УДК 004.051 DOI: 10.31673/2518-7678.2023.020707

Гніденко М.П., к.т.н., **Прокопов С.В.,** к.т.н.,
Гніденко М.М.

ПІДВИЩЕННЯ БЕЗПЕКИ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ (SDNs)

Hnidenko M.P., Prokopov S.V., Hnidenko M.M. Enhancing the security of Software-Defined Networks (SDNs).

Software-defined networking (SDN) is an emerging paradigm, which breaks the vertical integration in traditional networks to provide the flexibility to program the network through (logical) centralized network control. SDN has the capability to adapt its network parameters on the fly based on its operating environment. The decoupled structure of SDN serves as a solution for managing the network with more flexibility and ease. In SDN, the centralized cost effective architecture provides network visibility which helps to achieve efficient resource utilization and high performance. Due to the increasingly pervasive existence of smart programmable devices in the network, SDN provides security, and network virtualization for enhancing the overall network performance. The work presents various security threats that are resolved by SDN and new threats that arise as a result of SDN implementation. The recent security attacks and countermeasures in SDN are also summarized in the form of tables. Also provided a survey on the different strategies that are implemented to achieve energy efficiency and network security through SDN implementation. In an effort to anticipate the future evolution of this new paradigm, were discussed the main ongoing research efforts, challenges, and research trends in this area. With this work, researchers and students can have a more thorough understanding of SDN architecture, different security attacks and countermeasures.

Keywords: Software-defined networks (SDNs), SDN security, OpenFlow network.

Гніденко М.П., Прокопов С.В., Гніденко М.М. Підвищення безпеки програмно-визначених мереж (SDNs).

Програмно-визначена мережа (SDN) — нова парадигма, яка порушує вертикальну інтеграцію в традиційних мережах, щоб забезпечити гнучкість програмування мережі через (логічне) централізоване керування мережею. У роботі представлені різні загрози безпеці, які вирішуються SDN, і нові загрози, які виникають в результаті впровадження SDN. Нещодавні атаки на безпеку та контрзаходи в SDN також підсумовані у формі таблиць. Також надано опитування щодо різних стратегій, які реалізуються для досягнення енергоефективності та безпеки мережі через впровадження SDN. Щоб передбачити майбутню еволюцію цієї нової парадигми, було обговорено основні поточні дослідницькі зусилля, виклики та тенденції досліджень у цій галузі. Завдяки цій роботі дослідники та студенти можуть мати більш повне розуміння архітектури SDN, різних атак на безпеку та заходів протидії.

Ключові слова: Програмно-визначені мережі (SDNs), безпека SDN, мережа OpenFlow.

Вступ

Захист мережної інфраструктури різного призначення від різних видів атак є надзвичайно актуальним завданням, оскільки від ефективного його вирішення залежить її стійкість і безперервна висока продуктивність. Існує багато різних принципів і методів мережевої безпеки, які можуть бути використані для захисту мережі. Загалом, це поширені практики, такі як правильне налаштування мережі, захист від вторгнень, захист від вірусів і шкідливих програм, захист від програм для злому паролів, захист від переходу за межі мережі і використання антивірусного програмного забезпечення.

Аналіз останніх досліджень і публікацій. Однак програмно-визначені мережі SDN належать до мереж нового типу, особливість роботи яких міститься в централізації управління мережею, постійним моніторингом стану та швидкою реакцією на появу традиційних загроз. Крім того, зараз існує уявлення, що SDN було розроблено для забезпечення гнучкості конфігурації мережі та покращення загальної продуктивності мережі. Але з самого початку ідея SDN виникла саме для вирішення проблеми безпеки мереж [1, 4].

У 2006 році науковці компанії HPE і Stanford University співпрацювали над проектом “Ethane”. Програма Clean Slate, в межа цього проекту, поставила запитання: якби ми почали будувати мережі заново — без будь-яких традиційних методів — як би ми їх побудували? Чи виглядала б мережева технологія так, як вона виглядає сьогодні, чи виглядала б інакше?

Відповідь, яка була отримана за допомогою Clean Slate, полягає в тому, що повинна існувати система контролю та управління. Сама мережа має керуватися цілями мережевого рівня (а не конфігураціями розподілених пристроїв). Крім того, ця централізована система зможе контролювати всю мережу та приймати оптимальні, розумні та передбачувані рішення щодо того, як трафік має перенаправлятися та маршрутизуватися по всій мережі.

Ця центральна система керування — під назвою ”Ethane” — використовувала інформацію про політику та базу даних різноманітної інформації (топологія, реєстрація та прив’язки) для адміністрування правил щодо доступу окремих пристроїв до мережі (рисунок 1). Завдяки централізованому управлінню переадресацією між мереживими пристроями, стає неможливим зловмисне перенаправлення трафіку з метою крадіжки інформації, що підвищує безпеку мережі.

