УДК 004.7

Волинець Б. О., магістрант, група КБм-21-1,
Науковий керівник: Єфіменко А. А., канд. техн. наук, доцент,
Вакалюк Т. А., д-р пед. наук, професор, професор кафедри ІПЗ
Державний університет «Житомирська політехніка»

АНАЛІЗ ТА ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ БАГАТОТОЧКОВИХ ДИНАМІЧНИХ ВІРТУАЛЬНИХ МЕРЕЖ

Динамічна багатоточкова віртуальна приватна мережа (DMVPN, Dynamic Multipoint VPN) – це технологія розроблена компанією Cisco, що забезпечує захищений обмін даними між сайтами (маршрутизаторами) без проходження трафіку через центральний сервер (маршрутизатор) віртуальної приватної мережі компанії. DMVPN дозволяє організаціям створювати мережу VPN з декількома сайтами без необхідності статичного налаштування пристроїв. DMVPN будує сітчасту VPN топологію «Hub and Spoke», в якій маршрутизатор кожного віддаленого сайту налаштований на підключення до центральної точки VPN компанії, щоб забезпечити доступ до необхідних ресурсів. У той же час кожен сайт («клієнт») може з'єднуватися безпосередньо з усіма іншими клієнтами, незалежно від їх розташування і без необхідності проходження через центральний вузол [1].

За допомогою DMVPN підключення між філіями забезпечуються через загальнодоступне підключення до глобальної мережі або Інтернет. DMVPN працює як на маршрутизаторах, так і на міжмережних екранах компанії Cisco. Кожен віддалений сайт має маршрутизатор, налаштований для підключення до VPN-хабу, що знаходиться в головному офісі компанії.

Коли два користувача обмінюються даними (наприклад, для забезпечення виклику Voice over IP) один із клієнтів зв'яжеться з центральною інстанцією (Hub) та отримає необхідну інформацію про іншого клієнта для створення між ними динамічного тунелю IPsec VPN. Користувачі не використовують постійне VPN-з'єднання, натомість вони спілкуються через з використанням централізованої модель «Hub-and-Spoke», яка застосовує захист VPN та детальний контроль доступу за потреби [1].

DMVPN складається з таких ключових складових [4]: багатоточкові тунельні інтерфейси (mGRE, Multipoint Generic Routing Encapsulation); протокол наступного переходу (NHRP, Next Hop Resolution Protocol); механізм виявлення кінцевої точки тунелю (TED, Tunnel Endpoint Discovery); протокол маршрутизації.

DMVPN і mGRE дозволяють компанії додавати кілька пунктів призначення, маючи лише один тунельний інтерфейс на кожному маршрутизаторі. По суті, mGRE має один інтерфейс GRE на кожному маршрутизаторі з можливістю кількох пунктів призначення. Цей інтер-фейс захищається за допомогою кількох тунелів IPsec і зменшує за-гальний обсяг конфігурації DMVPN. Однак, якщо двом маршрутизаторам потрібно тунелювати трафік, mGRE та GRE типу «Point-to-Point» можуть не знати, які IP-адреси використовувати. Щоб вирішити цю проблему, використовується протокол наступного переходу NHRP [4].

NHRP може розгортати кінцеві пристрої з призначеними IP-адресами. Клієнтів можуть з'єднати з хабом DMVPN. Цей протокол потрібен одному маршрутизатору гілки, щоб знайти публічний IP-адрес іншого маршрутизатора. NHRP використовує модель «сервер-клієнт», де один маршрутизатор функціонує як сервер NHRP, а інші маршрутизатори є клієнтами NHRP. У багатоточковій топології GRE/DMVPN маршрутизатор, який відіграє роль хаба є сервером NHRP, а всі інші маршрутизатори відіграють роль клієнтів. Кожен клієнт реєструється на сервері та повідомляє свою публічну IP-адресу, яку сервер відстежує у своєму кеші. Завдяки процесу, який включає реєстрацію та запити на вирішення від клієнтських маршрутизаторів, а також відповіді на вирішення від маршрутизатора сервера, увімкнено трафік між різними маршрутизаторами в DMVPN [4].

