УДК 621.372.88

Кабаченко М. Д., магістрант; **Трапезон К. О.** к.т.н.
(Національній технічний університет України «Київський політехнічний інститут»)

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ МЕРЕЖАХ З ПІДТРИМКОЮ ПРОТОКОЛУ IPv6

Кабаченко М.Д., Трапезон К.О. Особливості забезпечення інформаційної безпеки в корпоративних мережах з підтримкою протоколу IPv6. Виявлено основні уразливості, які присутні в корпоративних сегментах мереж з підтримкою IPv4. Наведені та проаналізовані основні технічні рішення, які доцільно використовувати в мережах з підтримкою протоколу IPv6 для підвищення безпеки мережі на етапах її впровадження та функціонування. Сформульовано основні проблеми, з якими стикаються адміністратори при переході сегментів мереж з традиційного протоколу IPv4 на IPv6. Визначені основні чинники, які треба враховувати при організації тунелювання пакетів. Визначені недоліки, які має протокол перетворення між IPv6 та IPv4 – NAT-PT. Розглянуто сценарій Mobile IPv6 та визначені відмінності з концепцією MobileIPv4.

Ключові слова: інформаційна безпека, корпоративна мережа, протокол, IPV6, IPV4, тунелювання пакетів, протокол перетворення NAT-PT

Кабаченко М.Д., Трапезон К.А. Особенности обеспечения информационной безопасности в корпоративных сетях с поддержкой протокола IPv6. Найдены основные уязвимости, которые существуют в корпоративных сегментах сетей с поддержкой IPv4. Приведены и проанализированы основные технические решения, которые целесообразно применять в сетях с поддержкой IPv6 для повышения безопасности сетей на этапах их внедрения и функционирования. Сформулированы основные проблемы, с которыми сталкиваются администраторы при переходе сегментов сетей с традиционного протокола IPv4 на IPv6. Определены основные факторы, которые необходимо учитывать при организации туннелирования пакетов. Определены недостатки, которые имеет протокол преобразования между IPv6 и IPv4 – NAT-PT. Рассмотрен сценарий MobileIPv6 и определены отличия при сравнении с концепцией MobileIPv4.

Ключевые слова: информационная безопасность, корпоративная сеть, протокол, IPV6, IPV4, туннелирование пакетов, протокол преобразования NAT-PT

Kabachenko M.D., Trapezon K.O. Features of providing of informative safety in corporate networks with support of protocol of IPv6. The basic are found to vulnerability, that exists in the corporate segments of networks with support of IPv4. Basic technical decisions over, that it is expedient to apply in networks with support of IPv6 for the increase of safety of networks on the stages of their introduction and functioning, are brought and analyzed. Basic problems into that administrators run in transition of segments of networks from traditional protocol of IPv4 to IPv6 are set forth. Basic factors that must be taken into account during organization of tunneling of packages are certain. Defects has that protocol of transformation between IPv6 and IPv4 are certain - NAT-PT. The scenario of Mobile IPv6 is considered and differences are certain when compared to conception of Mobile IPv4.

Keywords: informative safety, corporate network, protocol, IPV6, IPV4, tunneling of packages, transformation protocol NAT-PT

Вступ. Питання про захист критично важливих пристроїв та устаткувань, які входять до складу мережної інфраструктури і залежать від мережі, є дуже пріоритетним в аспекті темпів сучасного розвитку телекомунікаційних технологій у всьому світі. Нині комп'ютерні атаки зазвичай не націлені на одну робочу станцію або одну мережу, а стають більш і більш автоматизованими та складними і можуть призвести врешті-решт до великої розподіленої відмови в обслуговуванні елементів, які в цілому впливають на ключові компоненти інформаційних мереж.

На сьогодні головним завданням в мережах з підтримкою нового комунікаційного протоколу IPv6 є адаптація і вироблення шляхів удосконалення існуючої архітектури інформаційної безпеки для забезпечення можливостей, які стали доступні завдяки розробникам комунікаційного протоколу IPv6 з долученням нових функцій задля підвищення безпеки мережі та її компонентів [1].

В статті визначені особливості принципу “End-to-end security” між хостами корпоративної мережі з підтримкою IPv6. Розглянуті сценарії захисту даних в мережних моделях з IPv6 є ознаками методів боротьби, які дозволяють зменшити ризик як навмисних мережних атак ззовні, так і ненавмисних дій з боку користувачів цієї мережі.

