DOI: 10.58254/viti.5.2024.14.154

УДК 004.7

д-р техн. наук, професор Стрельбіцький М. А. ORCID: 0000-0001-8030-3228 (НАДПСУ)
канд. техн. наук Хоптинський Р. П. ORCID: 0000-0001-9351-7938 (НАДПСУ)
Ваврічен О. А. ORCID: 0000-0001-7777-9188 (НАДПСУ)
Городиський Р. О. ORCID: 0000-0002-0918-864X (НАДПСУ)

ПІДХІД ДО СТВОРЕННЯ МОДЕЛІ ПРОГРАМНО-ОРІЄНТОВАНОЇ КОМУНІКАЦІЙНОЇ МЕРЕЖІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Підвищення рівня захисту інформаційних ресурсів Державної прикордонної служби України (далі – Держприкордонслужби) як складової сил оборони України є важливим завданням, особливо в умовах воєнного стану. Ефективна та надійна корпоративна мережа прикордонного відомства стає ключовою складовою для забезпечення безпеки, координації та оперативності реагування на внутрішні та зовнішні загрози. Одним із аспектів розвитку інформаційного простору став розвиток транспортної мережі Держприкордонслужби. Аналіз існуючих технологій, визначення їхніх переваг та недоліків дозволив виокремити технологію Software-Defined Wide Area Networking як таку, що найбільш повно відповідає критеріям відповідності, що визначені експертами Управління зв’язку та інформаційних систем. Зазначена технологія дозволяє не лише оптимізувати мережевий трафік та забезпечити високу швидкість передачі даних, але й гарантує гнучкість в управлінні мережею та підвищує рівень безпеки. Для Держприкордонслужби, яка відповідає за безпеку кордонів країни, використання передових технологій Software-Defined Wide Area Networking може мати вирішальне значення для оптимізації роботи та забезпечення найвищого рівня захисту інформації.

У статті приділено увагу розробці концептуальної моделі для побудови корпоративної мережі Держприкордонслужби на основі технології Software-Defined Wide Area Networking. Основною метою дослідження є розгляд можливості впровадження цієї технології в контексті її застосування силами оборони України та аналіз її переваг і недоліків. Завданням дослідження було вивчення технічних аспектів впровадження Software-Defined Wide Area Networking, а саме: конфігурації мережевих пристроїв, управління трафіком, моніторингу безпеки та захисту даних.

Слід зазначити, що Cisco Software-Defined Wide Area Networking застосувала оптимальний підхід до архітектури мережі, який відокремлює площину керування від площини даних усіх периферійних маршрутизаторів і реалізує всі функції керування в централізованому програмному контролері під назвою vSmart. Практичні рекомендації дослідження дозволили забезпечити безперервне мережеве обслуговування шляхом зміни маршруту в обхід збоїв і потенційних причин простою.

Ключові слова: *модель, комунікаційна мережа, Держприкордонслужба, технологія програмно-орієнтованих мереж, управління мережею, Software-Defined Wide Area Networking.*

M. Strelbitskyi, R. Khoptynskyi, O. Vavrichen, R. Horodyskyi Approach to creation model of software-oriented communication network of the State Border Guard Service of Ukraine.

Enhancing the level of information resource protection of the State Border Guard Service of Ukraine, as a component of Ukraine's defense forces, is an important task, especially in times of war. An effective and reliable corporate network of the border agency becomes a key component for ensuring security, coordination, and responsiveness to both internal and external threats. One aspect of developing the information space is the development of the transport network of the State Border Guard Service. Analysis of existing technologies, identifying their advantages and disadvantages, allowed for the identification of Software-Defined Wide Area Networking technology as the one that best meets the conformity criteria defined by the experts of the Communication and Information Systems Management. This technology not only allows for optimizing network traffic and ensuring high-speed data transmission but also guarantees flexibility in network management and enhances security. For the State Border Guard Service, responsible for the security of the country's borders, the use of advanced Software-Defined Wide Area Networking technologies can be crucial for optimizing operations and ensuring the highest level of information security.

The article focuses on developing a conceptual model for building the corporate network of the State Border Guard Service based on Software-Defined Wide Area Networking technology. The main goal of the research is to consider the possibility of implementing this technology in the context of its application by Ukraine's defense forces and to analyze its advantages and disadvantages. The research task was to study the technical aspects of implementing Software-Defined Wide Area Networking, namely: configuration of network devices, traffic management, security monitoring, and data protection.

Cisco's Software-Defined Wide Area Networking has applied an optimal approach to network architecture, which separates the control plane from the data plane of all peripheral routers and implements all control functions in a

centralized software controller called vSmart. Practical recommendations from the research allowed for ensuring continuous network service by rerouting around failures and potential causes of downtime.

Keywords: *model, communication network, State Border Guard Service, Software-Defined Networking technology, network control, Software-Defined Wide Area Networking.*

Постановка проблеми у загальному вигляді. Функціонування інформаційно-комунікаційних систем в умовах воєнного стану передбачає значного підвищення рівня керованості мережевою складовою та безпеки інформаційних ресурсів Держприкордонслужби як складової сил оборони України. В умовах постійних викликів, які виникають при виконанні прикордонним відомством функціональних завдань, ефективна та надійна корпоративна мережа стає ключовою складовою для забезпечення безпеки, координації та оперативності реагування на внутрішні та зовнішні загрози.