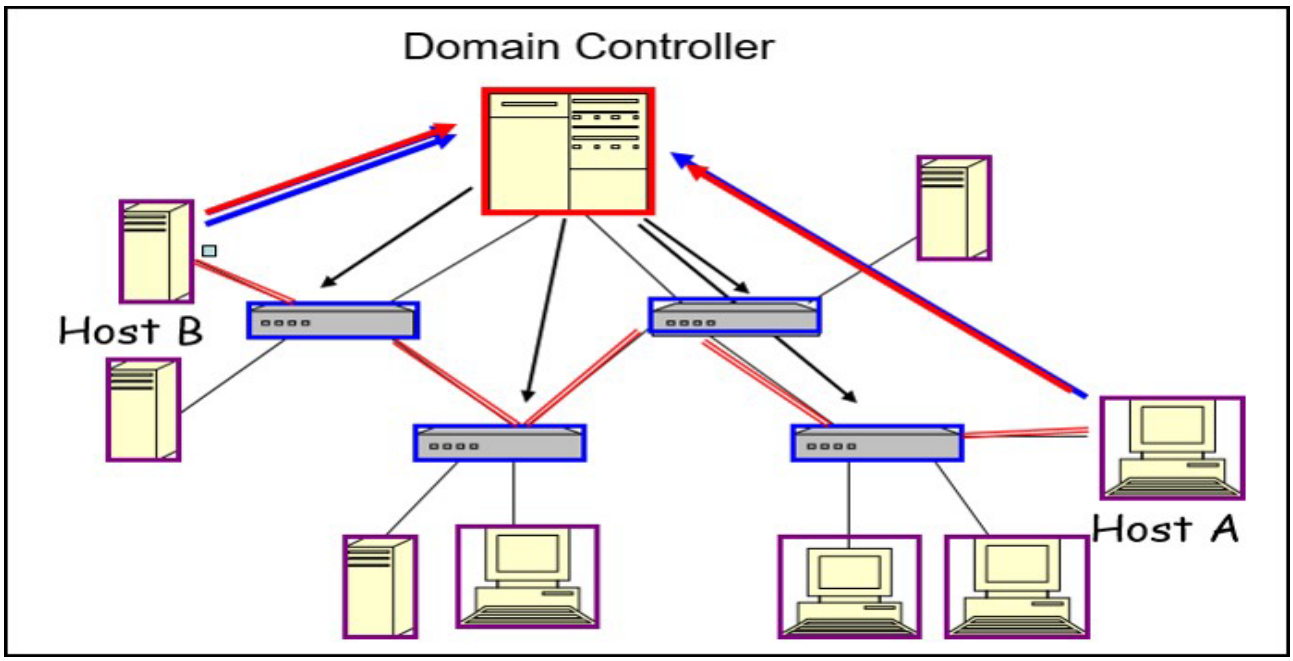

Рисунок 1 – Централізоване управління переадресацією трафіку.

“Ethane” є свого роду рішенням для контролю доступу до мережі (network access control - NAC). Типові системи NAC потребують функціональних можливостей керування на пристрої (наприклад, RADIUS або адаптивного порталу) або функціональних можливостей у спеціальному вбудованому пристрої для досягнення бажаної функціональності. Це рішення було досягнуто без спеціального програмного забезпечення на пристрої чи приладі — усе це було зроблено за допомогою простих пристроїв, які виставляли свої «таблиці потоку» центральному контролеру.

Таким чином SDN — це нова технологія, яка може забезпечити рішення для підвищення безпеки від традиційних загроз, оскільки вона здатна виявляти атаки та діяти адаптивно швидше, ніж традиційні мережі. Однак останнім часом з’явилися нові види атак, націлені безпосередньо на SDN [2,3]. У зв’язку з цим зараз виникає і стає невідкладною необхідність шукати нові підходи для підвищення безпеки SDN мереж.

Постановка завдання. Впровадження SDN в інфраструктуру мереж та підвищення безпеки програмно-визначених мереж (SDNs) від різних видів атак має як плюси так і мінуси із за її подвійної природи. Як було показано вище, з однієї сторони, природа SDN мереж тісно пов’язана із можливістю підвищення безпеки і ця функція реалізується через централізовану гнучку систему контролю та управління. У зв’язку з цим необхідно проаналізувати типові

програми безпеки SDN, які нативно вирішують проблеми безпеки від різних видів атак, таких як атаки вторгнення, аномальні атаки та DDoS атаки. Дослідження варіантів захисту, які реалізуються за допомогою адаптивності та програмованості системи SDN, дозволяє виявити основні проблеми безпеки. Вірна оцінка потенційної ефективності реакції на загрози системи SDN має надати можливість розширити функції програмування. Однак є кілька нових загроз, які виникають у результаті впровадження SDN. Зауважимо, що атаки є поширеними в SDN, оскільки він здебільшого залежить від програмного забезпечення для визначення своєї поведінки, що може поставити під загрозу безпеку всієї системи, що робить можливим для зловмисників проникнути в систему. У зв'язку з цим, необхідно розглянути атаки на безпеку від нових видів загроз, а також проблеми та контрзаходи в SDN. Уразливості безпеки в SDN можуть поставити під загрозу всю мережу та погіршити продуктивність. У зв'язку з цим необхідно дослідити не лише атаки проти програмованого контролера SDN, як рівня управління, який є найбільш очевидною мішенню для зловмисників, але і атаки на інші складові системи: прикладному рівні, рівні даних, мережних комутаторів, каналів передачі, протоколу OpenFlow [2,4]. Різноманітність форм, видів, напрямів та рівнів атак ускладнює пошук ефективних методів захисту, але в той же час представляє собою невідкладне завдання, яке вимагає свого обов'язкового вирішення.

Метою дослідження є підвищення ефективності протидії від різних видів атак та безпеки програмно-визначених мереж (SDNs).

Виклад основного матеріалу досліджень.

Різні загрози безпеці, які можна усунути за допомогою SDN, підсумовано в таблиці 1. У цій таблиці надано визначення різних типів загроз. Детальний опис можливих контрзаходів і їх застосування обговорюється нижче.

Таблиця 1 - Типові програми безпеки SDN як парадигми безпеки.

