортання [RFC7872]. Розуміння ролі змінних заголовків розширень є важливим, і в цьому розділі перелічено ті, які потребують ретельного розгляду.

Пояснення щодо того, як проміжні вузли повинні обробляти існуючі пакети із заголовками розширень та будь-якими заголовками розширень, визначеними в майбутньому, міститься в [RFC7045]. Єдиний формат TLV, який буде використовуватися для визначення майбутніх заголовків розширень, описаний у [RFC6564].

Слід також зазначити, що в пакеті немає вказівки, чи вказує поле Наступний протокол на заголовок розширення чи на заголовок транспорту. Це може заплутати деякі правила фільтрації.

В IETF триває робота з правил фільтрації для цих заголовків розширень: [ID.ietf-opsec-ipv6-eh-filtering] для маршрутизаторів транзиту.

Порядок і повторення заголовків розширень

Хоча [RFC8200] рекомендує порядок і максимальне повторення заголовків розширень, на час написання цього документа все ще існують реалізації IPv6, які підтримують нерекомендований порядок заголовків (наприклад, ESP перед маршрутизацією) або незаконний повтор заголовків (наприклад, заголовки кількох маршрутів). Те саме стосується опцій, що містяться у заголовках розширень. У деяких випадках це призводило до збою вузлів при отриманні або пересиланні неправильно відформатованих пакетів.

Для забезпечення рекомендованого порядку та кількості випадків заголовків розширень слід використовувати брандмауер або будь-який крайній пристрій.

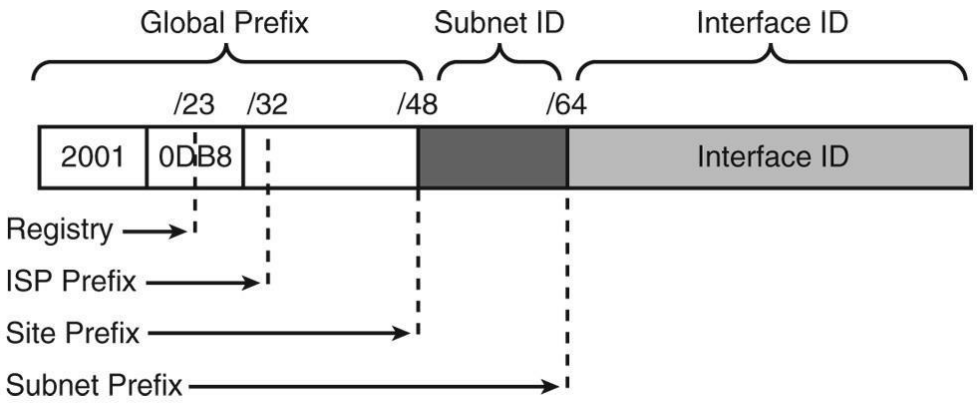

Рисунок 1.3 – Схематичне представлення адреси IPv6

На рисунку 1.3 зображено схематичне представлення адреси IPv6.

Заголовок параметрів стрибка

Заголовок параметрів переходу за переходом, коли він присутній у пакеті IPv6, змушує всі вузли на шляху перевіряти цей заголовок у вихідній специфікації IPv6 [RFC2460]. Звичайно, це було великим шляхом для відмови

в обслуговуванні, оскільки більшість, якщо не всі маршрутизатори, не можуть обробляти цей тип пакетів в апаратному забезпеченні, але повинні «витягувати» цей пакет для обробки програмного забезпечення.

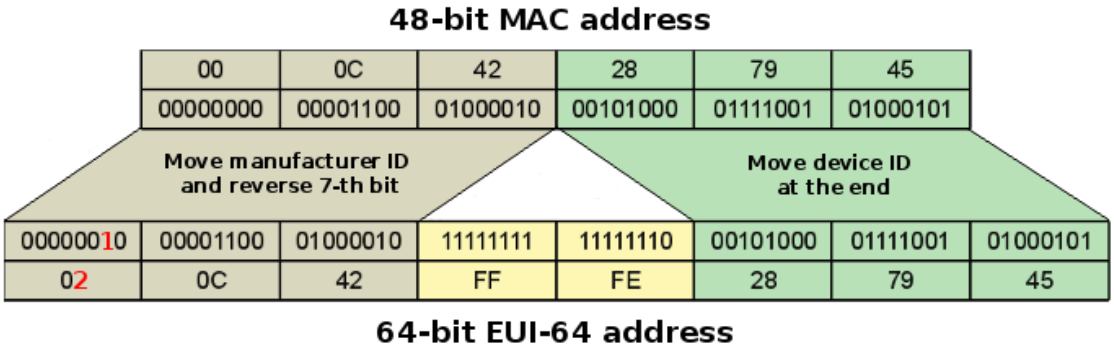

Рисунок 1.4 – Формування ідентифікатора для інтерфейсу (формат EUI-64)

За допомогою формату EUI-64 відбувається перетворення MAC адреси пристрою, зображено на рисунку 1.4.

Заголовок фрагмента

Рисунок 1.5 – Заголовок мережевого протоколу IPv6

Заголовок фрагмента використовується джерелом (і лише джерелом), коли він повинен фрагментувати пакети. [RFC7112] та [RFC8200] пояснюють, чому важливо:

– брандмауер та захисні пристрої повинні видаляти перші фрагменти, які не містять цілого ланцюжка заголовків ipv6 (включаючи заголовок транспортного рівня);

– вузли призначення повинні відкидати перші фрагменти, які не містять цілого ланцюжка заголовків ipv6 (включаючи заголовок транспортного рівня).

В іншому випадку фільтрацію без громадянства може обійти ворожа сторона. [RFC6980] застосовує більш суворе правило до NDP, застосовуючи випадання фрагментованих пакетів NDP. [RFC7113] описує, як повинна поводитися функція захисту RA, описана в [RFC6105], у присутності фрагментованих пакетів RA.

1.3. Link-Layer Security

IPv6 значною мірою покладається на протокол Neighbor Discovery (NDP) [RFC4861], щоб виконувати різноманітні операції зв’язку, такі як виявлення інших вузлів на зв’язку, вирішення їх адрес на рівні каналу та пошук маршрутизаторів на зв’язку. Якщо не захищений, NDP вразливий до різних атак, таких як підробка повідомлень маршрутизатора/сусідів, атаки перенаправлення, DoS-атаки виявлення дублікатів адрес (DAD) тощо. Багато з цих загроз безпеці для NDP були задокументовані в IPv6 ND Trust Models and Threats [RFC3756] та в [RFC6583].

Обмеження норми ND/RA

Neighbor Discovery (ND) може бути вразливим до атак відмови в обслуговуванні (DoS), коли маршрутизатор змушений виконувати роздільну здатність адрес для великої кількості непризначених адрес. Можливі побічні ефекти цієї атаки перешкоджають приєднанню нових пристроїв до мережі або ще гірше, роблячи останній хоп-маршрутизатор неефективним через велике використання процесора. Прості кроки для пом'якшення включають обмеження швидкості "Сусідські запити", обмеження кількості стану,

зарезервованого для невирішених запитів, та розумне управління кешем/таймером.

[RFC6583] детально обговорює потенціал DoS та пропонує вдосконалення впровадження та оперативні методи пом'якшення наслідків, які можуть бути використані для пом'якшення або пом'якшення наслідків таких атак. Ось декілька можливих варіантів пом'якшення, які сьогодні можуть використовувати оператори мережі:

- Вхідне фільтрування невикористаних адрес за ACL. Вони вимагають статичної конфігурації адрес; наприклад, виділення адрес із a/120 та використання певного ACL, щоб дозволити лише трафік до this/120 (звичайно, фактичні хости налаштовані з префіксом/64 для посилання).
- Налаштування процесу NDP (де підтримується).
- Використання /127 для посилання точка-точка за [RFC6164].
- Використання локальних адрес посилань лише на посиланнях, де є лише маршрутизатори, [RFC7404].

Крім того, IPv6 ND широко використовує багатоадресну передачу для сигналізації повідомлень по локальному каналу, щоб уникнути широкомовних повідомлень для ефективної роботи дроту. Однак це має деякі побічні ефекти для бездротових мереж, особливо негативний вплив на час автономної роботи смартфонів та інших пристроїв, що працюють від акумулятора, підключених до таких мереж.

Фільтрація RA/NA

Підробка реклами маршрутизатора - це добре відомий вектор атаки, який був широко задокументований. Наявність зловмисних RA, навмисних чи зловмисних, може спричинити частковий або повний збій у роботі хостів за посиланням IPv6. Наприклад, хост може вибрати неправильну адресу маршрутизатора, яка може бути використана як атака "людина посередині" (MITM), або може прийняти неправильні префікси, які використовуватимуться для конфігурації адрес без громадянства (SLAAC). [RFC6104] узагальнює сценарії, в яких можуть спостерігатися неправдиві PA,

та представляє перелік можливих рішень проблеми. [RFC6105](RA-Guard) описує основу вирішення проблеми неправдивої RA, де сегменти мережі розроблені навколо комутаційних пристроїв, які здатні ідентифікувати недійсні RA і блокувати їх до того, як пакети атаки насправді досягнуть цільових вузлів.

Однак з'явилося кілька методів ухилення, які обходять захист, наданий RA-Guard. Ключовим викликом цій техніці пом’якшення є фрагментація IPv6. Зловмисник може приховати атаку, фрагментуючи свої пакети на декілька фрагментів, так що комутаційний пристрій, який відповідає за блокування недійсних RA, не може знайти всю необхідну інформацію для фільтрації пакетів у тому самому пакеті. [RFC7113] описує такі техніки ухилення та надає рекомендації виконавцям RA-Guard таким чином, що вищезазначені вектори ухилення можуть бути усунені.

З огляду на те, що заголовок фрагментації IPv6 можна використовувати для обходу поточних реалізацій RA-Guard, [RFC6980] оновлює [RFC4861] таким чином, що використання заголовка фрагментації IPv6 заборонено у всіх повідомленнях Neighbor Discovery, за винятком "Реклама шляху сертифікації", таким чином дозволяючи прості та ефективні заходи для протидії атакам Neighbor Discovery.