У цьому контексті технологія програмно-орієнтованої комунікаційної мережі SDN (Software – Defined Networking) дозволяє не лише оптимізувати мережевий трафік та забезпечувати високу швидкість передачі даних, але й забезпечує гнучкість управління мережею та підвищує рівень безпеки. Для Держприкордонслужби, яка відповідає за безпеку кордонів держави, використання передових технологій SDN може мати вирішальне значення для оптимізації роботи та забезпечення високого рівня захисту інформації.

Аналіз останніх публікацій. Протягом останніх років ситуація в інформаційних та комунікаційних системах суттєво змінювалась завдяки імплементації хмарних технологій [1–3]. Розвиток комунікаційних засобів сприяв збільшенню швидкостей обміну даними, що спонукало застосуванню технології Ethernet як стандарту для всіх каналів зв’язку. Це призвело до того, що різниця між локальною мережею (LAN) і глобальною мережею (WAN) стала практично мінімальною. Разом із тим, незмінними залишились основні функції комутації та маршрутизації, які зазвичай реалізовані на апаратному автономному пристрої. З точки зору даних ці пристрої є самодостатніми стосовно завдань комутації або маршрутизації.

З метою збереження переваги на ринку комунікаційних засобів різні компанії, такі як Cisco, Juniper і HP, вдосконалили свої пристрої функціями, що призвели до появи мережевих засобів, які ґрунтуються на застарілих протоколах, наприклад, Border Gateway Protocol (BGP) [4]. Використання цих протоколів повинно було забезпечити інкапсуляцію заголовків на різних рівнях. Разом із тим, такий підхід зменшив максимальний розмір передачі пакетів (MTU). Зазначимо, що таке нашарування абстракцій не сприяє управлінню мережею, де шаблони трафіку визначаються в кожному шарі незалежно.

У цьому контексті варто зазначити потребу використання протоколу BGP для обміну інформацією про маршрутизацію та доступність вузлів. Це пов’язано із тим, щоб міграція всіх складових корпоративної мережі SDN відбувалася поступово і таким темпом, який не становить загрози безпеці та керованості інформаційно-комунікаційних систем, які функціонують на основі Intranet-мережі [5].

Інтегрована інформаційно-комунікаційна система Держприкордонслужби забезпечує автоматизацію практично всіх завдань інформаційного характеру, які виконують органи та підрозділи прикордонного відомства. Особливістю організаційної структури Держприкордонслужби є значна розосередженість прикордонних підрозділів, що, в свою чергу, вимагає використання різнорідної якості обслуговування передачі даних з метою забезпечення функціонування засобів автоматизації. Постійне вдосконалення складових мережі призводить до її варіантності стосовно типів комунікаційного обладнання та складності керування такою мережею.

Тому для Держприкордонслужби стає актуальним застосування автоматизованого програмного підходу при підключенні до інформаційно-комунікаційної систем її підрозділів. Застосування програмно-керованої глобальної мережі (SD-WAN)SD-WAN розширить програмно-визначені мережі (SDN) в рішення, яке підрозділи зможуть використовувати для

швидкого створення інтелектуальної гібридної Wan мережі, що включить MPLS, LTE, широкосмуговий Інтернет і бездротові підключення підрозділів.

Метою статті, є розробка адаптованої концептуальної моделі архітектури SD-WAN комунікаційної мережі Держприкордонслужби на основі технологій інтелектуального управління.

Виклад основного матеріалу дослідження.

Запобігання ризикам і загрозам у прикордонній сфері потребує ефективної та надійної комунікаційної інфраструктури. Швидкість передачі даних, безпека і доступність є критично важливими аспектами у контексті функціонування прикордонного відомства. Аналіз стратегій впровадження технології SD-WAN для оптимізації передачі даних та забезпечення стабільної та безпечної роботи комунікаційної мережі дозволить визначити конкретні вимоги і потреби Держприкордонслужби, розглянути варіанти конфігурацій та здійснити вибір оптимальних рішень для створення високоефективної, масштабованої та безпечної мережі, яка забезпечує високу надійність комунікацій у державних структурах.

При вирішенні питання про перенесення традиційної архітектури WAN на програмно-визначену WAN застосовують поетапний процес, зокрема розгортання контролерів, міграція основних центрів обробки даних і вузлів і, нарешті, віддалених сайтів, таких як підрозділи та філії. Основні засади виконання такої послідовності полягають в тому, щоб сайти-концентратори направляли трафік між SD-WAN і не-SD-WAN-вузлами протягом періоду міграції. Однією з головних переваг програмно-визначеної глобальної мережі є можливість розгортання контролерів у загальнодоступній хмарі. Це може значно зменшити витрати і підвищити загальну доступність і резервування площини керування/контролю. Cisco пропонує на вибір наступні варіанти: хмара, розміщена на Cisco; загальнодоступна хмара; розгортання контролерів у центрах обробки Держприкордонслужби. Саме останній варіант пропонується для вибору з причини «чутливості» прикордонного інформаційного ресурсу. Такий підхід передбачає відповідальність підрозділів зв’язку за резервне копіювання та аварійне відновлення.

