ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «**РОЗРОБКА СИСТЕМИ ЗАХИСТУ ГЛОБАЛЬНИХ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЇ PALO ALTO NETWORKS»**

на здобуття освітнього ступеня бакалавра (магістра)
зі спеціальності ___122 Комп'ютерні науки_____
(код, найменування спеціальності)
освітньо-професійної програми ___Комп'ютерні науки_____
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ ____Анастасія Кравець____
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувачка вищої освіти гр. КНД-41
____Анастасія Кравець_____
Ім'я, ПРІЗВИЩЕ
Керівник: _____Микола Гніденко_____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра ____Комп'ютерних наук_____

Ступінь вищої освіти ____«Бакалавр»_____

Спеціальність ____«122 Комп'ютерні науки»_____

Освітньо-професійна програма ____«Комп'ютерні науки»_____

ЗАТВЕРДЖУЮ
Завідувач кафедрою ____Комп'ютерні науки__
___Віктор Вишнівський___ Ім'я, ПРІЗВИЩЕ
«____» _____ 20__ р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

_____Кравець Анастасія Андріївна_____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Розробка системи захисту глобальних програмно-визначених мереж на основі технології Palo Alto Networks»

керівник кваліфікаційної роботи Микола Гніденко, доцент кафедри, кандидат технічних наук, академік Української академії наук,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 р. № 36

2. Строк подання кваліфікаційної роботи «31» травня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: мультисервісні системи, технології SD-WAN, системи безпеки мережі, архітектури мережевих інфраструктур, інструменти керування і моніторингу, VPN і шифрування, бізнес-вимоги і політики, науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Моделі та стратегія SD-WAN від Palo Alto Networks_____

2. Концепції та сервіси для WAN і віддалених місць
3. Деталі дизайну Palo Alto Networks
4. Моделі проєктування SD-WAN

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання 24.02.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Огляд літератури та формулювання мети роботи	04.03-10.03.24	вик.
2	Аналіз моделей дизайну SD-WAN від Palo Alto Networks	11.03-30.03.24	вик.
3	Дослідження основних концепцій та сервісів WAN	01.04-10.04.24	вик.
4	Вивчення конструкцій та управління розгортанням SD-WAN	11.04-30.94.24	вик.
5	Аналіз методів маршрутизації в SD-WAN	01.05-16.05.24	вик.
6	Дослідження моделей проєктування SD-WAN	17.05-18.05.24	вик.
7	Проведення практичних досліджень та аналіз результатів	19.05-20.05.24	вик.
8	Узагальнення результатів дослідження та підготовка остаточного варіанту роботи	20.05-24.05.24	вик.

Здобувач(ка) вищої освіти _____ Анастасія Кравець
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Микола Гніденко
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 70 стор., 31 рис., 5 табл., 8 джерел.

Мета роботи – аналіз моделей та стратегій SD-WAN від Palo Alto Networks, вивчення концепцій і сервісів для WAN та віддалених місць, а також дослідження методів маршрутизації та захисту в SD-WAN.

Об'єкт дослідження – програмно-апаратні рішення для управління широкосмуговими мережами (WAN) та захисту віддалених місць, які пропонує Palo Alto Networks.

Предмет дослідження – архітектурні моделі SD-WAN, методи маршрутизації, стратегії безпеки, управління розгортанням та інтеграція з хмарними сервісами у рамках рішень від Palo Alto Networks.

Короткий зміст роботи:

Робота досліджує моделі та стратегії SD-WAN від Palo Alto Networks, зокрема моделі дизайну безпеки SD-WAN на основі PAN-OS та CloudGenix. Описується стратегія Palo Alto Networks щодо SD-WAN, а також надається огляд концепцій та сервісів для WAN і віддалених місць. Включає огляд різних опцій доступу до Інтернету для віддалених місць і технологію Secure Access Service Edge (SASE). Розглядаються деталі дизайну Palo Alto Networks, зокрема нові конструкції для PAN-OS Secure SD-WAN, керування розгортанням SD-WAN за допомогою Panorama, створення зон безпеки та оверлей AutoVPN, а також маршрутизація SD-WAN і захист місць.

Також досліджуються різні моделі проєктування SD-WAN, зокрема модель PAN-OS Secure SD-WAN та CloudGenix з Prisma Access. Висновки роботи підсумовують результати дослідження та надають рекомендації щодо впровадження SD-WAN технологій у підприємствах.

КЛЮЧОВІ СЛОВА: SD-WAN, Palo Alto Networks, PAN-OS, CloudGenix, Prisma Access, WAN, Маршрутизація, Безпека мережі, Panorama, AutoVPN, Secure Access Service Edge (SASE), Оверлейні мережі, Віддалені місця, Зони безпеки, Інтернет-доступ.

ЗМІСТ

ВСТУП

У сучасному цифровому світі безпека мережі є однією з найважливіших проблем. Захист глобальних програмно-визначених мереж (SDN) від кіберзагроз стає все складнішим завданням через постійний розвиток технологій і збільшення кількості кібератак.

Одним з передових рішень у цій галузі є використання технології від компанії Palo Alto Networks, яка пропонує ефективні засоби захисту мережі. Заснована у 2005 році, вона зарекомендувала себе як створювач інноваційної системи безпеки, що включає в себе файрвол, захист кінцевих точок та хмарну платформу для виявлення кіберзагроз. Остання складова надає антивірусне програмне забезпечення у форматі SaaS. Компанія спеціалізується на наданні послуг безпеки для великих корпорацій у таких сферах, як виробництво, охорона здоров'я, освіта і фінанси.