Робоча група з удосконалення перевірки адреси джерела (SAVI) працювала над іншими способами пом'якшення наслідків таких атак. [RFC7513] допоможе у створенні прив’язок між призначеною IP-адресою джерела DHCPv4 [RFC2131]/DHCPv6 [RFC8415] та прив’язувальним якорем [RFC7039] на пристрої SAVI. Крім того, [RFC6620] описує, як отримати подібні прив'язки, коли DHCP не використовується. Прив'язки можуть бути використані для фільтрації пакетів, що генеруються за локальним посиланням із підробленою IP-адресою джерела.

Як і раніше рекомендується використовувати RA-Guard та SAVI як першу лінію захисту від загальних векторів атак, включаючи неправильно

налаштовані хости. Ця лінія захисту є повністю ефективною, коли дивні фрагменти скидаються маршрутизаторами та комутаторами.

Різка методика запобігання всім атакам NDP заснована на ізоляції всіх хостів із певними конфігураціями. Хости (тобто всі вузли, які не є маршрутизаторами) не можуть надсилати кадри рівня каналу передачі даних на інші хости, тому не може відбуватися жодної атаки на хост-хост. Цю конкретну настройку можна встановити на деяких комутаторах або бездротових точках доступу. Звичайно, це не завжди легко здійснимо, коли господарям потрібно спілкуватися з іншими хостами.

Захист DHCP

Протокол динамічної конфігурації хосту для IPv6 (DHCPv6), як детально описано в [RFC8415], дозволяє серверам DHCP передавати параметри конфігурації, такі як мережеві адреси IPv6 та іншу інформацію про конфігурацію вузлам IPv6. DHCP відіграє важливу роль у більшості великих мереж, забезпечуючи надійну конфігурацію з вибором стану та в контексті автоматизованого забезпечення системи.

Дві найпоширеніші загрози для клієнтів DHCP походять від зловмисних (він же зловмисник) або ненавмисно неправильно налаштованих серверів DHCP. Шкідливий DHCP-сервер встановлюється з метою надати клієнту неправильну інформацію про конфігурацію, щоб викликати атаку відмови в обслуговуванні або здійснити атаку "людина посередині". Ненавмисно налаштований DHCP-сервер може мати такий самий вплив. Додаткові загрози DHCP обговорюються в розділі міркувань безпеки [RFC8415].

[RFC7610], DHCPv6-Shield, визначає механізм захисту підключених клієнтів DHCPv6 від неправдивих серверів DHCPv6. Цей механізм заснований на фільтрації пакетів DHCPv6 на пристрої рівня 2; адміністратор визначає інтерфейси, підключені до серверів DHCPv6. Крім того, заголовки розширень можуть використовуватися для обходу DHCPv6-Shield, якщо не буде застосовано [RFC7112].

Рекомендується використовувати DHCPv6-Shield та аналізувати відповідні повідомлення журналу.

3GPP Link-Layer Security

Посилання 3GPP - це посилання типу точка-точка, яке не має адреси рівня посилання. Це означає, що на цьому посиланні може бути лише кінцевий хост (мобільна ручна установка) і маршрутизатор першого стрибка (тобто вузол підтримки шлюзу GPRS (GGSN) або пакетний шлюз (PGW)). GGSN/PGW ніколи не налаштовує локальну адресу, яка не є посиланням, використовуючи рекламний префікс/64 на ній. Рекламований префікс не повинен використовуватися для визначення он-лайн. Немає необхідності в роздільній здатності адрес за посиланням 3GPP, оскільки немає адрес рівня посилання. Крім того, GGSN/PGW призначає префікс, який є унікальним для кожного посилання 3GPP, яке використовує автоконфігурацію адреси без стану IPv6. Це дозволяє уникнути необхідності виконувати DAD на рівні мережі для кожної адреси, побудованої мобільним хостом.

Сама модель посилання 3GPP пом'якшує більшість відомих атак відмови в обслуговуванні, пов'язаних з NDP. На практиці GGSN/PGW потрібно лише спрямовувати весь трафік на мобільний хост, який підпадає під префікс, призначений йому. Оскільки на посиланні 3GPP також є один хост, немає необхідності захищати цю адресу IPv6.

[RFC6459] для більш детального обговорення моделі зв’язку 3GPP, NDP щодо неї та деталей конфігурації адреси. У деяких мобільних мережах DHCPv6 також використовується, включаючи DHCP-PD.

SeND та CGA

SEcure Neighbor Discovery (SeND), як описано в [RFC3971], є механізмом, який був розроблений для захисту повідомлень ND. Цей підхід передбачає використання нових варіантів NDP для передачі підписів на основі відкритих ключів. Криптографічно створені адреси (CGA), як описано в [RFC3972], використовуються для того, щоб гарантувати, що відправник повідомлення Neighbor Discovery є фактичним "власником" заявленої адреси

IPv6. Була представлена нова опція NDP, опція CGA, яка використовується для перенесення відкритого ключа та пов’язаних параметрів. Ще одна опція NDP, опція RSA Signature, використовується для захисту всіх повідомлень, що стосуються виявлення сусідів та маршрутизатора.

SeND захищає від:

- DoS-атака виявлення повторюваних адрес.
- Атаки на запрошення маршрутизатора та рекламу.
- Повтор атаки.
- Dosed Attacks DoS Neighbor Discovery.

SeND не захищає:

- статично налаштованих адрес.
- адреси, налаштовані за допомогою фіксованих ідентифікаторів (тобто EUI-64).

1.4 Висновок до першого розділу

В даному розділі проведено опис використання ULA, опис Loopback адреси, наведено опис статично налаштованих адрес, наведено опис заголовків розширень. Наведено пояснення щодо того, як проміжні вузли повинні обробляти існуючі пакети.

РОЗДІЛ 2. ОГЛЯД ВРАЗИВОСТЕЙ ПРОТОКОЛУ IPV6

Порівняно з IPv4, його наступник IPv6 охоплює чотири основні модифікації: Довжина адреси була до 128 біт, надаючи 3,4 · 1038 унікальних адрес. Вони містять префікс підмережі та ідентифікатор інтерфейсу, і представлені 8 чотирикратними шістнадцятковими значеннями розділені двокрапками [2]. Щодо суми одержувачів, розрізняють три типи адрес: одноадресну, будь-яку передачу та багатоадресні адреси. Адреси трансляції в IPv6. Формат заголовка був спрощений та зафіксований 40 байт. Фрагментація та інші необов'язкові функціональність перенесена на додаткові заголовки розширень, які вставляються між IP і протоколом верхнього рівня заголовок. Фрагментація була надалі обмежена кінцевими вузлами з метою вивантаження маршрутизатора. Раніше обов'язковий IPsec [3]-[5] розглядається як п'ята основна модифікація описується як необов'язковий [6].

2.1 Контроль площини безпеки

[RFC6192] визначає площину управління маршрутизатором. Це визначення повторюється тут для зручності читача. Зверніть увагу, що визначення повністю агностичне щодо версії протоколу (більша частина цього розділу стосується IPv6 так само, як і IPv4).

Сучасна архітектура маршрутизатора підтримує суворе розділення апаратного та програмного забезпечення площини переадресації та управління маршрутизатором. Площина управління маршрутизатором підтримує функції маршрутизації та управління. Як правило, це описується як апаратні та програмні компоненти архітектури маршрутизатора для обробки пакетів, призначених для самого пристрою, а також для побудови та надсилання пакетів, що походять локально на пристрої. Площина переадресації зазвичай описується як апаратні та програмні компоненти архітектури маршрутизатора, відповідальні за прийом пакета на вхідний інтерфейс, виконання пошуку для

ідентифікації наступного стрибка IP пакета та визначення найкращого вихідного інтерфейсу до пункту призначення та пересилання пакету через відповідний вихідний інтерфейс.

Хоча площина переадресації зазвичай реалізується у високошвидкісному обладнанні, площина управління реалізується загальним процесором (з іменем процесора маршрутизатора RP) і не може обробляти пакети з високою швидкістю. Отже, на цей процесор можна атакувати, заповнивши його чергу вводу більшою кількістю пакетів, ніж він може обробити. Тоді процесор площини управління не може обробити допустимі пакети управління, і маршрутизатор може втратити сумісність OSPF або BGP, що може спричинити серйозні збої в роботі мережі.

Техніка пом'якшення наслідків:

– Щоб скинути нелегітимний пакет управління, перш ніж вони потраплять у чергу до RP (це може бути зроблено за допомогою площини переадресації ACL).

– Для швидкості обмежте решту пакетів до швидкості, яку може підтримувати RP. Слід також зробити захист, специфічний для протоколу (наприклад, підроблений пакет OSPFv3 може ініціювати виконання алгоритму Дейкстра, тому кількість виконання Дійскра також повинна бути обмежена за швидкістю).

У цьому розділі буде розглянуто кілька класів контрольних пакетів:

– Протоколи управління: протоколи маршрутизації: такі як OSPFv3, BGP та, за розширенням, Neighbor Discovery та ICMP.

– Протоколи управління: SSH, SNMP, IPfix тощо.

– Винятки пакетів: це звичайні пакети даних, які вимагають специфічної обробки, наприклад, генерування занадто великого ICMP-повідомлення або використання заголовка параметрів стрибковим переходом.

Протоколи контролю

Цей клас включає OSPFv3, BGP, NDP, ICMP.

Вхідний ACL, який застосовуватиметься до всіх інтерфейсів маршрутизатора, СЛІД бути налаштований, наприклад:

– викинути пакети OSPFv3 (ідентифікований Next-Header як 89) та RIPng (ідентифікований UDP-портом 521) з не локальної адреси.

– дозволити пакети BGP (ідентифіковані TCP-портом 179) від усіх сусідів BGP, а інші видалити.

– дозволити всі пакети ICMP (транзитні та до інтерфейсів маршрутизатора).

Скидання пакетів OSPFv3, які автентифікуються за допомогою IPsec, може бути неможливим на деяких маршрутизаторах, ACL яких не може проаналізувати заголовки розширення IPsec ESP або AH.

Протоколи управління

Цей клас включає: SSH, SNMP, syslog, NTP.

Вхідний ACL, який застосовуватиметься до всіх інтерфейсів маршрутизатора (або до вхідних інтерфейсів периметра безпеки або за допомогою певних функцій платформи) СЛІД конфігурувати, наприклад:

– викинути пакети, призначені для маршрутизаторів, за винятком тих, що належать протоколам, які використовуються (наприклад, дозволити TCP 22 і скинути всі, коли використовується лише SSH);

– видаляйте пакети там, де джерело не відповідає політиці безпеки, наприклад, якщо з'єднання SSH мають походити лише з NOC, тоді ACL повинен дозволити TCP-порт 22 пакети лише з префікса NOC.