За умови налаштування та запуску контролерів, вони повинні встановити безпечні з’єднання між собою. На сьогодні є два варіанти на вибір, коли мова йде про базовий безпечний протокол: TLS, який використовує транспорт TCP, і DTLS, який використовує транспорт UDP. За замовчуванням усі контролери використовують параметр DTLS. При розгортанні SD-WAN у середовищі нульової довіри інформація передається для всіх постійних з’єднань між контролерами. Слід зазначити, що кожне ядро на vManage та vSmart створює постійне з’єднання DTLS з vBond, що призводить до чотирьох з’єднань між vManage та vBond і двох з’єднань між vSmart і vBond.

Безпечне підключення граничних пристроїв WAN є дуже важливою частиною рішення SD-WAN. Рішення Cisco SD-WAN використовує модель білого списку для автентифікації та довіри до пристроїв vEdge [6]. Це означає, що перед тим, як прикордонному маршрутизатору WAN буде дозволено приєднатися до рівня керування, він повинен бути заздалегідь відомий усім контролерам SD-WAN. Кожен пристрій унікально ідентифікується ідентифікатором шасі та серійним номером сертифіката. Коли контролери SD-WAN розгорнуті та отримали дійсні сертифікати, периферійні маршрутизатори WAN можуть почати процес адаптації. На цьому етапі найважливіше переконатися, що пристрої vEdge мають доступ до всіх контролерів через усі доступні транспортні засоби.

Розглянемо типовий сценарій, коли віддалений сайт має один приватний канал MPLS і одне широкосмугове підключення до Інтернету. Є три поширені реалізації, які вирішують таке завдання:

1. MPLS має доступ до публічної хмари завдяки маршрутизації через центр обробки даних або регіональний хаб, який має обидва транспортні засоби.

2. Загальнодоступні маршрутизовані IP-адреси контролерів перерозподіляються в хмару MPLS, а граничний маршрутизатор постачальника повідомляє про них vEdge.

3. Встановлюється з’єднання з площиною управління лише через Інтернет-з’єднання. Edge зможе приєднатися до структури SD-WAN, але не матиме резервування площини керування, тому цей підхід взагалі не рекомендується.

Фундаментальна мета кожної мережі – забезпечити безперервне мережеве обслуговування шляхом зміни маршруту в обхід збоїв і потенційних причин простою. Cisco SD-WAN забезпечує високу доступність завдяки поєднанню чотирьох принципів:

- резервування контролерів;
- vEdges-резервування;
- надійний дизайн мережі;
- аварійного відновлення.

Щодо резервування контролерів, то усі контролери SD-WAN працюють як віртуальні машини або контейнери. Незалежно від методу розгортання основним принципом високої доступності є наявність кількох контролерів кожного типу, бажано розгорнутих у розрізнених географічних місцях. Це гарантує, що централізована площина управління залишається стійкою, якщо один із контролерів виходить з ладу.

Оскільки кожен контролер SD-WAN виконує різні функції, то кожен їхній тип використовує різні технології масштабування та підключення, як показано на рисунку 1 [7].

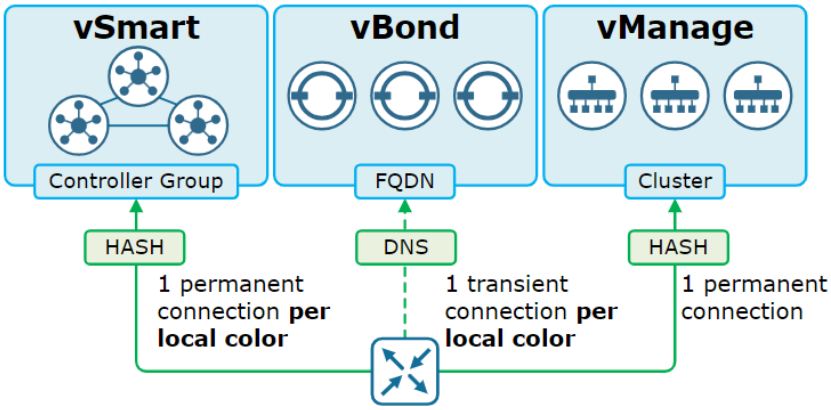

Рис. 1. Принципи високої доступності Cisco SD-WAN

Оркестратор Cisco vBond виконує дві основні функції в домені SD-WAN:

- перевіряє та автентифікує всі пристрої, які намагаються приєднатися до домену SD-WAN;
- керує встановленням керуючих з’єднань між контролерами та маршрутизаторами vEdge.

Оркестратор Cisco vBond працює як віртуальна машина локально або в хмарі. Однак це єдиний контролер, який також може працювати на звичайному маршрутизаторі vEdge, налаштованому для роботи як оркестратор vBond.