Порівняння механізмів безпеки в IPv6 та IPv4 мережах. Порівняння аналізу потенційних загроз і методів ослаблення для обох типів корпоративних мереж з підтримкою IPv4 або IPv6 показує їх схожість. В рекомендації RFC 2460 щодо безпечного розгортання IPv6 вказано, що безпека IPv6-мереж повинна бути забезпечена з самого початку, а не бути представлена у вигляді доповнення до IPv4. Важливо зазначити, що підвищення безпеки в мережах з протоколом IPv6 є повторне введення End-to-end моделі безпеки без деяких обмежень, які існують зараз у мережах IPv4. Розробники протоколу IPv6 прийняли до уваги відомі уразливості безпеки мережі IPv4 та розробили рішення, які дозволяють зменшити ці ризики [2]. До них належать питання broadcast storm, фрагментація атак і служб безпеки, серед яких аутентифікація пристроїв, цілісність і конфіденційність даних.

Відомо, що IPv4-мережі сприятливі до різних типів фрагментаційних атак, але стандарт IPv6 забезпечує кращий захист в цьому плані, завдяки наступним заходам:

• фрагментація заборонена проміжними пристроями – має незначну перевагу, коли остаточно відомо, що для зв’язку між деякими учасниками не буде використовуватися нефрагментований трафік;

• перекриття фрагментів заборонено – мається на увазі, що тільки джерело може фактично створити фрагментований трафік;

• пристрої змушені відкидати зібрані пакети, об’єм яких менше ніж 1280 байт – мінімум інформаційного блоку фрагментації MTU.

Ще однією проблемою в мережах IPv4 є посилення трансляції (broadcast amplification). У специфікації IPv6 відсутнє поняття розподіленої трансляції з протоколу і визначена унікальна мова в RFC2463 для пом'якшення цих типів атак. Стандарт IPv6 також вимагає, щоб всі IPv6-сумісні пристрої підтримували протокол IPSec для забезпечення аутентифікації, цілісності і конфіденційності послуг на мережному рівні. У той час як протокол IPv4 модифікував заголовки IPSec у вихідний кадр IPv4, IPv6 має можливість підтримувати IPSec в межах визначеної структури пакета з використанням додаткових заголовків. Архітектура безпеки IPv6 повинна бути побудована з оглядом на використання End-to-end моделі безпеки і внести відповідні зміни скрізь, де це необхідно.

Сценарії організації роботи мереж з IPv6. З метою оцінки рівня інформаційної безпеки в корпоративних мережах нового покоління розглянемо декілька приватних сценаріїв організації мереж IPv6, які за своєю сутністю використовують переваги протоколу IPv6. На Рис. 1 представлені найбільш поширені сценарії, які сьогодні превалюють при роботі корпоративних мереж з підтримкою протоколу IPv6.

Сценарій “E-government”. За цим сценарієм урядова мережа складається з взаємозв'язків між різними державними відомствами і центральними мережами. Вона пропонує послуги як внутрішнім клієнтам, так і громадянам (наприклад, онлайн-голосування, податкової декларації, реєстрації автомобілів і т.д.). Видаливши службу NAT в протоколі IPv6 можна очікувати, що використання IPv6 сприятиме використанню більш широко послуг електронного уряду та полегшить управління мережею.