Винятки пакетів

Цей клас охоплює кілька випадків, коли пакет площини даних передається процесору маршруту, оскільки він вимагає конкретної обробки:

– генерація занадто великого повідомлення пакета ICMP, коли пакет площини даних не може бути переадресований, оскільки він занадто великий;

– генерація повідомлення про закінчення терміну дії обмеження ICMP, коли пакет площини даних не може бути переадресований, оскільки його поле обмеження стрибків досягло 0;

– генерування недоступного повідомлення призначення ICMP, коли пакет площини даних не може бути перенаправлений з будь-якої причини;

– обробка заголовка параметрів стрибкового стрибка, нові реалізації слідують розділу 4.3 [RFC8200], де ця обробка є необов'язковою;

– або більш конкретно для певної реалізації маршрутизатора: велика ланцюжок заголовків розширення, яка не може бути оброблена апаратним забезпеченням і змусити пакет пробиватися до загального процесора маршрутизатора.

На деяких маршрутизаторах не все може зробити спеціалізоване обладнання площини даних, яке вимагає, щоб деякі пакети були "пробиті" в загальний RP. Це може включати, наприклад, обробку довгих ланцюжків заголовків розширення з метою застосування ACL на основі інформації рівня 4. [RFC6980] і в цілому [RFC7112] висвітлює наслідки для безпеки великих ланцюжків заголовків розширень на маршрутизаторах та оновлює оригінальні специфікації IPv6, [RFC2460], так що перший фрагмент пакета повинен містити всю ланцюжок заголовків IPv6. Ці зміни включені до стандарту IPv6 [RFC8200]

Вхідний ACL не може допомогти зменшити атаку площини управління, використовуючи ці винятки пакетів. Єдиним захистом для RP є обмеження швидкості тих винятків пакетів, перенаправлених до RP, це означає, що деякі пакети площини даних будуть скинуті без будь-яких повідомлень ICMP назад до джерела, що може спричинити діри MTU шляху.

На додаток до обмеження швидкості передачі пакетів площини даних, що стоять у черзі до RP, важливо також обмежити швидкість генерації повідомлень ICMP як збереження RP, але і запобігання атаці посилення, використовуючи маршрутизатор як відбивач. Варто зазначити, що деякі платформи застосовують це обмеження швидкості в апаратному забезпеченні. Звичайно, наслідок негенерування повідомлення ICMP порушить деякі механізми IPv6, такі як Path MTU discovery або простий трасування.

2.2 Маршрутизація безпеки

Маршрутизацію безпеки загалом можна розділити на три розділи:

1. Автентифікація сусідів.
2. Забезпечення оновлення маршрутизації між сусідами.
3. Фільтрування маршрутів.

[RFC5082] також застосовується до IPv6 і може гарантувати, що пакети протоколів маршрутизації надходять з локальної мережі; слід також зазначити, що в протоколі IPv6 усі внутрішні протоколи шлюзу використовують адреси локальних посилань.

Автентифікація сусідів

Основним елементом маршрутизації є процес формування суміжних, сусідніх або однорангових зв'язків з іншими маршрутизаторами. З точки зору безпеки, дуже важливо встановлювати такі взаємозв'язки лише з маршрутизаторами та/або адміністративними доменами, яким людина довіряє. Традиційним підходом було використання MD5 HMAC, що дозволяє маршрутизаторам автентифікувати один одного до встановлення відносин маршрутизації.

OSPFv3 може покладатися на IPsec для виконання функції автентифікації. Однак слід зазначити, що підтримка IPsec не є стандартною на всіх платформах маршрутизації. У деяких випадках для цього потрібне спеціалізоване обладнання, яке розвантажує криптографію до виділених ASIC або розширених програмних зображень (обидва з якими часто мають додаткові фінансові витрати) для забезпечення такої функціональності. Додатковою деталлю є визначення того, чи використовують реалізації IPsec OSPFv3 AH або ESP-Null для захисту цілісності. У ранніх реалізаціях усі конфігурації OSPFv3 IPsec покладались на AH, оскільки деталі не були вказані в [RFC5340]. Однак документ, який конкретно описує, як IPsec повинен бути реалізований для OSPFv3 [RFC4552] конкретно зазначається, що ESP-Null може бути впроваджений, оскільки він відповідає загальним формулюванням

стандартів IPsec. OSPFv3 також може використовувати звичайний ESP для шифрування корисного навантаження OSPFv3, щоб приховати інформацію про маршрутизацію.

[RFC7166] змінює опору OSPFv3 на IPsec, додаючи трейлер аутентифікації до кінця пакетів OSPFv3; він спеціально не автентифікує конкретного ініціатора пакета OSPFv3; швидше, це дозволяє маршрутизатору підтвердити, що пакет дійсно виданий маршрутизатором, який мав доступ до спільного ключа автентифікації.

З усіма механізмами автентифікації оператори повинні підтвердити, що реалізації можуть підтримувати механізми повторного введення ключів, які не спричиняють відключень. Були випадки, коли будь-яке повторне введення клавіш спричиняє збій, і тому компроміс між використанням цієї функціональності повинен бути зважений проти захисту, який вона забезпечує.

Що стосується IPv4, рекомендується вмикати протокол маршрутизації лише на інтерфейсі, де це потрібно.

Забезпечення оновлення маршрутизації між сусідами

Спочатку IPv6 передбачав надання можливостей IPsec у всіх вузлах. Однак, в оновленому стандарті вимоги до вузлів IPv6 [RFC8504] є "ПОТРІБНО", і більше не "МОЖЕ". Теоретично можливо, що зв'язок між двома вузлами IPv6, особливо маршрутизаторами, що обмінюються інформацією про маршрутизацію, буде зашифрований за допомогою IPsec. Однак на практиці розгортання IPsec не завжди можливо з огляду на апаратні та програмні обмеження різних розгортаних платформ, воно також несе операційні витрати, як описано в попередньому розділі.

Фільтрування маршрутів

Політики фільтрації маршрутів будуть різними залежно від того, чи стосуються вони фільтрації крайових маршрутів та внутрішньої фільтрації маршрутів. Як мінімум, політика маршрутизації IPv6, оскільки вона

стосується маршрутизації між різними адміністративними доменами, повинна прагнути підтримувати паритет з IPv4 з точки зору політики, наприклад,

– запобігання підробці джерела IP-джерел, коли це можливо, застосовуючи [RFC2827];

– фільтрувати адреси IPv6 для внутрішнього використання, що не підлягають глобальному використанню, по периметру;

– відкинути пакети від і до випуску та зарезервованого простору (див. [CYMRU] та [RFC8190]);

– налаштуйте вхідні фільтри маршрутів, які перевіряють походження маршруту, власність префіксу тощо за допомогою різних баз даних маршрутизації, наприклад, RADB. У цій галузі проводиться додаткова робота з офіційної перевірки походження AS оголошень BGP у [RFC8210].

Деякі хороші рекомендації щодо фільтрації можна знайти в команді CYMRU за адресою [CYMRU]. [RFC7454] - ще один цінний джерело вказівок у цьому просторі.

2.3 Протоколювання та моніторинг

Для проведення криміналістичних досліджень у разі будь-якого інциденту з безпекою або для виявлення ненормальної поведінки оператори мережі повинні реєструвати кілька частин інформації.

Це включає:

– журнали всіх програм, коли вони доступні (наприклад, веб-сервери);

– використання експорту інформації про потоки IP, також відомого як IPfix;

– використання SNMP MIB;

– використання історичних даних записів сусіднього кешу;

– використання кешованого кешу DHCPv6, особливо коли використовується агент ретрансляції;

– використання подій удосконалення перевірки адреси джерела (SAVI) [RFC7039], особливо прив'язки адреси IPv6 до MAC-адреси та конкретного інтерфейсу комутатора або маршрутизатора;

– використання РАДІУСУ для бухгалтерських записів.

Зверніть увагу, що існують проблеми конфіденційності або правила, пов’язані з тим, як ці журнали збираються, зберігаються та безпечно викидаються. Операторів закликають перевірити законодавство своєї країни (наприклад, GDPR в Європейському Союзі).

Усі ці відомості будуть використані для:

– судово-медичні розслідування, наприклад, хто що і коли робив?

– кореляція: які IP-адреси використовував конкретний вузол (припускаючи використання адрес розширень конфіденційності).

– виявлення ненормальної поведінки: незвичні шаблони трафіку часто є симптомами ненормальної поведінки, яка, в свою чергу, є потенційною атакою (відмова в послугах, сканування мережі, вузол, що є частиною бот-мережі).

Журнали програм

Ці журнали, як правило, являють собою текстові файли, де віддалена адреса IPv6 зберігається у всіх символах (не двійкових). Це може ускладнити обробку, оскільки одну адресу IPv6, наприклад 2001: db8:: 1, можна записати різними способами, наприклад:

– 2001: DB8:: 1 (у верхньому регістрі)

– 2001: 0db8:: 0001 (з провідними 0).

– багато інших способів, включаючи зворотне відображення DNS у повне доменне ім’я (якому не слід довіряти).

RFC 5952 детально пояснює цю проблему та рекомендує використовувати єдиний канонічний формат. Цей документ рекомендує використовувати канонічний формат для адрес IPv6 у всіх можливих випадках. Якщо існуюча програма не може ввійти в канонічний формат,

рекомендується використовувати зовнішню програму, щоб канонізувати всі адреси IPv6.

Лістинг 2.1 – Скрипт на perl

```
#! / usr / bin / perl -w
використовувати строго;
використовувати попередження;
використовувати Socket;
використовувати Socket6;

мій (@words, $ word, $ binary_address);

## пройдіть по файлу по одному рядку за раз
while (моя $ рядок = <STDIN>) {
  chomp $ рядок;
  передбачити моє $ слово (розділити / [\ s +] /, $ рядок)
{
    $ binary_address = inet_pton AF_INET6, $ word;
    if ($ binary_address) {
      надрукувати inet_ntop AF_INET6, $ binary_address;
    } ще {
      надрукувати $ word;
    }
    друк "";
  }
  надрукувати "\ n";
}
```

Експорт інформації про потоки IP за допомогою маршрутизаторів IPv6

Більше того, IPfix є дуже ефективним з точки зору обробки даних та транспортування. Він також може агрегувати потоки за ключем, таким як sourceMacAddress, щоб мати зведені дані, пов'язані з певним sourceMacAddress. Ця пам’ятка рекомендує використовувати IPfix та агрегацію на nextHeaderIPv6, sourceIPv6Address та sourceMacAddress.