Високодоступну мережу Cisco SD-WAN, яка має кілька контролерів vBond, що працюють в режимі активний/активний, бажано розгортати в різних локальних географічних розташуваннях або хмарних регіонах. Кожен із пристроїв SD-WAN посилається на оркестратор vBond за одним іменем FQDN у своїй системній конфігурації.

Контролери Cisco vSmart керують централізованою площиною керування мережею. Вони встановлюють постійні з’єднання DTLS/TLS з усіма пристроями SD-WAN у домені. Через ці канали керування вони регулярно обмінюються даними про мережевий домен, щоб забезпечити синхронізацію їхніх централізованих таблиць маршрутизації.

Високодоступна мережа Cisco SD-WAN має кілька контролерів vSmart, які бажано розгортати в різних географічних локаціях або хмарних сервісах. Кожен маршрутизатор vEdge за замовчуванням встановлює керуючі з’єднання з двома контролерами vSmart, як показано на рисунку 2 [7]. Коли один із контролерів виходить з ладу, інший безперешкодно бере на себе функції рівня керування мережею. Площина керування мережею працює безперебійно, доки в домені SD-WAN працює один контролер.

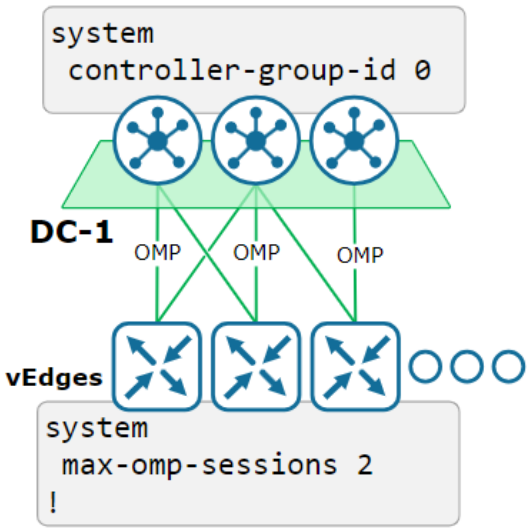

Рис. 2. Забезпечення високої доступності vSmart

Слід зазначити, що контролери vSmart встановлюють і підтримують повну мережу керуючих з’єднань між собою, над якою вони формують повну мережу сеансів OMP. Усі контролери синхронізують свою інформаційну базу маршрутизації, обмінюючись маршрутами, маршрутами TLOC, політиками та ключами шифрування. Крім того, кожен контролер встановлює постійне керуюче з’єднання з кожним оркестратором vBond. Потім ці канали керування використовуються оркестратором vBond для відстеження того, які vSmarts працюють у домені. Коли один із контролерів виходить з ладу, оркестратор перестане надавати IP-адресу недоступного vSmart маршрутизаторам vEdge, які приєднуються до домену SD-WAN.

Оскільки домен SD-WAN охоплює кілька географічних регіонів, зазвичай для відмовостійкості додається більше контролерів vSmart. Як правило, прикордонне відомство розгортає контролери в більш ніж двох регіонах, тому важливо переконатися, що vEdges підключаються до vSmarts в тому самому або суміжному географічному регіоні. Наприклад, існує три центри обробки даних: один на сході, один посередині та один на заході. У кожному центрі обробки даних існує окрема група контролерів vSmart, як показано на рисунку 3 [7].

Ієрархічна SD-WAN – це варіант дизайну використання Cisco SD-WAN, який надає можливість розділяти мережу WAN на незалежні регіони. Подібно до логіки області OSPF, ієрархічна мережа SD-WAN завжди повинна мати основну область, яка називається областю «0», що з’єднує всі інші області доступу. Одна з істотних переваг ієрархічної архітектури SD-WAN полягає в тому, що вона чітко відокремлює внутрішньо-регіональний трафік від міжрегіонального трафіку. Міжрегіональний трафік повністю обробляється набором виділених маршрутизаторів, які називаються прикордонними маршрутизаторами (BR), що створюють основну область «0». Подібно до OSPF, трафік, що надходить з одного регіону і призначений для іншої області, завжди проходить через основну область «0». Це вирішує сценарій використання роз’єднаних постачальників послуг. Основний регіон забезпечує зв’язок між двома регіонами, які використовують незв’язаних провайдерів.