Атаки	Загрози	Програми
Атаки вторгнення	Атака вторгнення створює доступ до системи без дійсних дозволів і ставить під загрозу безпеку та стабільність системи.	1. Хмарні обчислення. 2. Розумні мережі. 3. Віртуальні машини.
Аномальні атаки	Атаку спричинив невідомий користувач, порушивши політику та поставивши під загрозу всю систему.	1. Хмарні обчислення.
DDoS атаки	DDoS атака — це різновид атаки, при якій система атакується з кількох джерел розподіленим способом, створюючи відмову в обслуговуванні для дійсних користувачів.	1. Хмарні обчислення. 2. Мобільна інфраструктура

SDN як Intrusion Detection System (IDS) та Intrusion Prevention System (IPS):

Атака вторгнення — це несанкціонована діяльність у мережі, коли атаки поглинають мережеві ресурси, призначені для інших цілей. Завдяки можливості реконфігурації та програмуванню SDN, SDN можна реалізувати як IDS та IPS для постійного моніторингу мережевої діяльності для виявлення атак вторгнень. Найпоширеніші вектори атак вторгнень, від яких можна захиститись за допомогою адаптивності та програмованості SDN, є наступними:

атака з асиметричною маршрутизацією: зловмисник використовує більше одного маршруту до цільового мережевого пристрою, щоб обійти певні сегменти мережі та датчики вторгнення. Якщо мережі не налаштовані на асиметричну маршрутизацію, вони вразливі до цієї атаки;

атаки на переповнення буфера: ця атака перезаписує певні розділи пам'яті пристрою цільової мережі або замінює звичайні дані в певних місцях пам'яті шкідливим програмним забезпеченням для атаки на мережу з метою ініціювання відмови в обслуговуванні;

атаки, пов'язані з конкретними протоколами: мережеві протоколи, такі як TCP, UDP, ARP, IP, ICMP тощо, можуть ненавмисно залишити «задні двері» (backdoor) для вторгнень у мережу через підробку або подібне з метою компрометації чи навіть збою цільових пристроїв в мережі. Наприклад, під час зіставлення мережевих IP-адрес з фізичними адресами протокол ARP не виконує автентифікацію повідомлень, що дозволяє зловмисникам виконувати атаки типу «людина посередині»;

атаки з переповненням трафіку: зловмисник може створити занадто велике навантаження на трафік, щоб мережа перевантажила загальні ресурси мережі. Ці атаки можна легко контролювати за допомогою SDN;

атака на основі трояна: ця атака викликає DoS-атаки, стирає збережені дані або відкриває «задні двері» (backdoor), щоб дозволити зовнішнім зловмисникам контролювати систему.

Існують різні рішення захисту на основі SDN, які обговорюються нижче. CloudWatcher було запропоновано для керування потоком трафіку в SDN за допомогою програмної логіки та ефективного його маршрутизації через усі компоненти безпеки, присутні в інфраструктурі, такі як IDS мережі та брандмауери. Це запобігає проникненню шкідливих пакетів, які можуть становити загрозу для мережі.

Виявлення мережевого вторгнення та вибір заходів протидії у віртуальних мережевих системах (Network Intrusion detection and Countermeasure sElection - NICE) були запропоновані як для виявлення, так і для запобігання вторгненням. NICE має чотири модулі: NICE-A, профілювання віртуальної машини, аналізатор атак і контролер мережі. NICE-A працює як ідентифікатор мережі, профілювання віртуальних машин зберігає повну інформацію про дії віртуальних машин (включно з умовами трафіку, відкритими портами, уразливими місцями та попередженнями безпеки тощо), аналізатор атак відповідає за аналіз атак і забезпечення заходів протидії, а мережевий контролер допомагає аналізатору, повідомляючи повну інформацію про стан мережі.

Підходи до виявлення на трасі та виявлення поза трасою також були запропоновані. Під час виявлення на шляху підозрілі пакети виявляються шляхом підключення системи IDS на шляху переміщення пакетів. Це ефективніше, ніж виявлення поза маршрутом, коли IDS приєднується до системи як окремий фізичний модуль. Іншою функцією безпеки є здатність IDS повідомляти контролеру про підозрілі дії за допомогою сповіщень/сигналів тривоги, щоб контролер міг негайно вжити заходів для пом'якшення атак.

IDS і IPS були інтегровані з SDN для аналізу атак у мережі та забезпечення відповідних заходів протидії атакам. Контролер мережі використовується для збору необхідної інформації для аналізатора атак для виявлення цих загроз/атак.

SDN реалізовано разом із видатною системою IDS під назвою Snort для виявлення загроз у розширеній інфраструктурі вимірювання (Advanced Metering Infrastructure AMI), яка популярна в розумних енергетичних мережах. Автономний IDS не може запобігти проникненню зловмисного програмного забезпечення в систему, тому SDN вбудовано разом з ним, щоб охороняти та захищати систему. Snort виявляє зловмисне програмне забезпечення на основі попередньо визначених правил. Це різні методи включення Snort у SDN, включаючи дзеркальну реалізацію та підхід застосування повідомлення PACKET_IN. У дзеркальній реалізації Snort підключається до комутатора OpenFlow у SDN, де весь трафік проходить через комутатор OpenFlow і Snort для виявлення підозрілої активності. У підході PACKET_IN Snort працює як фонова програма, підключена до контролера OpenFlow, і контролеру повідомляється лише про підозрілу активність. Обмеження цих методів полягає в тому, що може виникнути перелив трафіку в мережі.

Запропоновано новий метод інтеграції, де правила Snort вбудовані в комутатори OpenFlow, і Snort починає діяти лише тоді, коли в системі є якась підозріла активність. Додаткові функції також вбудовано в OpenFlow, який включає сервер керування до контролера та агентів перевірки політики в комутаторах. Прозорі системи запобігання

вторгненням (Transparent Intrusion Prevention Systems - TIPS) були запропоновані для запобігання атакам вторгнень шляхом інтеграції SDN і обробки пакетів у режимі опитування. SDN-IPS було запропоновано для запобігання атакам вторгнень у мережі з високою ефективністю.

SDN для виявлення аномалій:

Виявлення аномалій (або виявлення викидів) у мережі — це ідентифікація подій або спостережень, які не відповідають очікуваній моделі. У наші дні атаки стають все більш витонченими, що ускладнює відстеження фактичного походження атаки. Технологія SDN дає нам привілей налаштовувати пристрої відповідно до наших потреб. Наприклад, домашній маршрутизатор, налаштований за допомогою SDN, ефективно виявляє шкідливі та шпигунські програми, які атакують систему. Графічний підхід, який був запропонований, покладається на комутатори на основі OpenFlow для відстеження походження атак, де можна визначити всі шляхи, вразливі до атак аномалій.