SNMP MIB від маршрутизаторів IPv6

RFC 4293 визначає інформаційну базу управління (MIB) для двох сімейств адрес IP. Ця пам’ятка рекомендує використовувати:

– таблиця ipIfStatsTable, яка збирає лічильники трафіку за інтерфейсом;

– таблиця ipNetToPhysicalTable, яка є вмістом кешу Neighbor, тобто відображення між адресами рівня IPv6 та рівня зв'язку.

Сусідній кеш маршрутизаторів IPv6

Сусідній кеш маршрутизаторів містить усі зіставлення між адресами IPv6 та адресами рівня зв'язку. Є кілька способів зібрати поточні записи в кеші сусідів, зокрема, але не обмежуючись ними:

– SNMP MIB;

– використання потокової телеметрії або NETCONF [RFC6241] для збору стану кешу сусідів;

– шляхом підключення через захищений канал управління (наприклад, SSH) та явного запиту дампа сусідського кешу через інтерфейс командного рядка або будь-який інший механізм моніторингу.

Кеш сусідів є надзвичайно динамічним, оскільки відображення додаються, коли в мережі з'являється нова адреса IPv6 (може бути досить часто з адресами розширення конфіденційності або коли вони видаляються, коли стан переходить з UNREACH в видалений (час за замовчуванням для видалення для кожного сусіда) Алгоритм виявлення недосяжності становить 38 секунд для типового хосту, такого як Windows 7. Це означає, що вміст кешу сусідів повинен періодично отримуватися з інтервалом, який не вичерпує ресурси маршрутизатора і все одно надає цінну інформацію (рекомендоване значення - 30 секунд але для перевірки у фактичній установці) та зберігання для подальшого використання.

Це важливе джерело інформації, оскільки це тривіально (на комутаторі, що не використовує алгоритм SAVI), перемогти відображення між адресою рівня каналу зв'язку та адресою IPv6. Переформулюємо попереднє твердження: доступ до поточного та минулого вмісту кешу сусідів має першорядне значення для судово-медичної та аудиторської перевірки.

Використовуючи підхід один / 64 на хост (Розділ 2.1.7) або DHCP-PD, замініть сусідні дампи кешу простим кешуванням виділеного префіксу / 64 у

поєднанні із суворим правилом примусового використання на маршрутизаторі та комутаторах, щоб запобігти спуфінгу IPv6.

Оренда DHCPv6

У деяких мережах адресами / префіксами IPv6 керує DHCPv6-сервер, який надає клієнтам адреси / префікси IPv6. Це справді дуже схоже на DHCP для IPv4, тому може виникнути спокуса використовувати цей файл оренди DHCP для виявлення зіставлення між адресами / префіксами IPv6 та адресами рівня зв'язку, як це зазвичай робили в епоху IPv4.

Це не так просто в епоху IPv6, оскільки не всі вузли використовуватимуть DHCPv6 (є вузли, які можуть виконувати лише автоконфігурацію без стану), але й тому, що клієнти DHCPv6 ідентифікуються не за адресою апаратного клієнта, як в IPv4, а за унікальним ідентифікатором DHCP (DUID), який може мати декілька форматів: деякі - це адреса рівня каналу передачі даних, інші - адреса рівня каналу передачі даних, що містить інформацію про час, або навіть непрозорий номер, який марний для безпеки роботи. Більше того, коли DUID базується на адресі лінії передачі даних, ця адреса може бути будь-яким інтерфейсом клієнта (наприклад, бездротовим інтерфейсом, тоді як клієнт фактично використовує свій дротовий інтерфейс для підключення до мережі).

Якщо в комутаторах рівня 2 використовується легкий агент ретрансляції DHCP, тоді DHCP-сервер також отримує інформацію про Interface-ID, яку можна зберегти для ідентифікації інтерфейсу комутаторів, які отримали конкретну орендовану адресу IPv6. Крім того, якщо "звичайний" (нелегкий) агент ретрансляції додає адресу рівня каналу передачі даних у опції Relay Agent Remote-ID або [RFC6939], тоді сервер DHCPv6 може відстежувати лінію передачі даних та орендовані адреси IPv6.

Коротше кажучи, файл оренди DHCPv6 менш цікавий, ніж в епоху IPv4. Сервери DHCPv6, які зберігають адресу ретрансляційного рівня передачі даних на додаток до DUID у файлі оренди, не страждають від цього обмеження.

Зіставлення між адресою рівня каналу передачі даних та адресою IPv6 можна захистити за допомогою комутаторів, що реалізують алгоритми SAVI. Звичайно, для цього також потрібно, щоб адреса рівня каналу передачі даних була захищена за допомогою механізму рівня 2, такого як [IEEE-802.1X].

Для інтерфейсів, де автентифікація користувача здійснюється через сервер RADIUS, і якщо ввімкнено облік RADIUS, сервер RADIUS отримує записи бухгалтерського типу Acct-Status-Type на початку та в кінці з'єднання, які включають усі адреси IPv6 (та IPv4) використовується користувачем. Ця техніка може бути використана, зокрема, для мереж Wi-Fi із захищеною адресою Wi-Fi (WPA) або будь-якого іншого дротового інтерфейсу IEEE 802.1X на комутаторі Ethernet.

Є й інші джерела даних, які потрібно зберігати точно так, як у мережі IPv4:

– історичне відображення адрес IPv6 користувачам віддаленого доступу VPN;

– історичне відображення MAC-адреси для перемикання інтерфейсу в дротовій мережі.

Криміналістичний випадок використання - це коли оператор мережі повинен знайти адресу IPv6, яка була присутня в мережі в певний час або все ще знаходиться в мережі.

Щоб знайти адресу IPv6 у корпоративній мережі, де оператор контролює всі ресурси, джерелом інформації може бути, за зменшенням, кеш сусідів, файл оренди DHCP. Потім процедура:

– на основі префіксу IPv6 адреси IPv6 знайти маршрутизатор (маршрутизатори), який використовується (є) для досягнення цього префіксу (припускаючи, що використовуються механізми підтасовування);

– на основі цього обмеженого набору маршрутизаторів, часу інциденту та адреси IPv6 для отримання адреси лінії передачі даних з кешу сусідів в реальному часі, з історичних даних кешу сусідів або з подій SAVI, або отримання адреси лінії передачі даних з Файл оренди DHCP.

– виходячи з адреси рівня каналу передачі даних, дізнайтеся, який інтерфейс комутатора був цією адресою рівня зв'язку. У випадку бездротової локальної мережі, журнал RADIUS повинен мати відображення між ідентифікацією користувача та MAC-адресою. Якщо використовується база даних управління конфігурацією (CMDB), відображення між адресою рівня каналу зв'язку та портом комутатора.

Для ідентифікації абонента адреси IPv6 є провайдером Інтернет-послуг, основним джерелом буде орендований префікс DHCP-PD, який часто буде пов’язаний з абонентом через журнал RADIUS. Як альтернатива, в базі інформації переадресації CMTS або BNG буде вказано CPE абонента, а журнал RADIUS може бути використаний для отримання фактичного абонента.

Загальніше, поєднання вищезазначених методів може бути використано у більшості, якщо не у всіх мережах.

RFC 7707 стосується труднощів зловмисником сканувати мережу IPv6 через величезну кількість адрес IPv6 на одне посилання (і чому в деяких випадках це все ще можна зробити). Незважаючи на те, що величезний адресний простір іноді можна сприймати як "захист", це також ускладнює завдання інвентаризації в мережі IPv6, тоді як це було тривіально робити в мережі IPv4 (просте перерахування всіх адрес IPv4, після чого пінг та сканування портів TCP / UDP). Отримання інвентаризації всіх підключених пристроїв має першочергове значення для безпечної роботи мережі.

Існує багато способів провести інвентаризацію мережі IPv6.

Перший прийом полягає у використанні інформації IPfix та витягуванні списку всіх вихідних адрес IPv6, щоб знайти всі вузли IPv6, які надсилали пакети через маршрутизатор. Це дуже ефективно, але, на жаль, не вдасться виявити мовчазний вузол, який ніколи не передавав такі пакети. Також слід зазначити, що локальні адреси посилань ніколи не будуть виявлені цим способом.

Другий спосіб - знову використовувати зібраний вміст кешу сусідів, щоб знайти всі адреси IPv6 у кеші. Цей процес також виявить усі локальні адреси посилань. Див. Розділ 2.6.1.4.

Інший спосіб працює лише для локальної мережі, він полягає в надсиланні ICMP ECHO_REQUEST на локальну багатоадресну адресу ff02:: 1, яка є всіма вузлами IPv6 у мережі. Усі вузли повинні відповідати на цей ECHO_REQUEST за [RFC4443].

Інші методи включають отримання даних з DNS, синтаксичний аналіз файлів журналів, використання виявлення послуг, таких як mDNS [RFC6762] та [RFC6763].

Перерахування зон DNS, особливо з урахуванням зворотних записів DNS та CNAMES, є ще одним поширеним методом, що застосовується різними інструментами. Як уже згадувалося в [RFC7707], це дозволяє зловмисникові обрізати дерево зворотного DNS IPv6 і, отже, перерахувати його у можливий час. Крім того, авторитетні сервери, що дозволяють передачу зон (AXFR), можуть бути додатковим джерелом інформації.

У мережі IPv4 легко пов’язати кілька журналів, наприклад, знайти події, пов’язані з конкретною адресою IPv4. Простої команди grep Unix було достатньо для сканування декількох текстових файлів та вилучення всіх рядків, що мають відношення до певної адреси IPv4.

У мережі IPv6 це трохи складніше, оскільки різні рядки символів можуть виражати одну і ту ж адресу IPv6. Тому просту команду Unix grep використовувати не можна. Більше того, вузол IPv6 може мати кілька адрес IPv6.