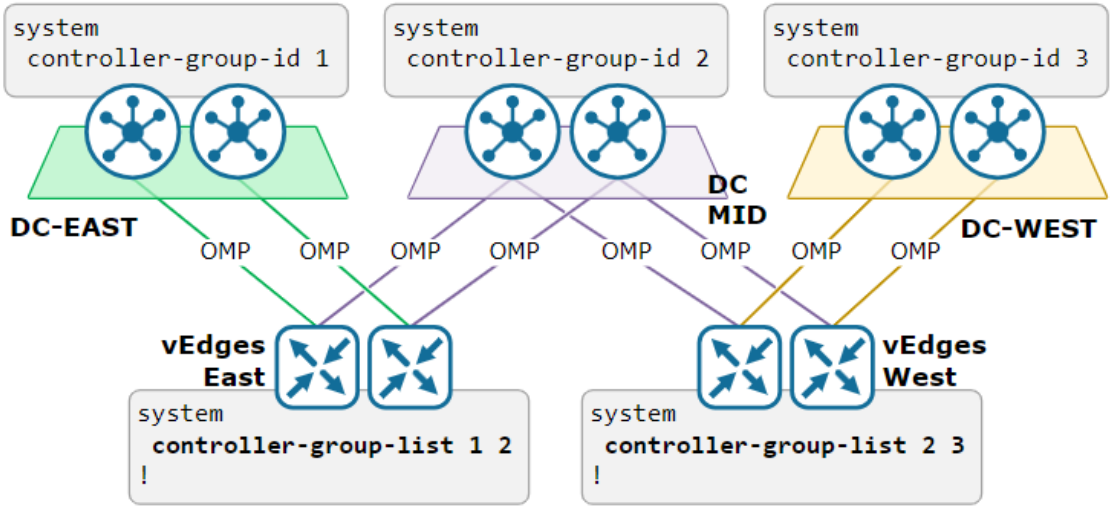

Рис. 3. Спорідненість контролера vSmart

Розділення міжрегіонального трафіку в незалежний регіон дозволяє Держприкордонслужбі використовувати різних постачальників послуг для магістральних каналів зв’язку і застосовувати різні політики до магістральних мереж передачі даних.

Ще однією великою перевагою ієрархічної архітектури є гнучкість використання різних постачальників послуг у кожному окремому регіоні. Це дозволяє вибрати найбільш економічно ефективного постачальника в кожному географічному регіоні без шкоди для доступності та керованості мережі. Крім того, можливо використовувати різні інфраструктури маршрутизації та різні політики трафіку для кожного регіону, що притаманно прикордонному відомству.

Ієрархічна архітектура SD-WAN дозволяє організації призначати різні виділені контролери vSmart для кожного незалежного регіону. Це значно спрощує розробку політики організації. Технічно кажучи, якщо регіон містить лише невелику кількість маршрутизаторів vEdge, пару контролерів можна призначити кільком регіонам. Однак для простоти та кращої керованості настійно рекомендується, щоб у кожному регіоні обслуговувалися спеціальні контролери vSmart.

Регіони доступу – це логічне групування маршрутизаторів vEdge, які обслуговують певну географічну область. Наразі максимальна кількість підтримуваних регіонів для розгортання SD-WAN становить вісім.

Ієрархічна архітектура SD-WAN накладає деякі дуже серйозні обмеження на домен накладання:

1. Мережеві пристрої, налаштовані на використання ієрархічної SD-WAN, не можуть підключатися до звичайних пристроїв SD-WAN. Для використання ієрархічної SD-WAN слід налаштувати всі пристрої або жоден із них. Таким чином, увімкнення ієрархічної SD-WAN для існуючого мережевого середовища є достатньо складним процесом.
2. Наскрізна маршрутизація з урахуванням програми не працює. AAR слід використовувати лише в межах регіону.
3. Мультитенантність не підтримується в ієрархічній SD-WAN.
4. Агрегація маршрутів протоколу керування накладенням (OMP) на прикордонних маршрутизаторах.
5. Міжрегіональна багатоадресна IP-адреса не підтримується в ієрархічній SD-WAN.

Програмно-орієнтовані рішення Cisco WAN пропонують багато функцій безпеки, орієнтованих на глобальну мережу та корпоративні мережі. Проте слід зазначити, що безпека SD-WAN є лише частиною ширшої стратегії безпеки більшості організацій.

Secure Access Service Edge (SASE) – це новий підхід до глобальної інфраструктури організації, який поєднує програмно-визначену глобальну мережу з розширеними функціями безпеки хмарної доставки. Інфраструктура SASE має на меті поєднати функції мережі, безпеки та ідентифікації в єдине уніфіковане рішення, що надається як послуга. SASE є відповіддю на поточні виклики переходу технологій до децентралізованих мереж і безпеки. Важливо розуміти, що SASE – це не окремий продукт, рішення чи функція. Це структура або філософія, яка поєднує пакет різних технологій. Таким чином, він не конкурує безпосередньо з будь-якими рішеннями і не замінює будь-який конкретний продукт.

Нині існує величезна складність, пов’язана з мережею та безпекою Cisco, а саме:

вибір – різні мережеві рішення і рішення безпеки (Meraki, Viptela, Umbrella, ThousandEyes, Duo тощо);

придбання – різні моделі ліцензування;

розгортання – кожне окреме рішення має складний процес навчання та вимагає високого рівня досвіду під час розгортання;

експлуатація – кожне окреме рішення потребує окремого набору інженерів для його експлуатації;

масштабування/оновлювання – з багатьма з’єднаними рішеннями стає дуже важко вносити зміни в архітектуру.

За допомогою SASE Cisco намагатиметься об’єднати все в одне рішення та знизити загальну складність на всіх можливих рівнях.