З впровадженням SDN спільне виявлення може бути реалізовано через уже наявний централізований контролер SDN, де кожен комутатор або хост повідомляє централізованому контролеру своє рішення щодо виявлення атак. Для двійкової змінної рішення $d_i \in \{0, 1\}$ кожного комутатора/хоста $i = 1, 2,...,N$, щоб прийняти рішення (D) про атаку, контролер SDN може використовувати логічну AND операцію (U) як:

$$D = \cup_{\forall i} d_i \tag{1}$$

або логічну OR операцію (П) як:

$$D = \Pi_{\forall i} d_i \tag{2}$$

Зауважимо, що оператор AND в (1) говорить про наявність атаки, коли $d_i = 1, \forall_i$ і тому цей підхід є більш обмежувальним/консервативним. У той час як оператор OR в (2) говорить про наявність атаки, коли будь-який з d_i є істинним, що робить його найменш консервативним. Таким чином, альтернативним підходом може бути рішення, засноване на більшості

$$D = 1 \text{ if } \sum_{i=1}^{N} d_i > \frac{N}{2}, \quad d = 0 \tag{3}$$

яка може бути більш прийнятною схемою для підвищення ефективності виявлення аномалій.

SDN для виявлення та запобігання DDoS атак:

DDoS атаки позбавляють легальних користувачів доступу до мережевих сервісів. Ці атаки можуть завдати значної шкоди, скомпрометувавши всю мережу. Звичайні мережі мають деякі методи виявлення DDoS атак і захисту мереж, але не пропонують дуже надійних і гнучких рішень для захисту. Завдяки програмованим функціям і реконфігураційному характеру SDN можна розробити, розгорнути та оцінити гнучкі та надійні підходи для виявлення та запобігання DDoS атак [1,3].

Мобільні пристрої стали потужнішими порівняно з минулим і використання цих пристроїв експоненціально зростає. Це збільшує ймовірність атак, у тому числі DDoS атак у мережі. Підхід до виявлення зловмисного програмного забезпечення для мобільних пристроїв було запропоновано, коли мобільний трафік від точок доступу спрямовується до контролера, підключеного до детектора зловмисного програмного забезпечення. Нижче наведено чотири алгоритми виявлення шкідливих програм:

чорний список IP-адрес: у системі зберігається список усіх підозрілих IP-адрес. Коли комутатори надсилають невідповідні пакети до контролера OpenFlow, він перевіряє IP-адресу, щоб побачити, чи є вона з чорного списку і відкидає пакет, якщо IP-адресу знайдено в цьому чорному списку;

коефіцієнт успішності підключення: якщо кількість невдалих підключень користувачів перевищує фіксоване порогове значення, тоді користувача ідентифікують як зловмисного:

регулювання з'єднання: шкідливий пристрій/хост, який намагається атакувати багато систем, визначається на основі списку нещодавно доступних хостів (RAH), який

підтримується в системі. Якщо список очікування хоста перевищує фіксоване порогове значення, тоді користувач ідентифікується як зловмисник;

сукупний аналіз: якщо один хост у мережі захищено зловмисною діяльністю, безпека інших користувачів у мережі також під загрозою. Цей алгоритм працює для виявлення інших інфікованих хостів на основі подібності (тобто часу підключення, місця призначення та однієї платформи).

Інтеграція SDN для мобільної хмарної інфраструктури була додатково досліджена для розробки складних механізмів для захисту мережі. Основною причиною виникнення DDoS атак в системі є бот мережі. Протокол для легкого відновлення після DDoS атак ботнету розроблено, де контролер SDN розширено модулем блокування DDoS. У SDN було використано для використання підходу Remote Triggered Black Hole (RBTH) для запобігання DDoS атак. Контролер SDN відіграє важливу роль у виявленні зловмисного трафіку, спрямованого від комутатора OpenFlow і відкидає його, щоб запобігти подальшому пошкодженню мережі. Крім того, було запропоновано розподілену структуру спільної роботи, щоб забезпечити автономне пом'якшення атак DDoS шляхом уникнення витоку конфіденційності та інших юридичних проблем.

Як обговорювалося вище, SDN пропонує рішення для захисту від різноманітних атак для забезпечення безпеки за допомогою функцій програмування. Однак є кілька нових загроз, які виникають у результаті впровадження SDN. Зауважимо, що атаки є поширеними в SDN, оскільки він здебільшого залежить від програм/програмного забезпечення для визначення своєї поведінки, що може поставити під загрозу безпеку всієї системи, що робить можливим для зловмисників проникнути в систему. У зв'язку з цим, представляємо атаки на безпеку, проблеми та контрзаходи в SDN. Уразливості безпеки в SDN можуть поставити під загрозу всю мережу та погіршити продуктивність. Атаки на SDN можуть відбуватися в різних модулях, таких як контролер, віртуальні машини та комутатори OpenFlow. Існує кілька атак, які виникають разом із впровадженням SDN. Типові вектори атаки та місця їх появи в SDN показані на рисунку 2.