Для кореляції журналів, пов'язаних з IPv6, рекомендується мати усі журнали з канонічними адресами IPv6. Потім потрібно шукати поточний (або історичний) набір даних кешу сусідів, щоб знайти адресу рівня каналу передачі даних адреси IPv6. Потім поточний та історичний сусідні кеші даних необхідно шукати для всіх адрес IPv6, пов’язаних із цією адресою рівня каналу зв'язку: це набір пошуку. Останнім кроком є пошук у всіх файлах журналів

(що містять лише адресу IPv6 у канонічному форматі) за будь-якими адресами IPv6 у наборі пошуку.

Більше того, [RFC7934] рекомендує використовувати кілька IPv6-адрес за префіксом, тому кореляція також повинна здійснюватися між цими кількома адресами IPv6, наприклад, виявляючи в кеші NDP всі адреси IPv6, пов'язані з однією і тією ж MAC-адресою та інтерфейсом.

Аномальну поведінку (наприклад, сканування мережі, спам, відмова в обслуговуванні) можна виявити так само, як у мережі IPv4

- раптове збільшення трафіку, виявлене лічильником інтерфейсу (SNMP) або сукупним трафіком із записів IPfix;
- зміна шаблону трафіку (кількість з'єднань в секунду, кількість з'єднань на хост...) із використанням IPfix

Хоча деякі джерела даних (IPfix, MIB, таблиці перемикачів CAM, журнали,...), що використовуються в IPv4, також використовуються для безпечної роботи мережі IPv6, файл оренди DHCPv6 менш надійний, і кеш сусідів має першочергове значення.

Той факт, що існує кілька способів виразити в рядку символів одну і ту ж адресу IPv6, робить використання фільтрів обов’язковим, коли потрібно зробити кореляцію.

2.4. Перехідні технології та співіснування

Оскільки очікується, що деякі мережі не працюватимуть чисто IPv6-способом, різні механізми переходу повинні бути розгорнуті та працювати безпечно. У цьому розділі пропонуються оперативні вказівки щодо найбільш відомих та застосовуваних методів переходу.

Подвійний стек

Подвійний стек часто є першим вибором розгортання для мережевих операторів. Подвійне укладання мережі забезпечує певні переваги перед іншими механізмами переходу. По-перше, зменшується вплив на існуючі

операції IPv4. По-друге, за відсутності тунелів або перекладу адрес, трафіки IPv4 та IPv6 є власними (легшими для спостереження та захисту) і повинні мати однакову обробку мережі (шлях, якість обслуговування,...). Подвійний стек дозволяє поступово вимикати операції IPv4, коли ваша мережа IPv6 готова до прайм-тайму. З іншого боку, операторам доводиться управляти двома мережевими стеками з додатковою складністю.

З точки зору оперативної безпеки це тепер означає, що ви маєте експозицію вдвічі більшу. Зараз потрібно подумати про захист обох протоколів. Як мінімум, частина IPv6 подвійної стекової мережі повинна підтримувати паритет з IPv4 з точки зору політики безпеки. Зазвичай для захисту мереж IPv4 на межі або периметрі безпеки застосовуються такі методи:

- ACL для дозволу або заборони руху;
- Брандмауери з інспекцією пакетів.

Рекомендується додатково налаштувати ці списки контролю доступу та / або брандмауери для захисту зв'язку IPv6. Примусовий захист IPv6 повинен відповідати політиці безпеки IPv4, інакше зловмисник використовуватиме версію протоколу, що має більш розслаблену політику безпеки. Підтримання відповідності між політиками безпеки може бути складним завданням (особливо з часом); рекомендується використовувати брандмауер або менеджер ACL з подвійним стеком, тобто систему, яка може застосувати один запис ACL до змішаної групи адрес IPv4 та IPv6.

Крім того, враховуючи наскрізне підключення, яке забезпечує IPv6, також рекомендується захистити хости від загроз. Загальні рекомендації щодо зміцнення пристрою наведені в Розділі 2.8.

Протягом багатьох років у всіх хост-операційних системах за замовчуванням увімкнено IPv6, тож навіть у мережі, що має лише IPv4, можна атакувати сусідніх жертв рівня 2 через їх локальну адресу посилання IPv6 або через глобальну адресу IPv6, коли вона неправда. RA або неправдиві адреси DHCPv6 надає зловмисник.

Механізми капсулювання

Існує багато тунелів, що використовуються для конкретних випадків використання. За винятком випадків, коли IPsec захищений, усі ці тунелі мають пару проблем безпеки; більшість з них через тунель, як описано в RFC 6169:

- ін'єкція тунелю: зловмисна людина, яка знає кілька частин інформації (наприклад, кінцеві точки тунелю та використовуваний протокол), може підробити пакет, який виглядає як законний та дійсний інкапсульований пакет, який із задоволенням прийме кінцева точка тунелю призначення, конкретний випадок підміни;
- перехоплення трафіку: протоколи тунелю не забезпечують конфіденційності (без використання IPsec або альтернативних методів шифрування), тому будь-хто на шляху тунелю може перехоплювати трафік і мати доступ до чистого тексту пакету IPv6; в поєднанні з відсутністю автентифікації, людина в середині атаки також може бути піднятий;
- викрадення послуги: оскільки немає авторизації, навіть неавторизований користувач може безкоштовно використовувати тунельне реле (це конкретний випадок введення тунелю);
- відбивальна атака: ще один конкретний випадок використання ін'єкції тунелю, коли зловмисник вводить пакети з адресою призначення IPv4, яка не відповідає адресі IPv6, змушуючи першу кінцеву точку тунелю повторно інкапсулювати пакет до місця призначення... Отже, кінцевий пункт IPv4 не буде побачити оригінальну адресу IPv4, але лише одну адресу IPv4 маршрутизатора ретрансляції.
- в обхід політики безпеки: якщо брандмауер або IPS знаходиться на шляху тунелю, він, ймовірно, ні перевірить, ні виявить зловмисний трафік IPv6, що міститься в тунелі.

Щоб пом'якшити обхід політик безпеки, рекомендується заблокувати всі тунелі конфігурації за замовчуванням, відмовляючи у всьому узгодженню трафіку IPv4:

- Протокол IP 41: це заблокує тунелі ISATAP, 6to4, 6rd, а також 6in4;
- Протокол IP 47: це заблокує тунелі GRE;
- Протокол UDP 3544: це заблокує інкапсуляцію тунелів Teredo за замовчуванням. Зараз Teredo в основному ніколи не використовується, і він більше не автоматизований у більшості середовищ, отже, він представляє меншу загрозу, однак, слід звернути особливу увагу на те, якщо можуть бути пристрої зі старими або неоновленими операційними системами, за замовчуванням працювали Teredo.

Фільтрування проникнення також слід застосовувати до всіх кінцевих точок тунелю, якщо це можливо, щоб запобігти підробці адреси IPv6.

Оскільки декілька методів тунелю мають однакову інкапсуляцію (тобто протокол 41 протоколу IPv4) і вбудовують адресу IPv4 в адресу IPv6, існує набір добре відомих атак циклу, описаних у RFC 6324, цей RFC також пропонує методи пом'якшення наслідків.

Статичні тунелі між сайтами

Статичні тунелі між сайтами описані в RFC 2529 та в GRE. Оскільки кінцеві точки IPv4 налаштовані статично і не є динамічними, вони дещо безпечніші (викрадення двонаправленої послуги в основному неможливе), але перехоплення трафіку та ін'єкція тунелю все ще можливі. Тому для цих тунелів рекомендується використовувати IPsec у транспортному режимі та захист інкапсульованих пакетів IPv4. Крім того, IPsec у тунельному режимі може використовуватися для транспортування трафіку IPv6 через ненадійну мережу IPv4.

ISATAP

Тунелі ISATAP [RFC5214] в основному використовуються в одному адміністративному домені та для підключення одного хосту IPv6 до мережі IPv6. Це часто означає, що цими системами, як правило, керує одна сутність; тому, як правило, можливий аудит та суворе підроблення, що підвищує загальну безпеку.

Потрібно бути особливо обережним, щоб уникнути циклічної атаки, застосовуючи заходи RFC 6324 та [RFC6964].

IPsec у транспортному або тунельному режимі можна використовувати для захисту трафіку IPv4 ISATAP для забезпечення конфіденційності трафіку IPv6 та запобігання крадіжці послуг.

Хоча 6-ті тунелі мають ту саму інкапсуляцію, що і 6to4 тунелі, вони розроблені для використання в одному домені SP, іншими словами, вони розгортаються в більш обмеженому середовищі, ніж 6to4 тунелі, і мають невеликі проблеми з безпекою, крім відсутності конфіденційності. Міркування щодо безпеки (Розділ 12) [RFC5969] описують, як захистити 6-й тунель.

IPsec для транспортованого трафіку IPv6 можна використовувати, якщо конфіденційність важлива.

6PE, 6VPE та LDPv6

Організації, що використовують MPLS у своєму ядрі, можуть також використовувати 6PE [RFC4798] та 6VPE [RFC4659], щоб забезпечити доступ до IPv6 через MPLS. Оскільки 6PE і 6VPE дійсно схожі на BGP / MPLS IP VPN, описані в [RFC4364], безпека цих мереж також подібна до тієї, що описана в [RFC4381]. Це спирається на: [RFC7552].

- Адресний простір, маршрутизація та поділ трафіку за допомогою VRF (застосовується лише до 6VPE);
- Приховування ядра IPv4, отже, усунення всіх атак на P-маршрутизатори;
- Забезпечення протоколу маршрутизації між CE та PE; у випадку 6PE і 6VPE можна використовувати локальні адреси посилань (див. [RFC7404]), і оскільки до цих адрес неможливо дістатися ззовні посилання, захист 6PE та 6VPE навіть вищий, ніж IPv4 BGP / MPLS IP VPN.

LDPv6 сам по собі не викликає нових ризиків, див. Також

DS-Lite

DS-lite - це скоріше механізм перекладу, і тому він аналізується далі в цьому документі.