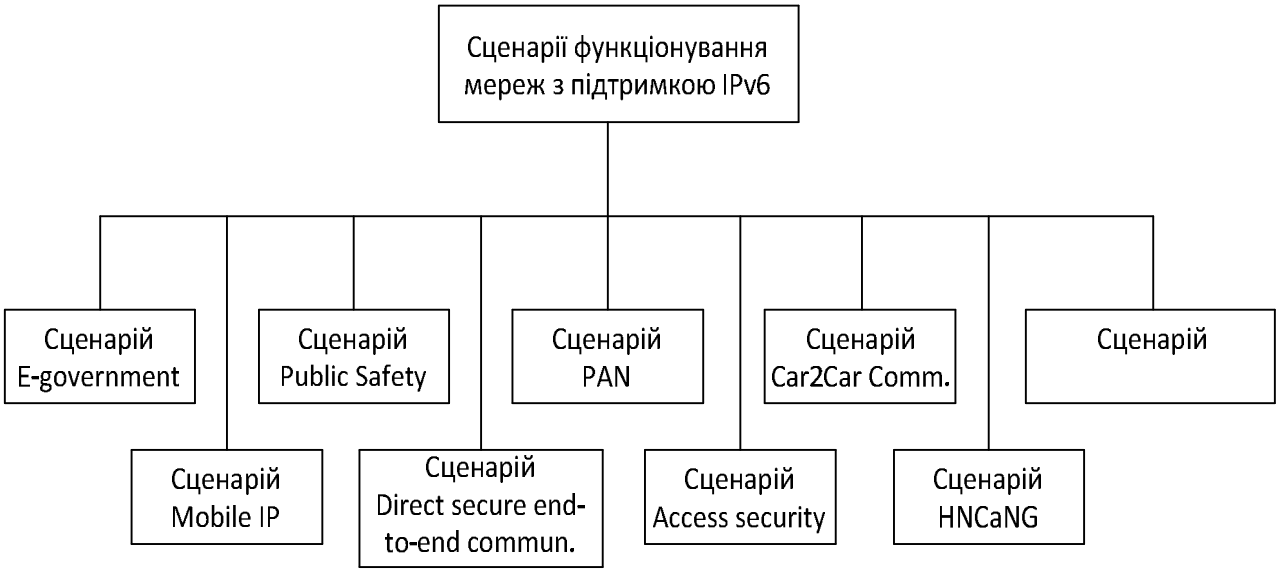

Рис. 1. Класифікація сценаріїв

Сценарій "MobileUser". Користувачі мобільних пристроїв можуть залишатися на зв'язку без перерв у роумінгу знаходячись при цьому між різними мережами доступу і послуг. Оскільки IPv6 забезпечує достатню кількість адрес та прогресивних особливостей, очікується, що у мобільних службах України буде використано Mobile IPv6.

Сценарій "Public Safety". Тут мова йде про те, що громадські організації закликають до безпеки на основі прив'язки IP-адреси (наприклад, обмін відео, фотографії, документи, повідомлень і т.д.) до місця розташування абонента. Перевагами використання IPv6 в цьому сценарії є автоконфігурація, підвищення мобільності та спрощена взаємодія між різними організаціями.

Сценарій "Direct secure end-to-end communication". Тут користувач мобільного пристрою може мати доступ до своєї корпоративної мережі або доступ до мереж при віддаленій роботі. У цьому випадку мобільний маршрут IPv6 може бути розгорнутий для того, щоб забезпечити прямий зв'язок між мобільним пристроєм і іншим терміналом без використання неефективної трикутної маршрутизації через опорну точку мобільності.

Сценарій "Personal Area Network (PAN)". Користувачі можуть мати кілька пристроїв (телефонів, ноутбуків, датчики, пристрої введення) і один з пристроїв може забезпечити доступ до Інтернету (через WLAN, 3G), що забезпечує мобільність сервісу для PAN за допомогою мобільності IPv6-мережі (NEMO).

Сценарій "Access security". На основі стандартів IEEE 802.1X пристрої функціонують з урахуванням контролю доступу до мережі. Тобто після одноразового підключення до мережі інфікованого пристрою або зловмисника, цей вузол здатен впливати на сусідні вузли і в IPv6 захищено дослідження сусідніх вузлів (SEND), і це запобігає впливу таких типів атак.

Сценарій "Car-to-car communication". Консорціум Car2Car communication стандартизує зв'язок між різними машинами (наприклад, обмін даних з датчиків), а також зв'язок між автомобілем та придорожніми пунктами, Інтернетом, або виробником автомобіля (наприклад, для обслуговування).

Сценарій "Home network connectivity and networked gaming". Зрозуміло, що мережні ігри сьогодні стають все більш і більш популярним. Протокол IPv6 забезпечує прозорість мережного рівня без NAT, що сприяє розгортанню мережних ігор, особливо піринговых ігор, що вимагають користувачів у домашніх умовах бути підключеними до IPv6.

Сценарій "Collective transports". Громадський та авіа- транспорт (наприклад, літак) забезпечує підключення до Інтернету для пасажирів, авіакомпаній. Мобільність IPv6-мережі (NEMO) забезпечує стабільність адрес завдяки використанню різних передових технологій.

Серед розглянутих сценаріїв найбільш перспективним серед розробників мережних пристроїв корпоративного сегменту вважається сценарій "Mobile IP". Це пояснюється стрімким розвитком мереж наступного покоління.