У процесі дослідження буде розглянуто основні проблеми забезпечення безпеки SDN і досліджено прототип системи захисту, який буде використовувати ключові можливості технології Palo Alto Networks. Вона має велике значення для розуміння принципів захисту мережі в умовах розширення SDN. Розглянута система може бути використана як основа для подальших досліджень і розвитку засобів захисту мережі в майбутньому.

У рамках роботи буде описана референтна архітектура, а саме як SD-WAN дозволяє організаціям ефективніше використовувати свої WAN-зв'язки та отримувати можливість відстежувати й контролювати як трафік користувачів на віддалених об’єктах, який направляється в Інтернет, так і WAN-трафік організації, що направляється в інший віддалений об’єкт, великий кампус або центр обробки даних. Ця архітектура включає рекомендації щодо найкращих практик, які спрощують та оптимізують WAN-дизайн для певної організації та одночасно забезпечують безпечний прямий доступ до Інтернету для хмарних додатків. Palo

Alto Networks надає організаціям дві рекомендовані моделі дизайну для розгортання SD-WAN: CloudGenix SD-WAN з Prisma Access та PAN-OS Secure SD-WAN. Крім широкого огляду WAN, робота буде охоплювати глибокі технічні аспекти як CloudGenix SD-WAN, так і PAN-OS Secure SD-WAN, і описувати найкращі методи інтеграції CloudGenix з Prisma Access.

1 МОДЕЛІ ТА СТРАТЕГІЯ SD-WAN ВІД PALO ALTO NETWORKS

1.1 Модель дизайну безпеки SD-WAN на основі PAN-OS

Брандмауери наступного покоління від Palo Alto Networks, що працюють під управлінням PAN-OS, мають вбудований набір функцій гарантії безпеки та SD-WAN, які затверджують найвищий рівень контролю для організації.

Версія PAN-OS 9.1 (рис. 1.1) включає підписку на SD-WAN, яка надає інтелектуальний вибір шляху на основі існуючої безпеки PAN-OS. Це дозволяє уникнути складності роботи з багатьма постачальниками, об'єднуючи функції в єдиний багатофункціональний засіб безпеки, що включає SD-WAN. Брандмауер наступного покоління забезпечує видимість використання застосунків і контроль доступу до них завдяки App-ID™, яка інспектує сесії та трафік, ідентифікуючи застосунки для детального контролю. Ця видимість важлива для інтелектуального вибору шляху в SD-WAN.

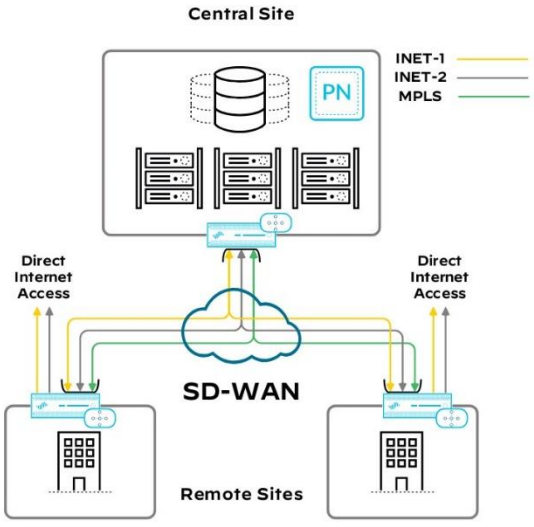


Рис. 1.1 PAN-OS Secure SD-WAN.

Рішення безпечного SD-WAN на основі PAN-OS керується за допомогою Panorama™, який використовують для конфігурації та моніторингу пристроїв на

центральному і віддалених об’єктах. При цьому застосовуються шаблони для конфігурації мережі та пристроїв, а також групи пристроїв для конфігурації політик та об'єктів, включаючи нові функції SD-WAN конкретно для PAN-OS версії 9.1. Panorama включає плагін SD-WAN, який використовується для створення оверлейної мережі на основі тунелів IPSec, конфігурації динамічної маршрутизації між місцями та забезпечення централізованої видимості для SD-WAN.

Крім можливостей SD-WAN, брандмауери наступного покоління від Palo Alto Networks надають комплексний захист, що дозволяє організаціям:

- Надавати користувачам, контенту та застосункам, включаючи застосунки SaaS, безпечний доступ до різних ресурсів і сервісів у мережі, шляхом класифікації всього трафіку незалежно від порту.
- Зменшувати ризик атаки за допомогою моделі позитивного виконання, що надає дозвіл на роботу всім бажаним застосункам та блокує решту.
- Застосовувати політики безпеки для блокування шкідливого ПЗ: вірусів, програм, що вимагають викупу, шпигунських програм, ботнетів тощо.
- Застосовувати послідовну безпеку для локальних (on-premises) та хмарних середовищ і відділень.

1.2 Модель дизайну SD-WAN від CloudGenix

Компанія Palo Alto Networks придбала компанію CloudGenix у квітні 2020 року. Її можливості хмарного розгалуження та підхід, що визначається застосунками, значно прискорили розвиток Palo Alto Networks в галузі безпечного доступу до сервісу на межі. Рішення CloudGenix SD-WAN, надане пристроями CloudGenix Instant-On Network (ION), дозволяє застосовувати політику на основі бізнес-наміру, забезпечує динамічний вибір шляху та надає видимість продуктивності та доступності для застосунків та мереж.