За допомогою версій інкапсуляції та перекладу відображення адреси та порту (MAP-E та MAP-T) мережа доступу є суто мережею IPv6, і протоколи MAP використовуються для надання хостів IPv4 в абонентській мережі та доступу до хостів IPv4 на Інтернет. Абонентський маршрутизатор виконує операції з викликом стану, щоб зіставити всі внутрішні адреси IPv4 та порти рівня 4 з адресою IPv4 та набором портів рівня 4, отриманих в процесі конфігурації MAP. Устаткування SP завжди виконує операції без стану (або декапсуляція, або переклад без стану). Отже, на відміну від розділу 2.7.3.3 не відбувається виснаження DoS-атаки на обладнання SP, оскільки його немає і немає жодної операції, спричиненої новим підключенням рівня 4 (жодної операції реєстрації).

Обладнання SP MAP ПОВИННО реалізовувати всі міркування щодо безпеки [RFC7597]; зокрема, переконавшись, що відображення адреси та порту IPv4 узгоджується з конфігурацією. Оскільки MAP має передбачувану адресу IPv4 та відображення портів, журналами аудиту легше керувати.

6 до4

Для правильної роботи тунелів 6to4 потрібна загальнодоступна IPv4-адреса. Вони можуть використовуватися для забезпечення підключення одного хосту IPv6 до Інтернету IPv6 або підключення кількох мереж IPv6 до Інтернету IPv6. Реле 6to4 - це, як правило, адреса будь-якої трансляції, визначена в [RFC3068], яка була припинена [RFC7526] і більше не використовується останніми операційними системами. Деякі міркування щодо безпеки пояснюються в [RFC3964].

[RFC6343] зазначає, що якщо оператор забезпечує добре керовані сервери та ретрансляції для 6to4, неінкапсульовані пакети IPv6 будуть проходити через чітко визначені точки (власні інтерфейси IPv6 цих серверів та ретрансляторів), в яких можуть застосовуватися механізми безпеки.

Використання клієнтом 6to4 за замовчуванням зараз не рекомендується, і необхідні суттєві запобіжні заходи, щоб уникнути експлуатаційних проблем.

Teredo

Тунелі Teredo [RFC4380] в основному використовуються в житлових умовах, оскільки завдяки інкапсуляції UDP вони можуть легко перетинати пристрій IPv4 NAT-PT, і вони підключають один хост до Інтернету IPv6. Teredo поділяє ті самі проблеми, що й інші тунелі: відсутність автентифікації, конфіденційність, можливі атаки підміни та відображення.

Рекомендується IPsec для перенесеного трафіку IPv6.

Найбільшою загрозою для Teredo є, мабуть, мережа лише з IPv4, оскільки Teredo розроблена для легкого проходження пристроїв IPV4 NAT-PT, які досить часто розміщуються разом із брандмауером із підтримкою стану. Отже, якщо брандмауер IPv4 із дозволом на роботу дозволяє необмежений вихід UDP та приймає зворотний трафік UDP, тоді Teredo фактично пробиває дірку в цьому брандмауері для всього трафіку IPv6 до Інтернету та Інтернету. Хоча політики хоста можуть бути розгорнуті для блокування Teredo в мережі, яка використовує лише IPv4, щоб уникнути цього обходу брандмауера, було б ефективніше блокувати весь вихідний трафік UDP на брандмауері IPv4, якщо це буде можливо (звичайно, принаймні порт 53 повинен залишати відкритим для трафіку DNS).

Зараз Teredo в основному ніколи не використовується, і він більше не автоматизований у більшості середовищ, отже, він представляє меншу загрозу, однак, слід звернути особливу увагу на те, якщо можуть бути пристрої зі старими або неоновленими операційними системами, які за замовчуванням працювали Teredo.

Механізми переходу між мережами IPv4 та IPv6 є альтернативними стратегіями співіснування під час переходу мереж на IPv6. Хоча структура описана в [RFC6144], конкретні міркування щодо безпеки задокументовані в кожному окремому механізмі. Здебільшого вони конкретно згадують про

втручання у розгортання IPsec або DNSSEC, про те, як зменшити підроблений трафік та про те, які можуть бути ефективні стратегії фільтрації.

NAT-класу несучої (CGN), який також називають NAT444 CGN або широкомасштабний NAT (LSN) або SP NAT, описаний в [RFC6264] і використовується як проміжний захід для продовження використання IPv4 у великій мережі постачальника послуг до тих пір, поки постачальник може розгорнути та ефективно рішення IPv6. [RFC6598] просив певний виділений IANA / 10 IPv4 адресний блок використовувати як адресний простір, спільний для всіх мереж доступу за допомогою CGN. Це було виділено як 100.64.0.0/10.

[RFC6269] перелічені деякі конкретні проблеми, пов’язані з безпекою, спричинені широкомасштабним спільним використанням адрес. У розділі "Міркування щодо безпеки" [RFC6598] також перераховані деякі конкретні методи пом'якшення можливого зловживання спільним адресним простором. Деякі правоохоронні органи визначили CGN таким, що перешкоджає їх розслідуванню в галузі кіберзлочинності (наприклад, прес-реліз Європолу про CGN). Багато методів перекладу (NAT64, DS-lite,...) мають ті самі проблеми безпеки, що і CGN, коли одна частина з'єднання має лише IPv4.

[RFC6302] містить рекомендації для серверів, що стоять перед Інтернетом, також реєструвати вихідні порти TCP або UDP вхідних з'єднань, намагаючись допомогти ідентифікувати користувачів, що стоять за такою CGN.

[RFC7422] пропонує використовувати детерміноване відображення адрес для зменшення вимог до ведення журналу для CGN. Ідея полягає в тому, щоб створити алгоритм, що відображає взаємно і назад внутрішнього абонента до загальнодоступних портів.

NAT64 / DNS64 та 464XLAT

NAT64 [RFC6146] із підтримкою стану дозволяє клієнтам, що працюють лише на IPv6, зв’язуватися з серверами IPv4 за допомогою одноадресного UDP, TCP або ICMP. Він може використовуватися разом з DNS64 [RFC6147], механізмом, який синтезує записи AAAA із існуючих

записів A. Існує також NAT64 [RFC7915] без громадянства, який схожий на аспекти безпеки, з додатковою перевагою бути без громадянства, отже, менш схильним до атак виснаження держави.

У розділах розгляду питань безпеки [RFC6146] та [RFC6147] перераховані вичерпні проблеми. Конкретна проблема використання NAT64 полягає в тому, що він буде перешкоджати більшості розгортань IPsec, якщо не використовується інкапсуляція UDP. DNS64 впливає на DNSSEC, див. Розділ 3.1 [RFC7050].

464XLAT [RFC6877] поділяє ті самі міркування щодо безпеки, що і NAT64 і DNS64, проте його можна використовувати без DNS64, уникаючи наслідків DNSSEC.

Dual-Stack Lite (DS-Lite) [RFC6333] - це технологія переходу, яка дозволяє постачальнику послуг ділитися адресами IPv4 між клієнтами, поєднуючи дві відомі технології: IP в IP (IPv4-в-IPv6) та мережеві адреси та порти Переклад (NAPT).

Міркування щодо безпеки щодо DS-Lite в основному спрямовані на реєстрацію даних, запобігання атакам DoS від неправдивих пристроїв (оскільки маршрутизатор перекладу сімейства адрес, функція AFTR [RFC6333] є державним) та обмеження послуг, що пропонуються AFTR лише для зареєстрованих клієнтів.

Розділ 11 [RFC6333] описує важливі проблеми безпеки, пов'язані з цією технологією.

Є багато середовищ, які занадто покладаються на мережеву інфраструктуру, щоб заборонити зловмисний трафік отримати доступ до критичних хостів. У нових розгортаннях IPv6 загальноприйнято бачити ввімкнений трафік IPv6, але жоден із типових механізмів контролю доступу не вмикається для доступу до пристрою IPv6. Зважаючи на можливість помилок конфігурації мережевих пристроїв та зростання IPv6 в цілому в Інтернеті, важливо забезпечити, щоб усі окремі пристрої були загартованими проти недоброзичливої поведінки.

Для забезпечення належного зміцнення хосту, будь то окремий комп’ютер чи маршрутизатор, брандмауер, балансування навантаження, сервер тощо, слід використовувати наступні вказівки.

- Обмежте доступ до пристрою уповноваженим особам.
- Відстежуйте та перевіряйте доступ до пристрою.
- Вимкніть усі невикористані служби на кінцевому вузлі.
- Зрозумійте, які адреси IPv6 використовуються для джерела трафіку, і за потреби змініть значення за замовчуванням.
- Використовуйте криптографічно захищені протоколи для управління пристроями, якщо це можливо (SCP, SNMPv3, SSH, TLS тощо)
- Використовуйте можливості брандмауера хосту для управління трафіком, який обробляється протоколами верхнього рівня.
- Використовуйте антивірусні сканери для виявлення шкідливих програм.

2.5 Особливості безпеки підприємств

Підприємства, як правило, мають надійну політику безпеки мережі для захисту існуючих мереж IPv4. Ці правила були створені завдяки багаторічному досвіду захисту мереж IPv4. Принаймні, рекомендується, щоб корпоративні мережі мали паритет між своїми політиками безпеки для обох версій протоколу. Цей розділ також стосується корпоративної частини всіх Інтернет-провайдерів, тобто тієї частини мережі, до якої підключені працівники Інтернет-провайдера.

Міркування щодо безпеки на підприємстві можна розділити на два розділи - зовнішній та внутрішній.

Міркування щодо зовнішньої безпеки:

Зовнішній аспект стосується забезпечення безпеки на межі або периметрі корпоративної мережі там, де вона відповідає мережі постачальників послуг. Це зазвичай досягається шляхом забезпечення

політики безпеки, або впровадженням спеціальних брандмауерів з інспекцією пакетів, що містять статус, або маршрутизатором з ACL. Типовою політикою IPv4 за замовчуванням для брандмауерів, яку можна легко перенести на IPv6, є надання дозволу на весь вихідний трафік, дозволяючи вхідний лише певний трафік, наприклад встановлені сеанси (див. Також [RFC6092]). Ось ще кілька речей, які можуть покращити політику за замовчуванням:

- Фільтруйте адреси IPv6 внутрішнього використання по периметру.
- Відкиньте пакети від і до bogon та зарезервованого простору, див. Також [CYMRU] та [RFC8190].
- Прийміть певні повідомлення ICMPv6, щоб забезпечити належну роботу ND та PMTUD, див. Також [RFC4890] або [REY_PF] для хостів.
- Фільтруйте конкретні заголовки розширень, приймаючи лише необхідні (підхід до білого списку), такі як ESP, AH (не забуваючи про необхідні транспортні рівні: ICMP, TCP, UDP,...), де це можливо на краю і, можливо, всередині периметра; див. також [ID.ietf-opsec-ipv6-eh-filtering].
- Фільтруйте пакети, що мають нелегальний ланцюжок заголовків IPv6 по периметру (а також можливо всередині).
- Відфільтруйте непотрібні послуги по периметру.
- Впровадити протидію підтасовуванню та виходу з експлуатації в площинах пересилання та управління.
- Впровадити відповідні обмежувачі тарифів та контролери літаків контролю.