Механізми переходу з IPv4 на IPv6. Для адміністратора мережі провести перехід з IPv4 на IPv6 в одну мить неможливо, але з використанням періоду співіснування IPv4 та IPv6 цей перехід стає більш реальним. Під час фази міграції можуть бути розгорнуті такі методи як подвійний стек, тунелювання. По можливості використовують вузли подвійного стеку і вузли з підтримкою IPv4 і IPv6 одночасно. Де ця можливість відсутня, механізм тунелювання може бути розгорнутий для з'єднання IPv6 вузлів через мережу IPv4. Але ці механізми пов'язані з деякими проблемами, серед яких такі:

– ***механізми тунелювання використовуються по різному:*** деякі використовуються для з'єднання IPv6 сайтів поверх IPv4-мереж (наприклад, 6in4, 6to4, 6RD), тоді як інші використовують надання індивідуального підключення подвійного стека до мережі IPv6 (наприклад 6over4, ISATAP, Teredo). Механізм тунелювання є вразливим до ін'єкції пакетів (наприклад для відбиття DoS-атак). Контрзаходами, є встановлення відповідної фільтрації на кінцевих точках тунелю, наприклад для джерела IPv4 та IPv6-адреси або розгортання IPsec для всіх тунелів трафіку. Крім того, деякі механізми тунелю (6to4, 6RD, ISATAP і Teredo) також уразливі до DNS атак у випадку, якщо кінцеві точки тунелю було виявлено використовуючи DNS.

Teredo забезпечує з'єднання для вузлів подвійного стека за межами NAT. Тим не менш, його використання має бути обмеженим, оскільки Teredo вимагає відкриття порту у фаєрволі мережі, що може бути використаний для атаки. Тому необхідно мати фаєрвол з функцією налаштування для використання Teredo, та спеціаліста, що може його правильно налаштувати;

– ***вразливість операційних систем на робочих хостах мережі:*** у минулому було виявлено кілька помилок у основних операційних системах для хостів та маршрутизаторів, які стосуються подвійного стеку. Наприклад, мала місце вразливість віддаленого виконання коду, що використовувала спеціально створені ICMPv6 Router сповіщення чи ICMPv6 Router інформаційні пакети. Також пристрій міг зазнати аварії у випадку отримання спеціального заголовку IPv6 Type 0 Routing. Ця помилка вже виправлена, але оновлення, що включає (це виправлення), залежить від обізнаності користувачів корпоративної мережі. Також ще більше помилок може бути знайдено через масштабне розгортання мережі;

– ***відсутність обізнаності в особливостях IPv6:*** в деяких операційних системах використання IPv6 включено, але за замовчуванням, наприклад Microsoft Vista (2007), Linux 2.6 kernel, Apple OS/10.3 (2002) та ін. Користувачі та деякі адміністратори можуть не знати

цього, і таким чином, захист від IPv6 атак може бути не належної якості за налаштуваннями. Отже, впровадження IPv6 також потребує підвищення практичного досвіду користувачів;

– ***атаки подвійного стеку:*** протягом перехідного процесу, необхідно враховувати можливі атаки як для IPv4 так і для IPv6 мереж. Як правило, комп'ютерний вірус, який вразив один вузол, буде шукати інші вузли для розповсюдження загрози у цій локальній підмережі. У випадку з IPv4 мережами, це досягається шляхом сканування (brute force scan). У випадку з IPv6 мережами сканування не можливе, але вірус може використовувати багатоадресний IPv6 пінг (ICMPv6 exo запит на групу адресів, наприклад FF02::1) для того, щоб знайти активні вузли. Таким чином, поширення вірусу у подвійному стеку може бути навіть швидше ніж у мережі IPv4. Контрзаходами є фільтрування ICMPv6 exo-запитів з груповою адресою призначення.

Слід відмітити, що існує протокол перетворення між IPv6 та IPv4 (протокол NAT-PT) який необхідний у випадку, коли вузли з підтримкою IPv6 планують використовувати модель безпеки IPv6 та подвійного стеку (IPv6/IPv4). Але NAT-PT включає в себе деякі проблеми розгортання. Наприклад, перетворення IP-заголовків недостатньо при використанні IP-адреси на високих рівнях протоколів (наприклад, SIP та SDP), так як потрібні шлюзи прикладного рівня для кожного з цих протоколів, які повинні бути поєднані з функціональністю NAT-PT. Тим не менш, ALGs (шлюзи прикладного рівня) не можуть працювати з трафіком, що є захищеним за допомогою IPsec або TLS.