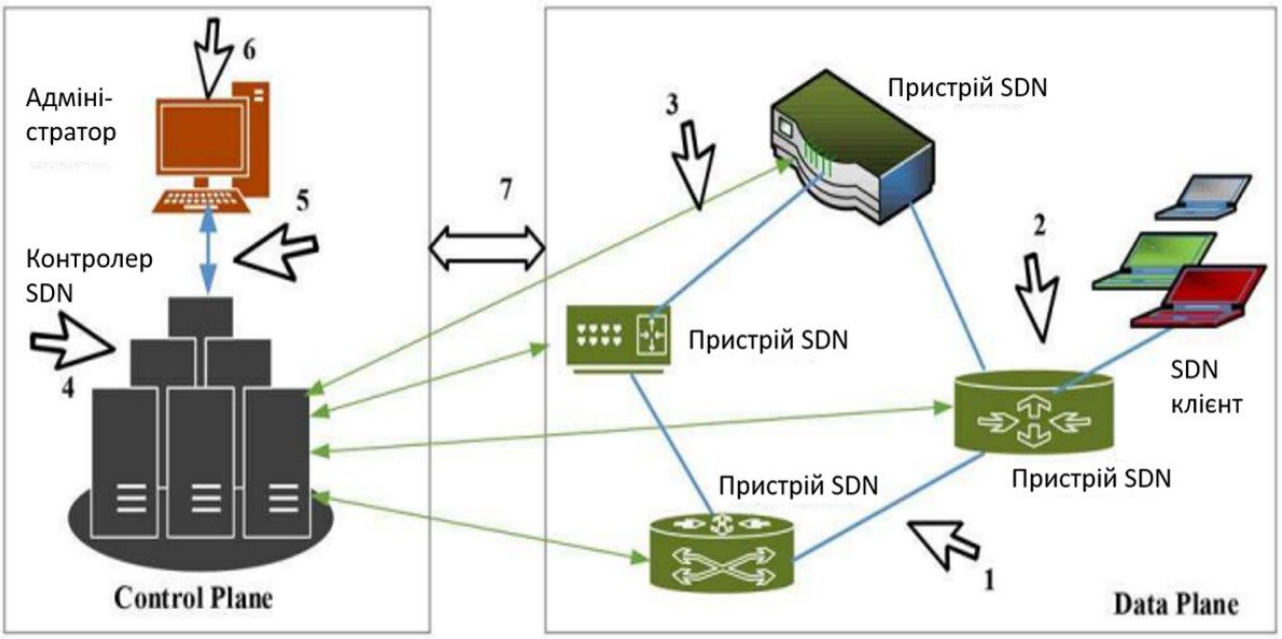

Рисунок 2 – Вектори загроз в SDN

Нижче наведено опис кожного вектору загрози, наведеного на рисунку 2:

вектор загроз 1 представляє фальшиві потоки трафіку, які виникають під час взаємодії пристроїв SDN у площині даних. Атака може відбуватися з використанням підробленої ідентифікації легітимних потоків або підробленої ідентифікації пристрою;

вектор загрози 2 представляє атаки на комутатори SDN у площині даних, які можуть відбуватися через вхідний і вихідний потік трафіку;

вектор загрози 3 представляє атаки, які можуть виникнути під час зв'язку пристроїв рівня даних із пристроєм рівня керування (контролером);

вектор загрози 4 представляє атаки на контролер;

вектор загрози 5 представляє атаки, які відбуваються між контролером і пристроями прикладного рівня (включаючи системи адміністрування);

вектор загрози 6 представляє атаки на станцію адміністратора, яка пов'язана з контролером;

вектор загрози 7 представляє атаки, спрямовані на обмін даними між рівнем даних і рівнем додатків.

Для захисту від цих векторів загрози були запропоновані захисні рішення, але більшість із них ще відкриті для вивчення. У таблиці 2 показані різні атаки в SDN, які відбуваються на різних рівнях і наводяться результати виникнення цих атак разом із методами пом'якшення, щоб запобігти цим атакам. Опис загроз на різних рівнях детально обговорюється нижче:

Таблиця 2 - Атаки на безпеку та заходи протидії в SDN.

Атаки	Вражені рівні	Результат атаки
Спуфінгова атака	Рівень даних. Інтерфейс контролю рівня даних.	Модифікація правила. Витік даних. Шкідливі програми.
Атаки вторгнення	Рівень даних. Рівень управління. Інтерфейс рівня контролю даних. Прикладний рівень. Інтерфейс контролю прикладного рівня.	Шкідливі програми. Несанкціонований вхід. Витік даних. Введення помилок. Збої програми/
Аномальні атаки	Прикладний рівень. Рівень управління. Рівень даних.	Витік даних. Модифікація даних. Несанкціонований доступ.
DoS і DDoS атаки	Рівень управління. Рівень даних. Інтерфейс контролю рівня даних.	Відмова служб. Затоплення контролера. Затоплення потокових записів.

контролер є найбільш очевидною мішенню для зловмисників, оскільки вся функціональність і поведінка мережі залежать від контролера. Після того, як контролер заблоковано, він може становити загрозу для всієї мережі. Вектори загрози 3, 4 і 5 пов'язані з площиною управління. Атаки можуть бути спрямовані з різних модулів, включаючи комутатори на рівні площини даних, північний інтерфейс, південний інтерфейс і прикладний рівень. DoS/DDoS, аномалії та атаки вторгнення є можливими атаками, які можуть виникнути в площині управління;

комутатори в SDN здатні виконувати лише мінімальні завдання, такі як пересилання пакетів. Однак загроза комутаторам може завдати величезної шкоди всій мережі. Вектори загрози 1 і 2 пов'язані з уразливими місцями в комутаторах. DoS, DDoS, атаки спуфінгу та атаки вторгнення – це деякі атаки, пов'язані з площиною даних;

вектори загроз 5, 6 і 7 пов'язані з атаками на прикладному рівні. Атаки, пов'язані з програмним забезпеченням, такі як помилки, збій програм, ін'єкція шкідливих програм, аномалії та атаки вторгнень є найпоширенішими загрозами на цьому рівні;

вектори загроз 3, 5 і 7 пов'язані з атаками на інтерфейси. Інтерфейси відіграють важливу роль у забезпеченні зв'язку між двома площинами. Більшість атак на інтерфейси схожі на

атаки, які відбуваються в інших площинах. Якщо інтерфейс скомпрометовано, це дозволяє обмінюватися зловмисним трафіком у системі.

Методи виявлення та пом'якшення вищезгаданих атак докладно наведено нижче та приведено відповідне обгрунтування.

DDoS і DoS атаки в SDN.