Міркування щодо внутрішньої безпеки

Внутрішній аспект стосується забезпечення безпеки всередині периметра мережі, включаючи кінцевий хост. Найбільш значні проблеми тут пов’язані з «Відкриттям сусідів». На рівні мережі рекомендується ретельно переглянути всі міркування щодо безпеки, які обговорюються в Розділі 2.3, а також поглиблено розглянути рекомендації.

При використанні мережевих VPN-мереж слід мати на увазі, що, враховуючи загальний обсяг глобальних адрес IPv6, на відміну від загального використання приватного адресного простору IPv4 [RFC1918], веб-сайти можуть мати можливість взаємодіяти Інтернет, навіть якщо механізм VPN недоступний, а отже, не виконується шифрування трафіку, і трафік може бути введений з Інтернету на сайті, див. [WEBER_VPN]. Рекомендується фільтрувати пакети з підключенням до Інтернету, що мають адресу джерела або пункту призначення, що належить до внутрішніх префіксів сайту; це слід робити для вхідного та вихідного трафіку.

Хости повинні бути загартовані безпосередньо через політику безпеки для захисту від загроз безпеці. Потрібно чітко розуміти можливості за замовчуванням брандмауера хоста, особливо сторонні, які можуть мати різні параметри для дозволу / заборони поведінки за замовчуванням IPv4 або IPv6. У деяких випадках сторонні брандмауери не підтримують IPv6, тоді як власний брандмауер встановлений за замовчуванням. Загальні рекомендації щодо зміцнення пристрою наведені в Розділі 2.8

Слід також зазначити, що багато хостів все ще використовують протокол IPv4 для транспортування таких речей, як RADIUS, TACACS +, SYSLOG тощо. Це вимагатиме додаткового рівня належної ретельності з боку оператора.

2.6 Огляд конфіденційності

Оскільки технології, що базуються на Інтернеті, стають все більш поширеними та демонструють тенденцію нехтувати приватністю користувачів, вирішення порушень конфіденційності є надзвичайно важливим. У цьому підрозділі ми висвітлимо проблеми, пов’язані з конфіденційністю, а також найсучасніші контрзаходи.

А. Адресація

Як зазначено вище, 128-розрядна адреса IPv6 складається з префікс мережі та ідентифікатор інтерфейсу. Поки перший є задається мережею, в якій знаходиться хост, інтерфейсом ідентифікатор генерується хостом незалежно. Спочатку модифікований EUI-формат, що містить MAC-адресу, був запропонований для генерації ідентифікатора інтерфейсу [12]. З моменту використання апаратна адреса призводить до унікальних ідентифікаторів навіть по всьому різних підмереж легко відстежити рух вузла мережі. Зараз у проекті пропонується навіть припинити їх існування [65].

Численні формати адрес пропонуються як альтернатива: (1) Розширення конфіденційності генерує хеш MD5 через регулярний інтервал часу - як правило, 24 години - і використовує це як ідентифікатор [66]. Хоча це перешкоджає довгостроковому відстеженню, короткострокове відстеження все ще можливо, оскільки ідентифікатор цього не робить змінювати одночасно з префіксом. (2) Інша альтернатива часто пропонується DHCPv6. Однак він спирається на статику Унікальний ідентифікатор DHCP (DUID). Локально обнюхуючи DUID або безпосередньо запитуючи відповідні сервери DHCP, зловмисник як і раніше може співвідносити вузол з його поточною адресою [67].

З мобільним IPv6 існує компроміс між збереженням відстеження всіх сеансів під час комутації мережі та конфіденційності порушення, що дозволяє простежити через різні мережі. Включаючи домашню адресу та адресу тимчасової опіки в одному пакеті потенційний супротивник може підслуховувати каналу зв'язку та визначити місцезнаходження пристрою. Це може запобігти шифруванню, напр. g. IPsec. Однак вузли взаємодія з мобільним пристроєм все ще може відстежувати останні.

Щоб запобігти таким порушенням конфіденційності, догляд за адресою та домашню адресу також слід одночасно змінювати [16].

B. Розвідка

Виявлення невідомих вузлів, як правило, є першим кроком під час тесту на атаку чи проникнення, але сам розмір адреси діапазон унеможливлює грубу

силу. Отже, необхідні більш досконалі методи: (1) У 2007 р. Аналіз IPv6 адреси в дикій природі показали часті адресні структури для вперше [68]. Хоча сервери та маршрутизатори, як правило, слідують модифікований формат EUI та “низькі” адреси у клієнтів значна частина адрес, породжених конфіденційністю розширення. Подальший аналіз можливий за адресою [69].

Результати такого аналізу призвели до сканування6 таких же набір інструментів. Цей інструмент здійснює пошук малого байту на базі IPv4 та порту або змінені адреси EUI. (2) Іншим джерелом адрес є DNS, який і буде стає популярнішим серед IPv6 через довжину адреси. По-перше, можна запитувати відомі домени. По-друге, реверс записи можуть бути використані в реалізаціях BIND або NDS [70]. Оскільки відповідь на порожній нетермінал відрізняється від інші повідомлення про помилки, можна зробити висновок, чи адреси починаючи з цього префіксу, відомі цьому серверу. (3) Поза DNS, цікавлять і всі інші джерела адрес, e. g. Інформаційні запити вузла [71], зворотне виявлення [72] або whois.net [73]. (4) Модифікована версія атаки smurf також здатна розвідки. Замість підробки адреси джерела, зловмисник вставляє власну адресу і отримує відповіді за допомогою раніше невідомі адреси джерел. Однак один повинен бути усвідомлюючи, що велика кількість відповідей може спричинити заперечення служіння собі [57]. Щоб запобігти виявленню окремих адрес, сервери, які прослуховують адреси anycast, також повинні використовувати ця адреса будь-якого трансляції як адреса джерела у відповіді [39].

Але властиві IPv6 особливості також роблять розвідку простіше: (1) Призначення декількох адрес для інтерфейс є законним, але для розвідки досить відкрийте один. (2) Адреси закінчуються через бажаний термін життя, але певний час все ще використовуються для існуючого з’єднання [13]. (3) Клієнти, які використовують розширення конфіденційності, також володіють а стабільна адреса, яку можна призначити випадковим чином або після модифікований формат EUI [65]. (4) ICMP не повинен повністю фільтруватися з IPv6. Навіть далі, фільтрування exo-запитів та відповідей вважається менш

важливим через можливий можливий ризик від сканування [74]. Огляд на цю тему також дає [73].

Хоча IPv6, безсумнівно, передбачає значну конфіденційність та вади безпеки, слід зазначити, що жоден з його попередників не був повністю захищений.

2.7 Висновок до другого розділу

Оскільки технології, що базуються на Інтернеті, стають все більш поширеними та демонструють тенденцію нехтувати приватністю користувачів, вирішення порушень конфіденційності є надзвичайно важливим. У цьому розділі ми висвітлили проблеми, пов’язані з конфіденційністю, а також найсучасніші контрзаходи.

РОЗДІЛ 3. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ХОРОНИ ПРАЦІ

3.1 Законодавство про охорону праці в галузі інформаційних технологій

Конституція України до числа соціальних прав включає право кожного на охорону здоров'я, медичну допомогу та медичне страхування (ст. 49), належні, безпечні й здорові умови праці (ст. 43). Відповідно до ст.12 Міжнародного пакту про економічні, соціальні й культурні права кожна людина має право на медичну допомогу та медичний догляд у разі хвороби. Серед основних трудових прав працівників ст. 2 Кодексу законів про працю України вказує на право на здорові та безпечні умови праці. Ст. 6 Основ законодавства України про охорону здоров'я закріплює право на охорону здоров'я, що передбачає серед інших право на безпечні й здорові умови праці.

Державні, громадські або інші органи, підприємства, установи, організації, посадові особи та громадяни зобов'язані забезпечити пріоритетність охорони здоров'я у власній діяльності, не завдавати шкоди здоров'ю населення й окремих осіб (ст. 5 Основ законодавства України про охорону здоров'я). Зазначаючи необхідність створення безпечних і здорових умов праці в процесі трудової діяльності працівників, наукова та навчальна література з трудового права завжди користувалася терміном "охорона праці". При цьому термін "охорона праці" вживається в двох значеннях: широкому й вузькому. Як вказує В.І. Прокопенко, в широкому розумінні до поняття "охорона праці" відносяться "ті гарантії для працівників, що передбачають усі норми трудового законодавства".

У широкому значенні під охороною праці розуміється сукупність правових норм, що охоплюють увесь комплекс питань застосування праці й приналежних до різних інститутів трудового права (трудового договору, робочого часу і часу відпочинку та ін.). До них належать норми, які

забороняють необґрунтовану відмову в прийнятті на роботу, обмежують переведення та звільнення працівників, встановлюють граничну тривалість робочого часу, регламентують час відпочинку, та багато інших, спрямованих на створення сприятливих загальних умов трудової діяльності.

Терміном "охорона праці" у вузькому розумінні завжди визначалося створення для працівників здорових та безпечних умов праці. Закон України "Про охорону праці" від 14 жовтня 1992 р. в ст. 1 так визначає охорону праці: "Охорона праці – це система правових, соціально-економічних, організаційно-технічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі роботи". Виходячи зі змісту закону та інших зазначених вище нормативно-правових актів, більш доцільно, на нашу думку, замість терміна "охорона праці" у вузькому розумінні вживати термін "охорона здоров'я працівників на виробництві", оскільки фактично метою таких заходів є саме охорона здоров'я працівника, збереження його працездатності на виробництві під час виконання трудових обов'язків.