Сценарій "мобільний користувач". У цьому сценарії, про який вже йшла мова у попередньому розділі статті, йдеться про реалізацію служби мобільності за допомогою розгортання Mobile IP. Рухливі опорні точки, домашні точки, управляються від мобільного оператора, який може бути або не бути авторизованим мобільним сервісом для конкретного мобільного вузла (мобільного пристрою, ноутбука, КПК або смартфону). Однією з ключових переваг Mobile IPv6 у порівнянні з Mobile IPv4 є стандартизований безпечний процес початкового налаштування Mobile IPv6. Таким чином, мобільний вузол автоматично дізнається адресу домашньої точки (яка обрана постачальником мобільного зв'язку за рахунок внутрішньої політики), домашню адресу (постійну IP-адресу), та налаштування безпеки. Крім того, для Mobile IPv6, стандартизовані AAA інтерфейси та повідомлення протоколу є чітко визначеними, що дає змогу на розгортання Mobile IPv6 для мобільних операторів.

На противагу цьому, для Mobile IPv4 необхідні негнучкі статичні конфігурації початкового налаштування чи масштабна робота зі стандартизації послуг. Крім того, у разі Mobile IPv6 розгортання IPsec (який має високий ступінь захисту, перевірений часом, і забезпечує шифрування) разом з IKE були стандартизовані для захисту зв'язку між мобільним і домашнім вузлом, в той час як в Mobile IPv4 захист зв'язку забезпечується конкретним модулем перевірки аутентифікації (яка не забезпечує шифрування і не перевірена як IPsec). Більше того, у випадку Mobile IPv6 надійність протоколу домашнього вузла в даний час знаходиться на стадії стандартизації і механізм розподілу навантаження був розроблений, для забезпечення стійкості до збоїв і атак (наприклад, атак відмови в обслуговуванні домашніх агентів) [3].

Співіснування IPv6/IPv4 можливе у випадку коли мобільний вузол приєднаний тільки до мережі доступу IPv4, у той час як мобільність обслуговування заснована на використанні Mobile IPv6. Подвійний стек Mobile IPv6 (DSMIPv6) є стандартизованим рішенням для цього

сценарію. У випадку, коли DSM IPv6 розгорнутий одночасно з NAT, протокол вразливий проти атаки Man In The Middle зовні заголовка IPv4 для виконання перенаправлення атаки. Тим не менш, ця вразливість присутня у MIPv4 з використанням NAT, що не є проблемою для IPv6.

Повідомлення, які повинні пройти фаєрвол, є сигнальними повідомленнями Mobile IPv6 (BU і BA захищені IPsec), IKE повідомлення (порт 500 або 4500), AAA повідомлення (наприклад, RADIUS (порт 1812) або Diameter (порт 3868)), та пакети даних користувача. Загальна проблема в цьому сценарії – це небажані повідомлення (без попереднього запиту), які можуть бути проблемою для фаєрволу, який просто пропускає трафік, якщо це треба. Тобто фаєрвол створює декілька станів для вихідних повідомлень і пропускає повідомлення, що мають необхідний стан.

Висновки. З'ясовано, що протоколи IPv6 та IPv4 використовують ті ж самі механізми безпеки по відношенню до IPsec. Однак, розгортання IPv6 є більш ефективним, так IPv6 забезпечує прозорий end-to-end зв'язок, чим спрощується його модель безпеки (наприклад з використанням IPsec/IKE end-to-end) без розгляду питань служб NAT. Більш точна політика безпеки та правила фільтрації можуть бути встановлені при використанні унікальних адрес. Також IPv6 надає можливість end-to-end идентифікації та аутентифікації.

Разом з тим, особливо в Україні, деякі інструменти безпеки та програмного забезпечення частково не готові до використання IPv6 або ще не перевірені (наприклад, фаєрволи для кишенькових комп'ютерів або мережі моніторингу та інструменти аудиту), і це вимагає та передбачає розвиток профільних спеціалістів та ретельного тестування. Деякі сценарії демонструють конкретні переваги безпеки IPv6. Наприклад, сценарій «Мобільний користувач» при використанні IPv6, кращий, завдяки стандартних безпечних процесів налаштування та завантаження певних інтерфейсів між Mobile IPv6 та AAA інфраструктурою.

Література

1. Tatipamula M. IPv6 integration and coexistence strategies for next-generation networks / M. Tatipamula, P. Grossetete // Communications Magazine, IEEE. –2004. –Vol. 42, № 1. – P. 88-96.

2. Wiljakka J. Transition to IPv6 in GPRS and WCDMA mobile networks / J. Wiljakka // Communications Magazine, IEEE. – 2002. – Vol. 40, № 4. – P. 134-140.

3. Платонов В. В. Программно-аппаратные средства защиты информации : учеб. пособие / В. В. Платонов. – М. : Академия, 2013. – 336 с.