Механізм TED дозволяє маршрутизаторам автоматично виявляти точки IPsec, тому статичні криптокарти між окремими кінцевими точками тунелю IPsec не потребують налаштування. TED дозволяє кінцевим точкам динамічно ініціювати переговори щодо тунелів IPsec для виявлення невідомих пристроїв. [1]

Протоколи маршрутизації дозволяють DMVPN ефективно та ефективно знаходити маршрути між різними кінцевими точками. Щоб створити масштабований і стабільний DMVPN, важливо вибрати правильний протокол маршрутизації. Одним з варіантів є використання протоколу внутрішньої маршрутизації. OSPF найкраще підходить для розгортання невеликих мереж на базі DMVPN . Для середніх та великих мереж більше підходять протоколи EIGRP або BGP. EIGRP не обмежений обмеженнями топології протоколу стану каналу, і його легше розгортати та масштабувати в топології DMVPN. BGP може масштабуватися до багатьох однорангових і маршрутів, і це створює менше навантаження на маршрутизатори в порівнянні з іншими протоколами маршрутизації [1].

Існує три різні типи або так звані фази дизайну DMVPN: Фаза 1, Фаза 2, Фаза 3. На першій фазі користувачі DMVPN реєструють на хабі. На цій початковій стадії немає прямого зв'язку між клієнтами, тому весь трафік проходить через головний сервер. Кожна кінцева точка використовує звичайні інтерфейси тунелю GRE типу «Point-to-Point» і вимагає лише маршруту за замовчуванням до вузла, щоб до-сягти інших кінцевих точок. В результаті конфігурація маршрутизації на цьому етапі проста [1].

На другій фазі можна розгортати тунель типу «Spoke-to-Spoke» з усіма сполучними маршрутизаторами, які використовують багатоточкові тунелі GRE. Ці прямі тунелі запускаються на основі трафіку клієнта. Це означає, що дані не повинні передаватися до вузла. Хоча центральна точка використовується для площини керування, йому не обов'язково знаходиться в кругообігу даних [1].

На третій фазі розгортаються прямі тунелі без використання певних заздалегідь прокладених маршрутів. Для забезпечення безпеки цих маршрутів на льоту на даному етапі використовуються сигнальні повідомлення NHRP про рух (перенаправляють та використовують короткі шляхи) з вузла зв'язку [1].

Також існує розширення технології DMVPN – технологія FlexVPN, яка ще нмає назву четверта фаза DMVPN. За своєю суттю FlexVPN створена на тих же фундаментальних технологіях як і DMVPN, але має певні відмінності [2]. Так, наприклад, IPsec на відміну від стандартного DMVPN використовують IKEv2 замість IKEv1 для узгодження IPsec SA. IKEv2 має кращі характеристики порівняно з IKEv1, починаючи від стійкості і закінчуючи швидкістю для встановлення захищеного каналу зв'язку [3]. У GRE використовуються ста-тичні та динамічні «Point-to-Point» інтерфейси, а не лише один статичний багатоточковий інтерфейс mGRE. Ця конфігурація забезпечує додаткову гнучкість, особливо в роботі клієнтів та вузлів [3].

У FlexVPN NHRP, як правило, використовується для ведення переговорів. Варто зазначити, що клієнти у цій технології не реєструються на центральному хабі [2]. Оскільки кінцеві пристрої не здійснюють реєстрацію NHRP, потрібно покладатися на інші механізми, щоб переконатися, що вузол і клієнти можуть спілкуватися в двох напрямках. Як і в DMVPN, можна використовувати протоколи динамічної маршрутизації. Однак FlexVPN дозволяє використовувати IPsec для введення інформації про маршрутизацію. Вводиться маршрут за замовчуванням для IP-адреси з іншого боку тунелю, що дозволяє забезпечити прямий зв'язок з центрольною інстанцією [2].

Окрім технологій DMVPN від компанії Cisco існують схожі рішення від інших розробників. Так, наприклад, компанія Huawei розробила технологію розумного динамічного VPN, яка ідентична DMVPN, завдяки чому їх часто використовують разом у випадках, коли неможливо забезпечити використання пристроїв лише однієї компанії [5]. Також існує рішення DMVPN на платформі Vyatta, для якої спільнота розробників створила власну реалізацію протоколу NHRP з відкритим кодом, назвавши його OpenNHRP. Цей проект не є повністю закінченим рішенням, але показує можливості відкритої реалізації фірмових складових технології DMVPN. Код проекту доступний через SourceForge.