Останнім часом вимоги з охорони здоров'я часто не дотримуються підприємствами різних організаційно-правових форм, які використовують працю найманих працівників. Чимало керівників підприємств безвідповідально ставляться до обов'язків щодо створення здорових і безпечних умов праці, часто розглядають ці питання як другорядні.

Такий стан охорони здоров'я на виробництві пояснюється передусім важким економічним становищем держави, а також іншими об'єктивними і суб'єктивними причинами, які полягають у зносі основних виробничих фондів, у тому, що немає зацікавленості власників у поліпшенні умов і безпеки праці, в некомпетентності більшості персоналу в питаннях охорони здоров'я, в низькій трудовій і технологічній дисципліні, в недостатній ролі органів нагляду і контролю за дотриманням законодавства про працю й охорону здоров'я у процесі праці. В умовах, що не відповідають санітарно-гігієнічним нормам, працює понад 3,4 млн чоловік. Забезпеченість працюючих засобами

індивідуального захисту не перевищує 40—50%. Щорічні виплати на відшкодування шкоди, заподіяної життю і здоров’ю працюючих, сягають 400 млн грн. Особливу тривогу викликає зростання кількості аварій з груповими нещасними випадками.

В Основних напрямах соціальної політики йдеться про необхідність реформування системи охорони праці, основною метою якої є істотне зниження рівня виробничого травматизму і професійних захворювань, зменшення чинників шкідливого впливу на організм працюючих і вивільнення працівників з шкідливих і важких умов праці. Хоча у Основних напрямах і вживається традиційний термін "охорона праці", але по суті мова йде про охорону здоров'я та працездатності працівників.

Для цього передбачається: завершити формування системи управління охороною праці на регіональному і виробничому рівнях для підприємств, установ, організацій усіх форм власності, видів діяльності; здійснити перегляд законодавчих і нормативних актів з питань охорони праці з урахуванням вимог нормативних актів Європейського Союзу; прийняти законодавчі акти про об'єкти підвищеної небезпеки і про безпеку промислової продукції; перейти до територіально-галузевого принципу здійснення державного нагляду за охороною здоров'я в процесі праці; забезпечити стабільне фінансування заходів щодо питань охорони здоров'я тощо. На жаль, деякі з цих заходів так і залишаються на папері.

Найважливіші норми щодо охорони здоров'я працівників на виробництві закріплені в Законі України "Про охорону праці" від 14 жовтня 1992 р., у трьох главах КЗпП (глава XI "Охорона праці", глава XII "Праця жінок", глава XIII "Праця молоді"), а також у підзаконних актах – положеннях, правилах, інструкціях, актах соціального партнерства, локальних нормативно-правових актах.

3.2 Аналіз шкідливих і небезпечних факторів

Мікрокліматичні умови

Санітарно–гігієнічне нормування умов мікроклімату здійснюється за [15], які встановлюють оптимальні і допустимі параметри мікроклімату залежно від загальних енерговитрат організму при виконанні робіт і періоду року.

Роботи, які виконуються персоналом, відносяться до фізичних робіт категорії «Легка Іа» за [15]. Оптимальні значення характеристик мікроклімату наведено у таблиці 3.1.

Таблиця 3.1 – Оптимальні показники мікроклімату

Період року	Температура повітря, °С	Відносна вологість, %	Швидкість руху повітря, м/с
Холодний період року	22–24	60–40	0.1
Теплий період року	23–25	60–40	0.1

Температура внутрішніх поверхонь робочої зони (стіни, підлога, стеля) технологічного обладнання (екрани і т. ін.), зовнішніх поверхонь устаткування, не повинна виходити більш ніж на 2°С за межі оптимальних температур повітря для даної категорії робіт.

Для підтримки сприятливого мікроклімату використовується кондиціонер. Для спроектованого приміщення, орієнтовна потужність «спліт»–кондиціонера становить – 5.8 кВт. Цій вимозі відповідає HITACHI RAS-18LH2/RAC-18LH1 з такими характеристиками:

– діапазон робочих температур: від −10°С до +43°С;
– холодопродуктивність: 4,89 – 4,91 кВт;
– теплопродуктивність: 5,70 – 5,72 кВт;
– рівень шуму при охолодженні (вис/ср/низ): 45/42/39/36 дБ(А);

– рівень шуму при нагріванні (вис/ср/низ): 43/39/36/36 дБ(А).

В холодний період року для підтримання сприятливого мікроклімату здійснюється опалення від дахової котельні, розміщеної над технічним поверхом будівлі. Система опалення двотрубна, з верхнім розведенням теплоносія. Опалювальні прилади – панельні радіатори Purmo. Для регулювання теплового потоку від опалювального приладу, на підводці теплоносія до приладу встановлено регулюючий клапан з термостатичною головкою.

Виробниче освітлення

Освітлення в кабінеті природне бічне і штучне загальне.

Бічне природне освітлення має здійснюватися через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природної освітленості (КПО) 1,5 % згідно з [16].

Відповідно до [16] роботи, що виконуються в приміщенні класифікується як середньої точності – виконується робота з об’єктами розпізнавання 0,5мм–1мм. Рівень освітленості на робочому місці має бути не менше 300 лк.

Захист від виробничого шуму

Джерелами шуму в приміщенні є вентилятори охолодження ЕОМ

(максимальний рівень шуму – 35 дБА) та «спліт»-кондиціонер (максимальний рівень шуму – 45 дБА). Звук можна вважати постійним так, як його рівень протягом робочого дня змінюється не більше ніж на 5 дБА.

Допустимий еквівалентний рівень звуку згідно [17] наступний: для програміста ЕОМ нормований звуковий тиск повинен бути не вище 50 дБА. У даному випадку сумарний рівень звукового тиску не перевищує нормованого значення.

Захист від електромагнітних полів

Джерелом електростатичного поля й електромагнітних випромінювань у широкому діапазоні частот (понад 50 Гц та інфранизькочастотному,

радіочастотному, інфрачервоному, видимому, ультрафіолетовому, рентгенівському) є персональні електронно– обчислювальні машини.

3.3 Висновок до третього розділу

В даному розділі проведено опис Законодавства про охорону праці в галузі інформаційних технологій та наведено аналіз шкідливих і небезпечних факторів.

ВИСНОВКИ

У цій роботі ми описали безпеку та конфіденційність вразливості IPv6 та оцінених доступних контрзаходів. Потім ми систематизували вразливості з повагою за такими критеріями: дія, об’єкт, ціль, походження та тип. Крім того, контрзаходи були систематизовані за дією, об’єктом та рівнем діяльності.

Оцінка показала, що для цього можна знайти контрзаходи більшість вразливостей, що призводить до висновку що IPv6 є досить безпечним протоколом. Однак деякі контрзаходи створюють нові уразливості. Наприклад, SeND запобігає атакам реклами маршрутизатора, але збільшує ризик відмови в обслуговуванні через збільшення зусиль на обчислення.

Нарешті, ми описали недосконалі вразливі місця та визначили три основні фактори IPv6: адреси, що забезпечують захист від зовнішніх факторів відстеження, дозволяють легке ведення журналу для адміністраторів, дозволяє проводити розвідку через активне зондування.

Також виконані завдання, які були поставленні в даній роботі, зокрема:

- розглянуто специфікацію мережевого протоколу IPv6;
- розглянуто питання розгортання протоколу IPv6;
- здійснено пошук можливих методів усунення небезпек та вразливостей.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Arbor Networks. Стаття Marc Eisenbarth [Електронний ресурс]: Режим доступу: http://www.arbornetworks.com/asert/2014/08/ipv4–is–not–enough/ – Назва з екрану. Дата перегляду – 3.05.2021 р.

2. IPv6 Readiness in the Communication Service Provider Industry. An Incognito Software Report, April 2014, 18 p.

3. Santosh Naidu P1, Amulya Patcha, IPv6: Threats Posed By Multicast Packets, Extension Headers and Their Counter Measures. IOSR Journal of Computer Engineering (IOSR–JCE), Nov. – Dec. 2013, 66–75 p.

4. Google Official Blog. Під ред. Lorenzo Colitti IPv6 Statistics [Блог]: Режим доступу: http://www.google.com/intl/en/ipv6/statistics/— Назва з екрану. Дата перегляду – 3.05.2021 р.

5. Diane Teare. Implementing Cisco IP Routing (ROUTE) Foundation

Learning Guide Foundation learning for the ROUTE 642–902 Exam– Индианаполис: Cisco Press, 2004. 765 с.

6. RFC 2460 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html /rfc2460 – Назва з екрану. Дата перегляду – 23.05.2021 р.

7. RFC 4443 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html /rfc4443 – Назва з екрану. Дата перегляду – 9.01.2018 р.

8. RFC 4861 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html /rfc4861 – Назва з екрану. Дата перегляду – 10.01.2021 р.

9. RFC 4429 [Електронний ресурс]: Режим доступу: https://tools.ietf.org/html/rfc4429 – Назва з екрану. Дата перегляду – 10.01.2021 р.

10. Google Official Blog. Під ред. Lorenzo Colitti Access Google services over IPv6 [Блог] : Режим доступу: www.google.com/intl/en/ipv6/ — Назва з екрану. Дата перегляду – 4.05.2021р.

11. *Gabi Nakibly Michael Arov* “Routing Loop Attacks using IPv6 Tunnels”– 7 USENIX Association Berkeley, CA, USA, 2009, 7 p.

12. *Sander Degen, Arjen Holtzer* Testing the security of IPv6 implementations – Nederland’s, March 2014, 42 p.

13. Модели, построенные с использованием теории графов [Електронний ресурс].– Режим доступу: http://inf–bez.ru/?p=762 – Назва з екрану. Дата перегляду – 12.05.2021 р.

14. ДСанПіН 3.3.2–007–98. Гігієнічні вимоги до організації роботи з візуальними дісплейними терміналами електронно–обчислювальних машин\МОЗ України–К.:1998.18с.

15. ДСН 3.3.6.042–99 Санітарні норми мікроклімату виробничих приміщень – Київ, 2000.

16. ДБН–В.2.5–28–2006–Природне і штучне освітлення.

17. ДСН 3.3.6.037–99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

18. Правила улаштування електроустановок ПУЕ–2009.

19. НАПБ Б.03.002–2007. Нормы определения категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности.

20. НПАОП 0.00–1.28–10 Правила охорони праці під час експлуатації електронно–обчислювальних машин.