Після розгортання на об’єкті, пристрої CloudGenix ION автоматично встановлюють VPN-з'єднання з центрами обробки даних через кожен інтернет-канал. Крім того, пристрої ION створюють VPN-з'єднання через приватні WAN-канали, які використовують одного постачальника послуг. Після цього можна визначити політику застосунків для продуктивності, безпеки та відповідності, яка відповідає бізнес-наміру організації. Пристрої ION автоматично вибирають найкращий шлях WAN для застосунків (рис. 1.2). Вони використовують бізнес-політику та аналіз в реальному часі метрик продуктивності застосунків та WAN-з'єднань для визначення відповідного шляху.

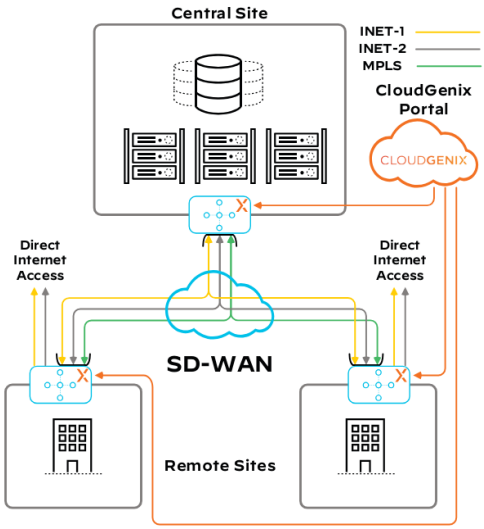


Рис. 1.2 CloudGenix SD-WAN.

У результаті виконуються всі аспекти конфігурації, управління, моніторингу апаратного та програмного забезпечення CloudGenix ION з багатопрофільного хмарного порталу управління CloudGenix. Пристрої ION попередньо сконфігуровані для аутентифікації в порталі та підтримують розгортання і встановлення без дотику до них.

1.3 Стратегія Palo Alto Networks щодо SD-WAN

Стратегія SD-WAN від Palo Alto Networks дозволяє обрати, яка архітектура SD-WAN найбільше підходить для організації. Компанія активно вдосконалює як

існуючу технологію CloudGenix SD-WAN, так і технологію PAN-OS Secure SD-WAN. Ця подвійна стратегія SD-WAN надає можливість реалізувати SD-WAN в приміщенні або в хмарі, з використанням обраної платформи.

Prisma Access для мереж надає безпеку та запобігання загрозам для віддалених мереж, дозволяючи безпечно використовувати застосунки та інтернет. Віддалені мережі підключаються до Prisma Access через пристрій з підтримкою IPSec VPN. Управління здійснюється через Panorama, що забезпечує повний набір функцій PAN-OS. Prisma Access підходить для віддалених місць з інтернет-з'єднаннями та забезпечує прямий доступ до інтернету і зв'язок з іншими віддаленими об’єктами. Вона надає прямий доступ до інтернету без перенаправлення трафіку на центральний об’єкт, забезпечуючи той самий рівень безпеки, видимості та контролю, що й брандмауери Palo Alto Networks на центральному об’єкті.

Навіть до придбання Palo Alto Networks, CloudGenix SD-WAN мав міцний зв’язок з Prisma Access (рис. 1.3). Поєднання цих двох технологій дозволяє мати незавантажений віддалений об’єкт, при цьому забезпечуючи комплексну безпеку.

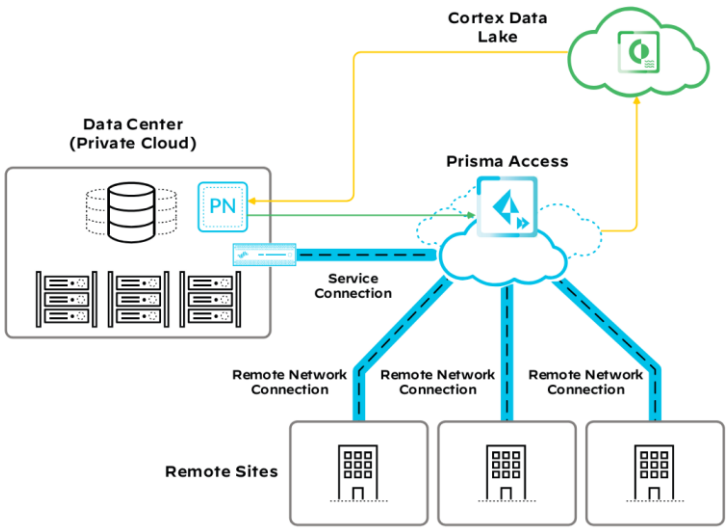


Рис. 1.3 Prisma Access для мереж.

2 КОНЦЕПЦІЇ ТА СЕРВІСИ ДЛЯ WAN І ВІДДАЛЕНИХ МІСЦЬ

Організації використовують різні підходи до захисту мережі центрального об’єкта. Він включає в себе високовидимий периметр мережі для організації, що обґрунтовує значні інвестиції у інфраструктуру безпеки для захисту цього периметру. Підхід, що використовується для центрального об’єкта, зазвичай включає "повний стек" мережевої безпеки, доповнений присутністю персоналу з оперативного управління безпекою для реагування на загрози.