Контролер SDN відіграє вирішальну роль у визначенні функціональності архітектури SDN, тому контролер став однією з головних цілей для DDoS/DoS атак. Деякі вразливі можливості в контролерах на основі FloodLight спонукають DDoS/DoS атаки. Зв'язки між комутаторами та контролером є предметом інтересу для проведення цих атак. Ці атаки можна пом'якшити, увімкнувши суворі механізми автентифікації транспортного рівня (Transport Layer Security - TLS) у каналах зв'язку між комутаторами та контролерами, а також надавши перевагу існуючим з'єднанням над новим з'єднанням. Зауважимо, що атаки DDoS можна виявити за допомогою методів, запропонованих для традиційних мереж, однак ті самі методи захисту, запропоновані для традиційних мереж, не можуть бути реалізовані безпосередньо в SDN через відмінності в архітектурі. Ідеї, запропоновані для традиційних мереж, можуть бути запозичені при розробці методів виявлення атак для SDN.

Типові DDoS атаки неможливо відстежити, оскільки вони здійснюються ботнетами з автоматизованими діями. Для виявлення DDoS атак існують різні підходи, які можуть легко виявити ботнети. Протоколи та IP-адреси можна перевірити для виявлення DDoS атак, однак ботнети можуть підробити ідентифікаційні дані, підробивши легальні адреси. У цьому випадку система виявлення може бути не в змозі виявити атаки, оскільки зловмисник підробляє протоколи та IP-адреси, які здаються законними для зловмисних законних користувачів або ботнетів. Крім того, DDoS атаки можуть відбуватися через випадковий інтервал і випадковий час і вони є постійними. Важливі рішення захисту від атак DDoS коротко обговорюються нижче:

розпізнавання шаблону атаки: якщо атака відбувається через певні проміжки часу, наприклад, у будь-яку задану дату та час і повторюється протягом однакових інтервалів, таких як рік або місяці, тоді модель атаки може бути розпізнана. Можна оцінити тривалість нападів і наскільки довго вони продовжуються. Характер атаки та пакети атак можуть дати нам натяк на те, який вид атаки здійснюється. Якщо цю інформацію можна зареєструвати, щоб створити базу даних із попереднього досвіду атаки для генерування статистики, тоді це означає, що модель атаки можна розпізнати;

кластеризація системи для додаткової безпеки: для наданої системи DDoS можна звести нанівець або зробити її складною шляхом кластеризації системи. Для кожного створеного кластера можна додати автентифікацію користувача. З вимогою автентифікації користувача необхідна додаткова довіра, щоб проникнути та спричинити хаос. Таким чином, кластеризація системи може забезпечити додатковий рівень безпеки, щоб мати можливість фільтрувати атаки. Крім того, якщо атака здійснюється на один кластер системи, інша частина кластера може бути безпечною, а не вся система схильна до DDoS атак;

виявлення високошвидкісної системи визначення рівня потоку (HiFIND): щоб виявити DDoS атаку та забезпечити істотний захист жертви та постачальника послуг, можна використовувати HiFIND. Він високо захищений завдяки великій ємності та стійкості до атак DDoS для пакетів даних високої щільності. Таким чином, HiFIND менш схильний і дуже стабільний, коли справа доходить до DDoSатак, спрямованих на слабкішу систему.

Було запропоновано легке виявлення DDoS атак, яке є схемою виявлення на основі карти, натхненною технікою самоорганізуючої карти (SOM). Це триетапний процес, який складається зі збирача потоку, екстрактора ознак і класифікатора. Екстрактор потоку використовується для збору статистики потоку з комутаторів OpenFlow. Екстрактор функцій вибирає конкретну інформацію, необхідну для виявлення, на основі того, який класифікатор визначає законного користувача. Підхід захисту безпеки під назвою Damask був запропонований у для захисту SDN від атак DDoS.

Ентропійний метод був запропонований для виявлення DDoS атаки на контролер за допомогою порогового значення. Ентропія IP-адрес обчислюється після кожних 50 вхідних пакетів і якщо вона перевищує порогове значення, це означає, що в системі є підозріла активність. Ці атаки в основному спрямовані під час спілкування з комутаторами. Інфіковані комутатори надсилають величезну кількість запитів і контролер буде задіяний у відповіді на ці підроблені запити, відхиляючи запити законних користувачів. Ця атака завдає прямої шкоди законним користувачам. Ці атаки можна пом'якшити, захистивши контролер від цих шкідливих потоків.

TopoGuard було розроблено доповнення безпеки до контролера OpenFlow для усунення вразливостей у топології мережі. Мережеві атаки стали найпоширенішими для багатьох контролерів, доступних на сьогоднішньому ринку, таких як Flood-light, Beacon і POX. Він зосереджений на заходах проти вразливостей, пов'язаних зі службами відстеження хостів і виявленням посилань у контролері OpenFlow. Ця архітектура підтримує запис профілю хоста, який включає MAC-адресу, IP-адресу та інформацію про місцезнаходження, щоб забезпечити безперебійне обслуговування без затримок у механізмі передачі. Профіль хоста контролюється та відстежується за допомогою служб відстеження хостів (Host Tracking Services - HTS), наявних у контролері. Це можна використовувати для визначення дійсного користувача. Якщо контролер не може відповідати файлу профілю хоста, створюється та зберігається новий профіль. Якщо місцезнаходження хоста залежить від профілю, він автоматично оновлюється за допомогою події HOST_MOVE, яка передбачає зміну місцезнаходження хоста. Цей вид функціональності не дуже безпечний і створює шлюз для зловмисників і атак спуфінгу, оскільки користувачі не перевіряються за допомогою жодних механізмів автентифікації. Якщо зловмисник може отримати доступ до місцезнаходження цілі, він може обдурити контролер, імітуючи хост, створюючи атаку імітації веб-сайту. Методи на основі відкритих ключів можуть бути реалізовані для перевірки хосту, але це не дуже ефективне рішення, оскільки керування цими ключами було б виснажливим завданням, пов'язаним із витратами. TopoGuard використовує методи попередньої та після умови для перевірки міграції хосту. Попередньою умовою є сигнал PORT_DOWN перед міграцією хосту, а умовою посту є перевірка розміщення посту хоста та переконання, що він не може бути досягнутий у цьому місці. Служба виявлення зв'язків (Link Discovery Service - LDS) використовує протокол рівня мережевих інтерфейсів (Link Layer Discovery Protocol - LLDP) для виявлення внутрішніх з'єднань між комутаторами. Атаки фабрикації посилань відбуваються шляхом введення підроблених пакетів LLDP, які здатні створювати атаки DoS і атаки типу "людина посередині". Методи вирішення таких атак включають додаткову автентифікацію пакетів LLDP за допомогою Type Length Variable (TLV) і підтвердження порту комутатора. Крім того, LineSwitch, яке є рішенням, заснованим на ймовірності та чорному списку, забезпечує стійкість проти атак на насичення площини керування на основі SYN затоплення та захист від уразливостей насичення буфера в SDN.