Програмно-визначена глобальна мережа не призначена для вирішення всіх проблем, з якими стикається мережа та інфраструктура безпеки під час переходу до децентралізованої хмарної моделі мережі. Ось деякі з помітних недоліків:

1. SD-WAN потребує надійної основи. Програмно-визначені рішення WAN створюють оверлейну структуру поверх основної інфраструктури глобальної мережі. Організаціям все ще потрібна надійна мережева магістраль. Управління та захист основної інфраструктури у великомасштабних багаторегіональних варіантах побудови все ще може бути складним і дорогим. Сама собою SD-WAN не вирішує основних проблем.

2. Віддалений працівник/віддалений доступ. Програмно-визначена накладна структура забезпечує безпечне та надійне підключення «сайт до будь-якого сайту» та «сайт до будь-якої хмари». Однак це рішення не призначене для надання віддаленого SSL VPN для мобільних працівників або для захисту конфіденційних корпоративних даних від віддаленого доступу. Сама собою SD-WAN не вирішує проблеми віддаленого працівника/віддаленого доступу.

3. Відсутність повного портфоліо безпеки. Головним завданням більшості програмно-визначених рішень WAN є допомога в автоматизації та масштабуванні інфраструктури глобальної мережі. Так, портфоліо Cisco SD-WAN містить багато можливостей безпеки. Однак SD-WAN сама собою не може вирішити всі проблеми безпеки, з якими стикаються організації під час впровадження децентралізованої хмарної інфраструктури та віддаленого доступу. Вона може інтегруватися з хмарними провайдерами безпеки, такими як Umbrella та Duo.

Поточна структура Cisco Secure Access Service Edge має три основні компоненти: Cisco Software-defined WAN, Cisco Umbrella, Cisco Duo.

На рисунку 4 показана діаграма високого рівня повної інтеграції трьох основних рішень [8].

Cisco Umbrella Secure Internet Gateway (SIG) об’єднує численні функції безпеки в одному хмарному рішенні, яке традиційно вимагало локальних пристроїв безпеки (FW, IPS, проксі). Umbrella поєднує в собі хмарний брандмауер, захищений вебшлюз (SWG), інспекцію рівня DNS, брокер безпеки доступу до хмари (CASB), запобігання втраті даних (DLP) і віддалену ізоляцію браузера (RBI) в одну хмарну службу, яка легко інтегрується з Cisco SD-WAN.

Мережевий шлюз Cisco Duo (DNG) дозволяє кінцевим користувачам отримувати доступ до локальних ресурсів, не турбуючись про керування обліковими даними VPN, а також забезпечує безпеку за допомогою Duo Multi-factor Authentication (MFA). Duo забезпечує детальний контроль доступу для програми та групи користувачів. Це гарантує, що лише довірені користувачі та кінцеві точки можуть отримати доступ до внутрішніх ресурсів організації.

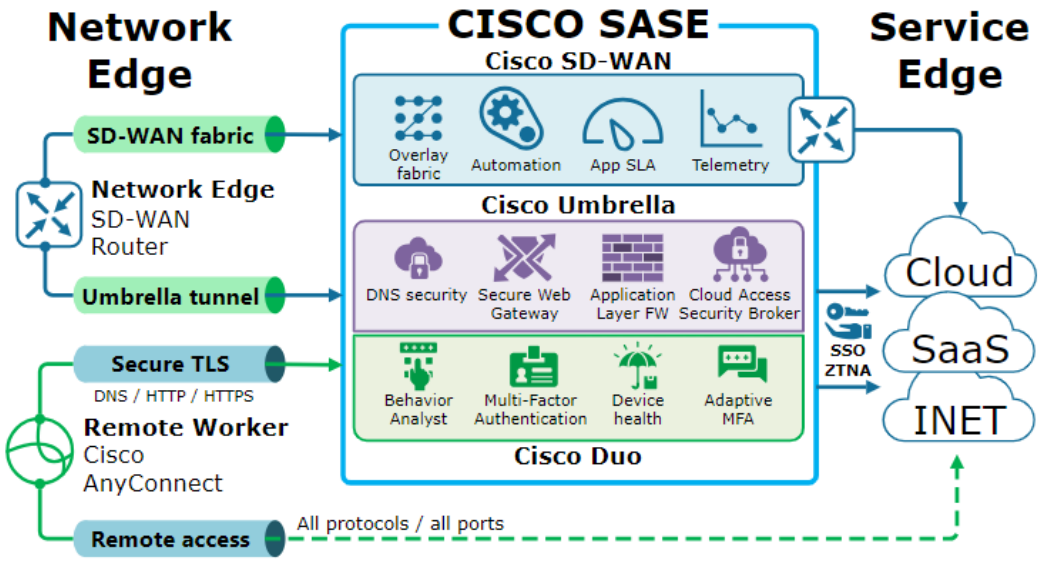

Рис. 4. Cisco SD-WAN and SASE

Разом і тим, рішення щодо високої доступності та безпеки часто суперечать одне одному. Cisco застосувала зовсім інший підхід до безпеки WAN, який базується на трьох основних принципах:

1. Fabric Security – рішення гарантує, що всі пристрої, які беруть участь у мережі, є справжніми та надійними. Весь зв’язок між мережевими пристроями автоматично шифрується.