Підхід для віддалених місць зазвичай відрізняється кількома способами. Персонал з оперативного управління безпекою рідко буває на місці віддаленого об’єкта. Також їх може бути величезна кількість, що ускладнює обґрунтування витрат навіть на масштабоване рішення "повного стеку". Більшість мережевого трафіку з віддаленого місця призначена для центрального або Інтернету. Якщо безпека є найважливішою, організації можуть вимагати пересилати весь мережевий трафік віддаленого об’єкта на центральний для перевірки.

Для врахування бізнес-вимог, що постійно розвиваються, організації використовують SaaS-застосунки та переносять внутрішні застосунки та робочі навантаження в хмару. Неефективно покладатися на застарілу мережеву та безпечну архітектуру, яка вимагає відправляти весь мережевий трафік на центральний об’єкт для перевірки, коли користувачі можуть отримати доступ до цих же застосунків більш ефективно завдяки прямому доступу через публічні мережі. Однак, дозволяючи доступ до публічних мереж з багатьох віддалених місць та не надаючи еквівалентних з центральним об’єктом можливостей безпеки, збільшується загальний ризик для організації.

Деякі організації вирішують взяти на себе певний ризик заради зменшення витрат. Зазвичай цей підхід передбачає використання недорогої системи об'єднаного управління загрозами (UTM), яка часто має менше функцій та можливостей порівняно з системами, розгорнутими на центральному місці. Ще

одним поширеним підходом є використання функцій брандмауера з підтримкою стану разом із простим перекладом мережевих адрес (NAT) на існуючому маршрутизаторі WAN.

2.1 Огляд WAN

Метою WAN є з'єднання локальних мереж (LAN) в центральних місцях організації і віддалених місць (рис. 2.1). Останніми роками багатопротокольне маркування (MPLS) та Інтернет витіснили більшість інших варіантів. SD-WAN продовжує це витіснення, дозволяючи комодифікацію як MPLS, так і Інтернету.

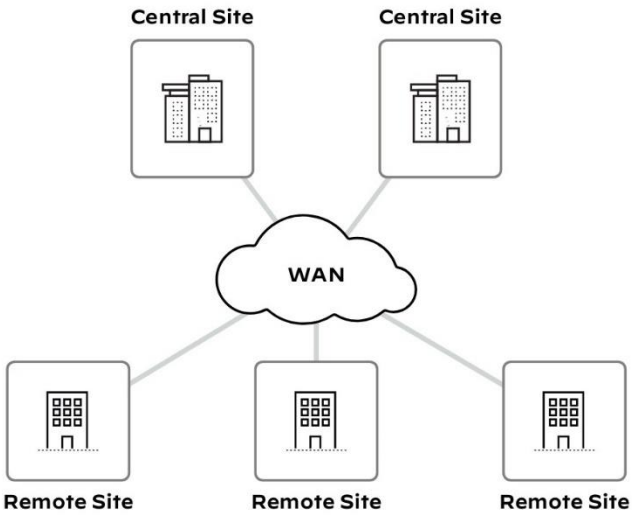


Рис. 2.1 Дизайн WAN.

Кожна описана технологія WAN має свої переваги та недоліки. Дослідження недоліків кожної з них та методів, розроблених для їх подолання, надасть чітке розуміння і ключові стимули розвитку SD-WAN.

MPLS VPN

У мережевій індустрії MPLS-послуги розглядаються як приватні послуги WAN, оскільки постачальник послуг забезпечує сегментацію та ізоляцію між

клієнтами, навіть якщо вони використовують спільну інфраструктуру по всій мережі. Мережа постачальника послуг MPLS використовує високошвидкісну основну мережу для з'єднання пристроїв обробки клієнтів (provider edge – PE), які постачальник використовує для доступу. Постачальник послуг може використовувати пристрої PE для кількох клієнтів: він створює віртуальну приватну мережу MPLS (VPN), що забезпечує логічну роздільність, для кожного клієнта. Пристрої PE використовують багатопротокольний BGP для розповсюдження інформації маршрутизації для кожного клієнта в MPLS VPN.

Центральні та віддалені місця використовують пристрої країв клієнта (customer edge – CE) для підключення до пристроїв PE в мережі MPLS. У той час як декілька клієнтів використовують спільні пристрої PE, кожен пристрій CE призначений для одного клієнта. Для з'єднань PE-CE можна використовувати як BGP, так і статичну маршрутизацію.

Мережа MPLS підтримує різноманітні розширені можливості, такі як QoS, інженерія трафіку, віртуальна приватна LAN-служба, псевдодроти та мультікаст. Доступ клієнта до мережі MPLS може використовувати традиційні служби мультиплексування за часом (T1, E1 та DS3), проте наразі все частіше використовує підключення Ethernet зі швидкістю передачі даних до кількох гігабіт (рис. 2.2).