Техніка FortNOX була представлена для усунення загроз безпеці на прикладному рівні та рівні керування SDN. Це програмне рішення, реалізоване в системі NOX OpenFlow для захисту системи. Він відповідає на запити на основі авторизації та привілеїв, наданих користувачам. Цей метод може допомогти визначити пріоритет дійсних користувачів над фальшивими.

Avant Guard був запропонований, який зосереджується на двох ключових аспектах, тобто безпеці між площиною даних і площиною керування та збільшенні швидкості відповіді контролера на запити площини даних. Ці дві проблеми SDN можна вирішити шляхом додавання деяких додаткових функцій безпеки в систему, а саме міграції підключення та активації тригерів. Міграція підключення використовується для підвищення безпеки в площині даних за допомогою етапу класифікації, звіту, міграції та ретрансляції. Для забезпечення суворої безпеки пакетам потоку дозволено взаємодіяти з контролером лише після проходження механізму рукостискання TCP. Цей метод може допомогти у виявленні зловмисників.

Була запропонована модель для аналізу загроз, які можуть виникнути під час зв'язку з площиною даних за допомогою протоколу OpenFlow. Аналіз виконується шляхом поєднання STRIDE та дерев атак для аналізу атак, таких як спуфінг, втручання, відмова, розкриття інформації, відмова в обслуговуванні та підвищення привілеїв.

Аномальні атаки в SDN.

Аномальні атаки пов'язані з багатьма ризиками, такими як несанкціонований доступ, ін'єкція зловмисних програм тощо, які можуть вплинути на безпеку як програм, так і мереж. Крім того, ці атаки є одними з найнебезпечніших атак, які можуть відбутися на будь-якому рівні мережі, їх неможливо відстежити та важко виявити. Були запропоновано чотири методи виявлення аномалій:

алгоритм Threshold Random Walk with Credit-Based (TRW-CB) вважає користувача підозрілим, якщо значення ймовірності (тобто співвідношення кількості невдалих з'єднань і спроб, зроблених користувачем) більше за фіксоване порогове значення;

алгоритм обмеження швидкості вважає користувача підозрілим, якщо користувач намагається встановити зв'язок із декількома пристроями за заданий час понад порогове значення;

виявлення максимальної ентропії надає оператору повний огляд мережі з усіх вимірів; це двоетапний процес, у якому спочатку класифікується пакети за різними класами на основі призначення, а потім виявляються аномалії на основі швидко змінюваних моделей трафіку;

мережева реклама (NETAD) — це двоетапний процес: на першому етапі він відфільтровує всі непотрібні дані, такі як пакети, що не належать до IP, вихідні потоки тощо; на другому етапі він відстежує мережу та виявляє події, що трапляються рідко, а потім повідомляє про це контролер.

Функції програмування SDN дозволяють зручно виправляти помилки, а також залучати зловмисників. Подібним чином було запропоновано No bugs In the Controller Execution (NICE), який є інструментом налагодження в мережах OpenFlow, який часто відстежує стан усієї системи та визначає одинадцять типів помилок, таких як хост недоступний після переміщення, затримка прямого шляху, надлишок flooding, наступний TCP-пакет завжди відкидається після реконфігурації, TCP-пакет відкидається після реконфігурації, ARP-пакети, забуті під час вирішення адреси, повторювані SYN-пакети під час переходів, пакети нового потоку відкидаються, пакети відкидаються, коли навантаження зменшується тощо. Підхід NICE забезпечує звіт про порушення політики та походження атаки, що допомагає системі відновити ці помилки.

FRESCO-DB було розроблено на основі маршрутизатора кліків, який містить два важливі модулі, вбудовані в контролер NOX для виявлення та протидії підозрілим загрозам. Модуль API створює різні схеми для протидії атаці зловмисного програмного забезпечення за допомогою IDS та інших програм захисту від зловмисного програмного забезпечення. Модуль Security Enforcement Kernel (SEK) використовується для контролю програм, пов'язаних із безпекою, визначених контролером.

Конфіденційність і автентичність додатків в SDN можуть бути захищені методом шифрування і криптографії. Метод перевірки Z3 використовує мову програмування високого рівня, щоб відрізнити легітимну програму від шкідливих програм для захисту конфіденційності та цілісності програм.

Атаки вторгнення в SDN.

Традиційні мережі мають вбудовані проміжні блоки (які можуть інтегрувати IDS, брандмауер і проксі) та інші функції для блокування зловмисних користувачів. Ці середні блоки недоступні в SDN, але є необхідними для захисту SDN від атак на безпеку компонентів рівня даних і контролера. Вони можуть бути не здатні повністю запобігти атакам, але можуть бути корисними для підвищення базової безпеки в SDN. Однак інтеграція цих модулів у SDN супроводжується деякими труднощами, оскільки SDN має відокремлену структуру, яка

покладається на централізований контролер для всіх завдань, таких як оновлення політик. Таким чином, включення додаткових модулів може призвести до накладних витрат на контролер, показуючи його вплив на всю мережу. Це може призвести до атак вторгнень у SDN, коли ефект атак не помічається як законні витрати на контролер. Існують різні методи, запропоновані для виявлення атак вторгнень у SDN.