Переваги використання DMVPN є такими: – спрощена конфігурація маршрутизації; підтримка динамічного розгортання кінцевих вузлів за допомогою NHRP; низькі адміністративні витрати; підтримка QoS; висока масштабованість та доступність.

Розлянемо дані переваги дещо детальніше. У DMVPN не потрібні кілька тунельних інтерфейсів для кожної гілки (клієнта) VPN. Замість цього проста конфігурація вузла і користувачів забезпечує мережеве підключення на вимогу з динамічною маршрутизацією та багатоадресною IP-адресою. DMVPN також підтримує розгортання «Zero Touch», щоб додати більше віддалених сайтів. Ця спрощена, масштабована топологія ідеально підходить для організацій, яким потрібне зашифроване підключення до глобальної мережі між віддаленими сайтами, включаючи мереж типу SOHO, мережі середнього та великого розміру [1].

За допомогою DMVPN і NHRP можна розгортати користувачів за допомогою динамічно призначених публічних IP-адрес. Кожен клієнт може створити VPN-тунель з іншими, знайшовши їх загальнодоступні IP-адреси [1]. DMVPN спрощує топологію WAN-мережі, зменшуючи витрати на конфігурування. Не потрібно налаштовувати крипто-карти, прив'язані до фізичного інтерфейсу, або вносити зміни в центрі, щоб додати більше користувачів. Крім того, централізовані зміни конфігурації в хабі контролюють поведінку розділеного тунелювання, що ще більше спрощує конфігурацію та знижує витрати [1].

DMVPN підтримує численні механізми розширеної якості обслуговування (QoS) , включаючи формування трафіку в інтерфейсах вузла за принципом Per-Spoke/Per-Spoke-Group, а також політику QoS Hub-to-Spoke/Spoke-to-Spoke. Також підтримує динамічні політики якості обслуговування QoS, які автоматично приєднують шаблони QoS до тунелів у міру їх встановлення [1].

DMVPN інтегрує шифрування в систему балансування навантаження сервера або поширюється на виділені головні VPN-маршрутизатори. Є можливість масштабуватися до тисяч користувачів з ієрархічним розгортанням вузла для більшої масштабованості. Щоб підвищити продуктивність, тунелі розподіляються між доступними вузлами [1]. DMVPN також забезпечує підвищену безпеку для під мереж кінцевих користувачів, підтримуючи сполучні маршрутизатори, які виконують трансляцію мережних адрес (NAT) або розміщені за динамічними пристроями NAT. Він також забезпечує ефективний і масштабований розподіл трафіку «One-to-Many» і «Many-to-Many» з підтримкою багатоадресного IP-трафіку між користувачем та вузлом [1]. Якщо порівнювати технологію DMVPN із звичайною VPN, то перша забезпечує багато переваг, включаючи наступні переваги: високу швидкість мережі і характерна надійність, покращення зв'язку між філіями за рахунок інтеграції VPN в існуючі методи комунікації, збереження пропускної здатності WAN та підвищена стійкість і резервування мережі [1].

Список використаних джерел

1. Dynamic Multipoint VPN (DMVPN) [Електронний ресурс] / Rahul Awati,. – Електрон. текст. дані. – Режим доступу: https://www.techtarget.com/searchnetworking/definition/dynamic-multipoint-VPN-DMVPN. – Дата останнього доступу: 16.11.2021. – Назва з екрану.
2. Cisco FlexVPN DMVPN, Part 1 – Overview and Design [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/. – Дата останнього доступу: 16.11.2021. – Назва з екрану.

3. Cisco IOS FlexVPN Data Sheet [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html. – Дата останнього доступу: 16.11.2021. – Назва з екрану.

4. Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/ configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html. – Дата останнього доступу: 16.11.2021. – Назва з екрану.

5. NetEngine AR V300R019 CLI-based Configuration Guide - VPN [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: https://support.huawei.com/enterprise/en/doc/EDOC1100112360/3ae1a4cf/implementationl. – Дата останнього доступу: 16.11.2021. – Назва з екрану.