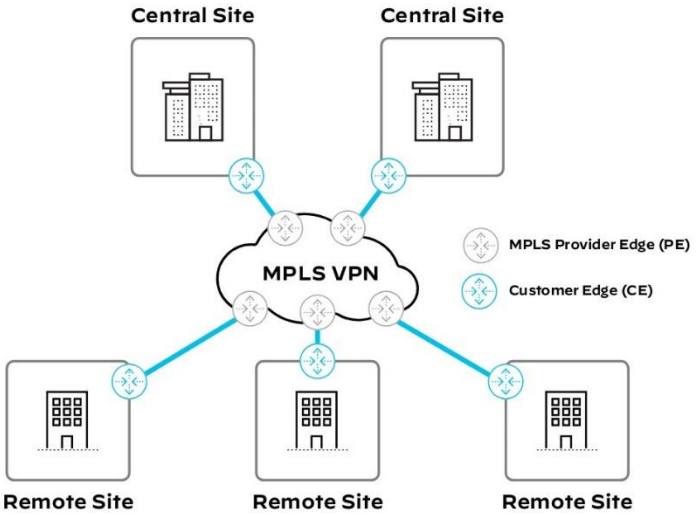


Рис. 2.2 MPLS VPN.

Internet VPN

Інтернет є відкритою мережею без явних гарантій конфіденційності даних. Це обмеження само по собі робить інтернет непридатним для використання як приватного транспорту WAN. Окрім того, він також не має розширених можливостей MPLS, найважливішою з яких є QoS. Однак, коли його поєднують з IPSec для створення зашифрованих VPN-тунелей, інтернет-VPN WAN надає відносно дешеву і безпечну альтернативу MPLS (рис. 2.3).

Доступ клієнта до Інтернету може використовувати традиційні методи, проте зараз все частіше використовує підключення Ethernet, DSL/cable (з Ethernet hando) або 4G/LTE.

Варто зазначити, що термін "Інтернет-VPN" передбачає, що мережа використовує шифрування для забезпечення конфіденційності та цілісності даних, тоді як термін "MPLS VPN" передбачає лише те, що постачальник послуг MPLS утримує дані клієнта логічно відокремленими від інших клієнтів. Якщо клієнт бажає шифрування, він зазвичай впроваджує його на своєму обладнанні на місці.

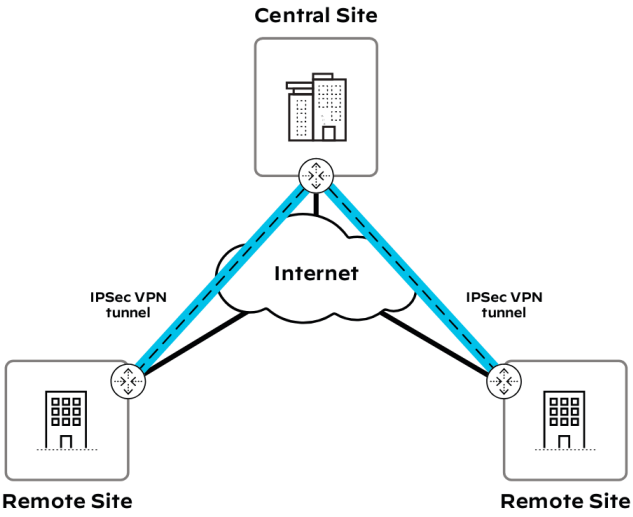


Рис. 2.3 Internet VPN WAN.

Наразі багато організацій в певній мірі застосовують інтернет-VPN для WAN. Об'єднані переваги відносно недорогої служби з конфіденційністю даних, забезпеченою за допомогою міцного шифрування, є переконливими.

- Ранні реалізації інтернет-VPN були не тільки важкі для управління, а й мали погану продуктивність через різноманітні причини, такі як відсутність апаратного прискорення шифрування та незрозумілі технічні характеристики. Ці технічні характеристики включають:
- Дотаткові витрати через капсуляцію тунелю: через них зменшується розмір максимальної передавальної одиниці (MTU) на тунелях, в результаті чого відбувається IP-фрагментація і втрата пакетів.
- Криптографічна аутентифікація за допомогою попередньо спільних ключів: великомасштабне використання та розподіл таких ключів є важким для управління та розподілу. Об’єкти з динамічною адресацією можуть вимагати універсальних попередньо спільних ключів, що в подальшому збільшує вплив їх оберту (key rotation – це процес зміни шифрувального ключа, який використовується для захисту даних під час передачі або зберігання).
- Криптографічна автентифікація за допомогою цифрових сертифікатів: вважається найкращою практикою в галузі. Проте доки не з'являться спрощені робочі процедури та інструменти для управління публічною інфраструктурою ключів, організації часто вважають впровадження та підтримку цифрових сертифікатів заважкими.
- Нестабільність тунелю при використанні спільної бази даних маршрутизації: динамічна маршрутизація зберігається в межах накладеної (тунельної) мережі окремо від маршрутизації, використовуваної для побудови накладення, особливо при використанні маршрутів за замовчуванням.

Поточні реалізації інтернет-VPN працюють ефективно при умові, що розширені функції увімкнуті, а кращі практики дотримуються. Під час розгляду інтернет-VPN слід обов’язково запевнитися, що пристрої здатні мінімізувати вплив IP-фрагментації. Ключова опція – це налаштування TCP MSS, яке вмикається на кінцевих точках VPN, аби переконатися, що комунікаційні кінцеві точки

узгоджують максимальний розмір сегмента TCP (MSS) на значення, яке усуває потребу в фрагментації. Комунікаційні кінцеві точки повинні використовувати техніки, такі як відкритий протокол управління повідомленнями Інтернету (ICMP), який виявляє максимальний розмір передавальної одиниці шляху задля визначення найменшого MTU. Варто наголосити, що якщо всі типи повідомлень ICMP блокуються, комунікаційні кінцеві точки не можуть визначити найбільш ефективний MTU за допомогою виявлення максимального розміру передавальної одиниці шляху ICMP.