2. Інтегрована безпека – рішення інтегрує всі функції безпеки, такі як брандмауер, IPS і AMP, у мікропрограму маршрутизаторів, усуваючи потребу в окремих виділених апаратних пристроях, які виконують функції безпеки.

3. Хмарна безпека – забезпечує повну інтеграцію з кількома постачальниками хмарної безпеки, що робить перехід до гібридної моделі безпеки дуже легким.

Першим кроком у стратегії мережевої безпеки є забезпечення надійності всіх мережевих пристроїв. Із традиційними механізмами безпеки, такими як «цей маршрутизатор розгорнуто нашим довіреним інженером» і «ми використовуємо автентифікацію BGP/OSPF/PIM/HSRP», постає питання, чи є впевненість, що використовується надійна інфраструктура? У цьому контексті варто зауважити, що забезпечення безпеки повинно починатись задовго до того, як спрацюють механізми безпеки програмного забезпечення, такі як автентифікація протоколу. Останніми роками спостерігається стрімке зростання кількості атак і експлойтів, наприклад, багато апаратних компонентів, таких як оперативна пам’ять, твердотільні накопичувачі та процесори, замінюються на скомпрометовані з попередньо встановленими троянськими програмами. Сьогодні безпека починається з обладнання під час виробництва. Усі фізичні пристрої Cisco мають модуль довіри (TAm), встановлений під час виробництва. Модуль TAM надає кілька надійних технологій:

1. Безпечне завантаження. Мікрозавантажувач, встановлений у модулі TAM, відстежує процес запуску та захищає від шкідливого коду під час завантаження.

2. Безпечне зберігання. Модуль TAm забезпечує безпечне зберігання криптографічних ключів, паролів, облікових даних клієнтів та іншої важливої інформації безпеки для пристрою. Однією з його переваг є можливість зберігати приватні ключі шифрування та паролі. Також можливе виділення безпечного сховища за межами модуля TrustAnchor.

3. Захищений унікальний ідентифікатор пристрою (SUDI). SUDI – це сертифікат SSL (X.509v3), який містить серійний номер пристрою та ідентифікатор продукту. Його встановлюють під час виробництва та перевіряють загальнодоступним центром кореневих сертифікатів. Сертифікат SUDI SSL разом із пов’язаними ключами зберігається в апаратному чипі Trust Anchor Module (TAm). Крім того, приватний ключ ніколи не може бути розкритий, оскільки пара ключів криптографічно прив’язана до конкретного чипа TAm.

4. Захист під час виконання (RTD). RTD захищає від впровадження шкідливого коду в мікропрограму під час виконання.

Ідентифікація для всіх пристроїв SD-WAN забезпечується сертифікатами SSL (x509v3). Усі пристрої постачаються з попередньо встановленими кореневими сертифікатами DigiCert, Symantec і Cisco. Крім того, усі фізичні маршрутизатори постачаються з попередньо завантаженим сертифікатом пристрою, встановленим під час виробництва та захищеним апаратним чипом (SUDI). Усі програмні пристрої, такі як хмарні маршрутизатори та контролери, не мають попередньо завантажених сертифікатів пристроїв і повинні пройти процес запиту на підписання сертифіката (CSR). Важливим моментом тут є те, що кожен пристрій SD-WAN повинен мати дійсний сертифікат SSL, який криптографічно підтверджує його ідентифікацію. Коли контролери встановлюють керуючі з’єднання один з одним, вони обмінюються SSL-сертифікатами своїх пристроїв під час процесу встановлення зв’язку DTLS/TLS. Потім кожен контролер перевіряє такі параметри, а саме:

перевіряє довіру для отриманого сертифіката пристрою за допомогою його попередньо встановлених кореневих сертифікатів;

порівнює серійний номер сертифіката зі списком авторизованих контролерів, який розповсюджується з vManage;

порівнює назву організації в полі OU отриманого сертифіката з локально налаштованою назвою організації.

Слід зазначити, що існує різниця в процесі перевірки для віртуальних і фізичних маршрутизаторів. Сертифікат SSL фізичного периферійного маршрутизатора встановлюється під час виробництва. Таким чином, неможливо закодувати назву організації в сертифікаті, оскільки на момент виготовлення невідомо, яка саме організація використовуватиме цей маршрутизатор.

З іншого боку, віртуальні маршрутизатори генерують запит на підписання сертифіката (CSR) після того, як ім’я організації налаштовано на маршрутизаторі, тому поле OU буде присутнє в сертифікаті SSL після того, як CSR буде підписано центром сертифікації. Якщо всі етапи перевірки пройдено успішно, маршрутизатор встановлює постійне з’єднання DTLS/TLS із контролером SD-WAN.

Коли два пристрої SD-WAN встановлюють захищене керуюче з’єднання DTLS/TLS, цілісність рівня керування забезпечується двома елементами безпеки: дайджестами повідомлень AES-GCM та парою відкритих і закритих ключів.