FlowGuard було запропоновано як брандмауер SDN і є більш складним у порівнянні з брандмауерам у звичайних мережах. FlowGuard пов'язано з подвійною функціональністю, щоб працювати як фільтр пакетів і засіб перевірки політики. Він відстежує мережу для виявлення шкідливих пакетів і порушень політики в SDN.

Архітектура FlowTag була запропонована для оптимізації системи шляхом додавання розширеної архітектури разом із середнім блоком, який позначає пакети, що проходять через нього. Це полегшує відстеження пропущених пакетів і пакетів зловмисного програмного забезпечення, присутніх у мережі серед інших. Хоча проміжні блоки мають багато переваг, пов'язаних із цим, керування ними в SDN є виснажливим завданням.

Архітектура NIMBLE була запропонована для керування середніми блоками на основі правил політики, наданих адміністратором. Витончена архітектура була запропонована для SDN на основі OpenFlow, яка здатна підтримувати різні пристрої, такі як NetFPGA, GPU та NP. Цей метод використовує окрему площину керування для керування всіма операціями середніх блоків, що підвищує гнучкість SDN.

Оскільки функції SDN повністю базуються на інструкціях, наданих контролером/програмним забезпеченням, він більш вразливий до перерв у процесі, а введення нових помилок може призвести до зниження загальної продуктивності SDN. Згідно з останнім стандартом (версія 1.3.0) openSwitch, наявність безпеки транспортного рівня (TLS) не є обов'язковою опцією. Однак південний API мережі, який більш схильний до загроз, вимагає рівня безпеки, такого як TLS, який автентифікує користувачів за допомогою методів шифрування перед наданням доступу.

Спуфінгова атака в SDN.

Спуфінгові атаки – це види атак, під час яких зловмисник використовує ідентифікаційні дані законного користувача, щоб вставити в мережу підроблені пакети та шкідливі програми. Завдяки гнучкості, яку пропонує SDN, атаки підробки легко реалізувати в програмно визначених мережах. Комутатори OpenFlow у SDN — це пристрої для пересилання даних без інтелектуальних програм. Їх можна підробити та використовувати для надсилання запитів контролеру. Контролер також не може блокувати ці фальшиві пакети, оскільки йому не вистачає базових компонентів, таких як середні блоки. Інший вид комутаторів у мережі OpenFlow – це програмні комутатори, які відповідають за віртуалізацію мережі. Ці комутатори підключаються безпосередньо до контролера, стаючи привабливою мішенню для зловмисників. Ці комутатори прокладають прямий шлях до зловмисників до контролера, де зловмисники можуть налаштувати політику маршрутизації комутаторів, вводячи в оману всі пакети в мережі. Ефект, викликаний цими атаками, можна зменшити шляхом раннього виявлення комутаторів зловмисного програмного забезпечення. Для цього всі пакети, що надходять у мережу, повинні бути ретельно перевірені.

Було запропоновано дві схеми пошуку підозрілих комутаторів. У першій схемі шкідливі комутатори в системі виявляються на основі потоку трафіку, що перевищує задане порогове значення. Друга схема в мережі передбачає вбудовування стороннього сервера для моніторингу комутаторів для виявлення будь-яких зловмисних дій.

Техніка під назвою Sphinx була запропонована для виявлення загроз/уразливостей у топології мережі та інтерфейсі зв'язку між площиною даних і площиною керування. Він використовує переваги потокових графіків для моніторингу кожного потоку. Він також використовує чотири важливі команди OpenFlow, такі як FLOW_MOD, PACKET_IN, STATS_REPLY і FEATURES_REPLY, щоб отримати всі необхідні дані від комутатора та

сповістити контролер, якщо поблизу комутаторів буде виявлено будь-яку підозрілу активність.

Усіх цих атак можна певною мірою уникнути, зберігаючи конфіденційність вмісту користувачів. Найбільш небезпечні атаки в мережах спрямовані на мережі на основі IP. Це обумовлює необхідність захисту ІВ в цілому. У SDN реалізовано спеціальний механізм під назвою OpenFlow random host muta tion (OF-RHM), який приховує фактичні IP-адреси та використовує випадкові віртуальні IP-адреси, що певною мірою запобігає атакам.

Висновки.

У роботі була досліджена архітектура програмно-визначеної мережі (SDN) та різні загрози безпеці, які вирішує SDN, і нові загрози, які виникли в результаті впровадження SDN. Були узагальнені нові види атак на безпеку та запропоновані можливі контрзаходи в SDN.

Список використаної літератури:

1. Martin Casado, Michael J. Freedman, Justin Pettit, Jianying Luo, Nick McKeown, Scott Shenker. Ethane: taking control of the enterprise. ACM SIGCOMM Computer Communication ReviewVolume 37, Issue 4, pp 1–12.

2. D. Kreutz, F. Ramos, P. Ver´ıssimo, C. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," Proceedings of the IEEE, vol. 103, pp. 14–76, 2015.

3. Danda B. Rawat, Senior Member, IEEE, and Swetha R. Reddy, Member, IEEE. Software Defined Networking Architecture, Security and Energy Efficiency: A Survey. IEEE communications surveys & tutorials, vol. 19, no. 1, first quarter 2017.

4. Гніденко М.П., Вишнівський В.В., Ільїн О.О. Побудова SDN мереж. – Навчальний посібник. – Київ: ДУТ, 2019. – 190 с.

Автори статті

Гніденко Микола – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Прокопов Сергій – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Гніденко Максим - аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна

Authors of the article

Hnidenko Mykola - Candidate of science (technic), associate professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

Prokopov Serhii - Candidate of science (technic), associate professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

Hnidenko Maksym – postgraduate student, State University of Information and Communication Technology, Kyiv, Ukraine.