При роботі з цифровими сертифікатами рекомендується використовувати автоматизовані процеси для їх реєстрації та анулювання, такі як простий протокол реєстрації сертифікатів і онлайн-протокол статусу сертифікатів. Ці процеси спрощують та оптимізують загальний робочий процес управління сертифікатами. Якщо попередньо було обрано використання спільних ключів, варто використати інструменти для генерації міцних, випадкових ключів та застосовувати унікальні ключі для кожного віддаленого об’єкта.

Якщо є можливість, також слід використовувати кілька віртуальних маршрутизаторів на кінцевій точці VPN. Зовнішній віртуальний маршрутизатор (або “front door” – "вхідні двері") надає маршрутну інформацію, яку використовують кінцеві точки для побудови VPN-тунелів. У той же час внутрішній віртуальний маршрутизатор надає маршрутну інформацію для трафіку, що проходить всередині VPN-тунелей. Використання кількох віртуальних маршрутизаторів розділяє контрольні точки маршрутизації, дозволяє використовувати кілька маршрутів за замовчуванням, а також запобігає нестабільності, коли кінцева точка VPN вивчає дубльовані маршрути через VPN-тунелі (рис. 2.4).

У цьому підході призначається зовнішній інтерфейс пристрою для вхідних дверей віртуального маршрутизатора, який потребує лише статичного маршруту за замовчуванням. Всі інші інтерфейси на пристрої, включаючи VPN-тунелі, продовжують використовувати віртуальний маршрутизатор за замовчуванням.

Також можливо реалізувати статичну або динамічну маршрутизацію на віртуальному маршрутизаторі за замовчуванням.

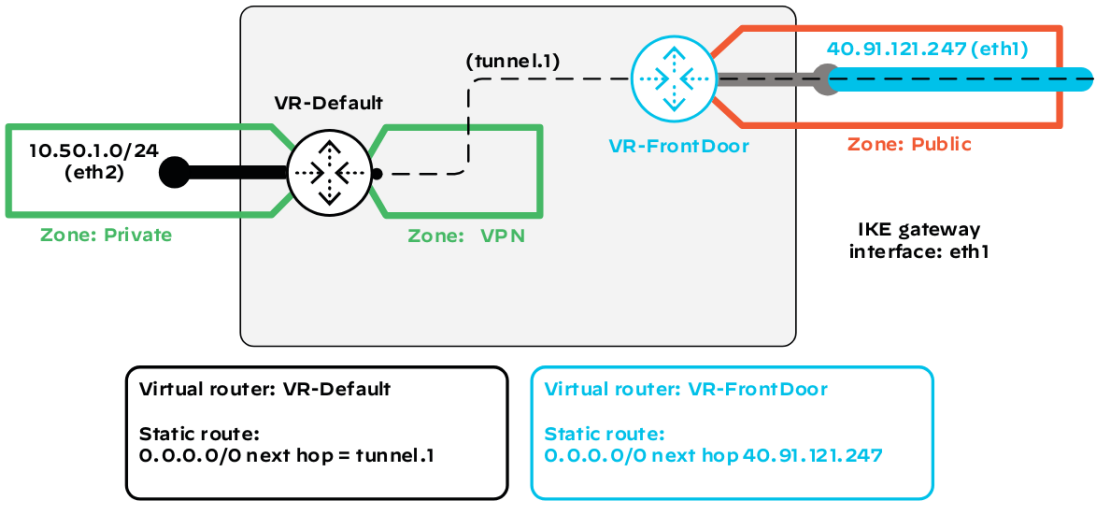


Рис. 2.4 Віртуальний маршрутизатор вхідних дверей.

Висока доступність WAN

Хоча MPLS й інтернет зазвичай є доволі надійними, у випадку виникнення відмови наслідки можуть бути значними. Відмови та порушення у WAN можуть відбуватися в мережі постачальника послуг. Не дивлячись на те, що вони трапляються рідко, відмови впливають на кілька клієнтів одночасно. Більш поширеними є відмови в WAN, які пов'язані з локальним доступом до віддаленого місця, у такому випадку відмова впливає лише на окремі місця для кількох клієнтів.

Ефективним підходом до підвищення загальної надійності WAN є включення кількох лінків і різноманітності лінків. Слід підключатися принаймні до двох WAN-транспортів у всіх ключових місцях організації. Обрані транспорти не повинні мати спільної інфраструктури, такої як живлення, фізичні медіа (волокно) або обладнання, і повинні використовувати різних постачальників послуг. Вартість покращеної різноманітності може бути високою, тому слід порівняти її з пов'язаним бізнес-ризиком відмов для віддалених об’єктів організації.

Після того, як у мережі є два або більше шляхи, слід покладатися на динамічні протоколи маршрутизації, щоб обрати найбільш оптимальні. Динамічні протоколи

маршрутизації використовують різні параметри для розрахунку таблиці маршрутизації, включаючи швидкість лінка, найкоротший шлях або автономну систему. Як варіант, можна використати статичну маршрутизацію, проте лише для об’єктів з єдиним шляхом.