AES-GCM забезпечує як шифрування, так і можливість перевіряти цілісність повідомлень контрольної площини, надісланих через тунелі DTLS/TLS. Він генерує дайджести повідомлень (просто дайджести) для кожного пакета, надісланого через захищені тунелі DTLS/TLS. Пристрій-одержувач потім генерує дайджест для пакета, і якщо вони збігаються, пакет перевіряється. Це підтверджує, що вміст пакета не було змінено під час передавання.

Другий компонент – це використання відкритих і закритих ключів. Коли встановлено з’єднання з площиною управління, локальний пристрій надсилає виклик віддаленому.

Віддалений пристрій шифрує виклик, підписуючи його своїм закритим ключем, і надсилає виклик на локальний пристрій, який потім використовує відкритий ключ віддаленого пристрою, щоб перевірити, що отриманий виклик відповідає надісланому виклику.

Ключі використовуються для того, щоб переконатися, що пакети були надіслані надійним пристроєм. Автентичність кожного пакета перевіряється шляхом шифрування та дешифрування за допомогою симетричних ключів, якими обмінювалися під час встановлення контрольного з’єднання.

Безпечна площина керування гарантує, що власна безпека мережевих протоколів, таких як SNMP і NETCONF, не викликає занепокоєння для організації, оскільки весь зв’язок на рівні керування проходить через з’єднання DTLS/TLS, отже, автентифікується та шифрується.

Площина даних (також називається площиною пересилання) забезпечує інфраструктуру для надсилання трафіку користувача через мережу накладання SD-WAN. Трафік площини даних зазвичай проходить у безпечних тунелях Internet Security (IPsec).

Висновки. Проведені дослідження та аналіз вимог до комунікаційної мережі Держприкордонслужби дозволили визначити потребу в параметрах високої доступності, які є ключовими для успішної реалізації цієї архітектури. Представлена ієрархічна модель архітектури цифрової мережі SD-WAN дозволяє оптимально розподіляти трафік і забезпечувати високу продуктивність мережі. Ця модель стане основою для подальшого розгортання та вдосконалення мережі Державної прикордонної служби України, забезпечуючи надійний та швидкий обмін даними.

Розроблена концептуальна модель дозволить підвищити ефективність та надійність комунікаційної інфраструктури Державної прикордонної служби України. Запровадження адаптованої концептуальної моделі архітектури цифрової мережі SD-WAN є кроком у цьому напрямку. Дані дослідження допоможуть у подальших роботах із розгортання та оптимізації мережі, забезпечуючи безперервний доступ до важливої інформації та покращуючи комунікаційні можливості Державної прикордонної служби України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Borovick L., Mehra R. Architecting the Network for the Cloud. White paper. *IDC. Analize the Future.* 2011. URL: https://www.cisco.com/c/dam/global/en_ca/solutions/midsize/docs/idc_architecting_the_network_for_the_cloud.pdf (date of access: 15.02.2024).

2. Azodolmolky S., Wieder P., Yahyapour R. Cloud computing networking: Challenges and opportunities for innovations. *IEEE Communications Magazine.* 2013. Vol. 51, no. 7. P. 54–62.

3. Banikazemi M. et al. Meridian: an SDN platform for cloud network services. *IEEE Communications Magazine.* 2013. Vol. 51, no. 2. P. 120–127.

4. Diarmuid Seosamh Ó. Briain. Department of Aerospace, Mechanical and Electronic Engineering. 2015.

5. BGP Routing Interoperability. URL: https://www.silver-peak.com/products/unity-edge-connect/bgp-routing (date of access: 15.02.2024).

6. How Cisco SD-WAN works? *NetworkAcademy.* URL: https://www.networkacademy.io/ccie-enterprise/sdwan/how-cisco-sd-wan-works (date of access: 15.02.2024).

7. Cisco SD-WAN High Availability. *NetworkAcademy.* URL: https://www.networkacademy.io/ccie-enterprise/sdwan/high-availability (date of access: 15.02.2024).

8. What is SASE? *NetworkAcademy.* URL: https://www.networkacademy.io/ccie-enterprise/sdwan/what-is-sase (date of access: 15.02.2024).

9. Monaco, Matthew, Oliver Michel and Eric Keller. Applying operating system principles to SDN controller design. // Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks. ACM, 2013.

10. Kannan, Kalapriya and Subhasis Banerjee. Compact TCAM: Flow entry compaction in TCAM for power aware SDN. // International Conference on Distributed Computing and Networking. Springer Berlin Heidelberg, 2013.

11. Banikazemi, Mohammad et al. Meridian: an SDN platform for cloud network services. // IEEE Communications Magazine 51.2. 2013. P. 120–127.

12. Hu, Hongxin et al. Towards a reliable SDN firewall. Presented as part of the Open Networking Summit 2014 (ONS 2014). 2014.

13. Masoud, Mohammad Z., Yousf Jaradat and Ismael Jannoud. On preventing ARP poisoning attack utilizing Software Defined Network (SDN) paradigm. Applied Electrical Engineering and Computing Technologies (AEECT), 2015 IEEE Jordan Conference on. IEEE, 2015.