Правильне проєктування WAN з використанням кількох транспортів WAN повинно швидко виявляти відмови в мережі та динамічно перенаправляти трафік на альтернативні шляхи. Зазвичай конфігуруються традиційні мережі WAN з використанням наступних методів (якщо є лише два шляхи):

- Активний/резервний: весь трафік пересилається по основному шляху, а на випадок відмови – по резервному. В інших випадках резервний шлях не використовується (рис. 2.5).
- Активний/активний: трафік розподіляється між обома шляхами на основі інформації про сесію. Якщо шлях відмовляє, трафік з відмовленого шляху перенаправляється на залишений активний шлях. Також він завжди може використовувати обидва шляхи.

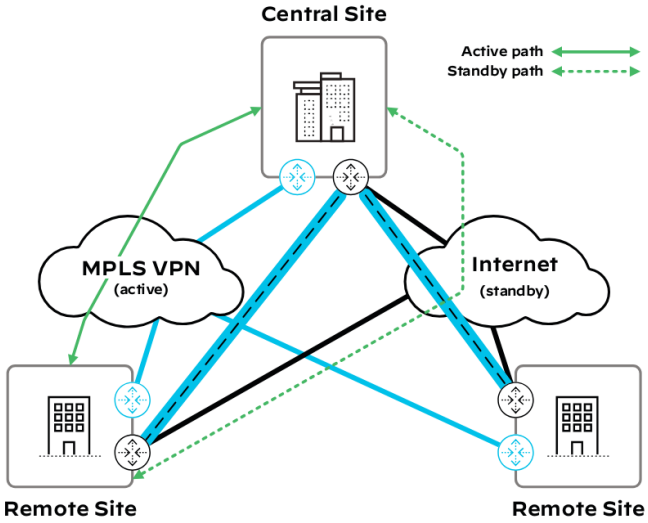


Рис. 2.5 Активний/резервний WAN з MPLS VPN і інтернет VPN.

Обидва методи мають свої переваги й недоліки. Наприклад, зайві витрати на WAN-транспорт, який використовується лише як резервний, не завжди є виправданими. Так само, якщо планується зменшити вплив перебоїв, то кожен

шлях, що використовується за методом активний/активний, повинен мати достатньо пропускної здатності для вміщення всього трафіку і ніколи не має перевищувати 50% використання, коли обидва шляхи активні.

Проєктування та впровадження різноманітності WAN ускладнюється, якщо комбінується різний транспорт, такий як MPLS і VPN WAN через інтернет, які не підтримують однакові можливості, наприклад, QoS. Додатки, що потребують QoS, можуть продовжувати працювати під час аварійних сценаріїв, коли вони перенаправляються в Інтернет, проте без QoS вони працюватимуть у погіршеному режимі.

Інші фактори, що впливають на впровадження різноманітності WAN, включають складність конфігурації. Постачальник послуг може вимагати BGP при підключенні до мережі MPLS, а VPN WAN може використовувати інший протокол маршрутизації, наприклад, OSPF. Ефективне розподілення навантаження та планування стійкості до відмов може бути неможливим, якщо всі шляхи не мають однакової пропускної здатності.

Програмно-визначена WAN

SD-WAN забезпечує збільшену гнучкість та контроль над трафіком мережі широкого доступу при використанні кількох транспортів WAN. Загалом рішення SD-WAN дозволяють створити мережу оверлей або мережеву тканину WAN з використанням різних транспортів WAN з різною пропускною здатністю та характеристиками продуктивності (рис. 2.6). SD-WAN, як правило, розподіляє навантаження трафіку по всіх шляхах у режимі активний/активний з урахуванням застосування. Ці рішення централізували майже всі аспекти керування пристроями, включаючи підключення пристроїв та робочі процеси з керування ключами, що робить розгортання на велику відстань відносно непомітним.

SD-WAN подолав обмеження MPLS VPN та інтернет-VPN, надаючи поширене шифрування даних, просту конфігурацію, активне використання всіх

зв'язків та швидку конвергенцію, а також знижуючи витрати за рахунок розширеного використання бюджетних транспортів WAN.

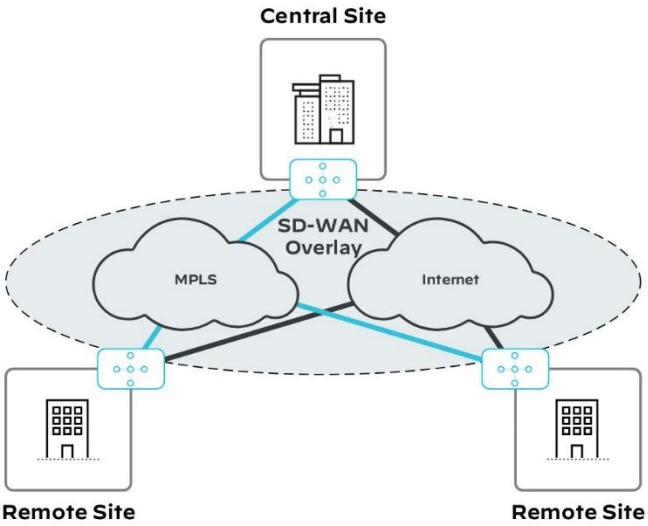


Рис. 2.6 Оверлей SD-WAN.

Усі пропозиції SD-WAN надають шифрування для конфіденційності даних з припущенням, що один або кілька транспортів використовують загальнодоступну мережу. Деякі пропозиції також можуть включати додаткові вбудовані можливості надання безпеки, але це не більше, ніж базові брандмауери. Стандартна стратегія гарантування безпеки для вендора, що спеціалізується на SD-WAN, полягає в інтеграції з постачальником безпеки стороннього вендора, таким як Palo Alto Networks. Якщо використовувати автономні брандмауери наступного покоління, можна розмістити їх у лінію з пристроєм SD-WAN. Аналогічно, можна розгорнути брандмауер серії VM у тій же хост-системі, що й віртуальну машину SD-WAN.

Кожне місце потребує пристрою SD-WAN, який підключається до різних транспортів WAN. Централізована платформа керування SD-WAN конфігурує та управляє пристроями SD-WAN. Як правило, використовуються як локальні, так і хмарні платформи управління. Можливості моніторингу та звітності платформи керування включають повну видимість всіх підключених місць та транспортів, якими кожне з них користується для доступу. У багатьох випадках як самі кінцеві пристрої WAN, так і платформи керування можуть бути віртуалізовані. Пристрої

SD-WAN збирають дані про продуктивність, використовуючи пасивний та/або активний моніторинг, і потім використовують цю інформацію для визначення характеристик реального часу продуктивності шляхів SD-WAN, таких як затримка, втрати та джитер (jitter).

Пристрої SD-WAN використовують ці дані про продуктивність для виявлення несправностей, таких як:

- Відмови в канал – повна відмова приєднаного каналу, часто виявлена через зміну протоколу лінії.
- Чорні діри – часткова відмова, що спостерігається, коли є повна втрата пакетів у одному напрямку.
- Погіршення – часткова відмова, що спостерігається при низькому рівні втрат (<10%) у одному або обох напрямках. Ця несправність має великий вплив на додатки голосу та відео і може спричинити повторну передачу для додатків TCP.
- Затримка – часткова відмова, що спостерігається, коли відносно середнього значення значно зростає затримка у взаємному обміні. Ця несправність має великий вплив на додатки голосу та відео вище певного порогу і може знизити пропускну здатність для передачі файлів.
- Джитер – часткова відмова, що спостерігається, коли відносне середньоквадратичне відхилення затримки збільшується значно відносно середнього. Ця несправність має великий вплив на додатки голосу та відео вище певного порогу.

Розширені можливості SD-WAN дозволяють організаціям створювати маршрутні політики, які відповідають додаткам з жорсткими вимогами до продуктивності та допомагають вибрати найкращий шлях. Пристрій SD-WAN використовує ці політики разом із даними про продуктивність для керування потоком мережевого трафіку.

Пристрої SD-WAN зазвичай можуть будувати VPN-тунелі з будь-якого інтерфейсу WAN. Замість потреби віртуального маршрутизатора вхідних дверей,

пристрій використовує інтерфейс-специфічні маршрути за замовчуванням. Ці маршрути надають інформацію про маршрутизацію, яку використовують кінцеві точки для побудови VPN-тунелі між кінцевими точками.

Оверлейна мережа SD-WAN інтегрується з мережами центрального та віддаленого об’єктів за допомогою статичної маршрутизації або стандартних протоколів, зазвичай BGP та OSPF. Однак сама оверлейна мережа SD-WAN може використовувати протоколи маршрутизації або централізований контролер SD-WAN для розподілу інформації про маршрутизацію. Пропрієтарні (власницькі) методи, такі як зонди, використовуються для підтримки маршрутизації, специфічної для додатків, та швидкого виявлення несправностей. Традиційні протоколи маршрутизації, такі як BGP, зазвичай не можуть ідентифікувати часткові відмови, такі як чорні діри або перебої в напрузі, у WAN. Агресивне налаштування таймерів протоколів маршрутизації може покращити час виявлення деяких випадків відмов, але з іншого боку виявлення несправностей SD-WAN перевершує підходи на основі протоколів маршрутизації, що використовуються в інших архітектурах WAN у всіх випадках.

2.2 Опції доступу до Інтернету для віддалених місць

Віддалені місця використовують WAN для зв'язку з головним офісом, центрами обробки даних тощо. Спільнота мережевих технологій зазвичай вважає WAN приватною мережею, хоча лише шифрування забезпечує справжню конфіденційність даних у мережі постачальника послуг. Шифрування даних у WAN досить просте: більшість підходів просто шифрують весь трафік, що залишається з місця без урахування використовуваних програм або точок зв'язку.

При розгляді мережевого трафіку, що покидає організацію, потрібно вживати додаткових заходів. Зовнішні зв'язки можуть включати зв'язок з бізнес-партнерами, хмарні сервіси та загальний доступ до веб-ресурсів. Простого шифрування недостатньо для захисту зовнішніх комунікацій. Для належного захисту необхідно

повністю бачити користувачів, програми та вміст, що проходить через корпоративні мережі, хмару і кінцеві точки. Тільки тоді можна реалізувати політики безпеки та вживати заходів, таких як блокування невідомого трафіку, ідентифікація складних атак або дозвіл лише на програми, що мають пов'язану з бізнесом ціль. Окрім шифрування, слід також використовувати брандмауери нового покоління для надання інспекції та видимості для трафіку, що входить та виходить з мережі.

Що стосується зовнішніх комунікацій для віддалених місць, існують різноманітні варіанти доступу до Інтернету для загального доступу до веб-ресурсів, а також до SaaS та інших хмарних сервісів.

Централізований доступ до Інтернету

Весь інтернет-трафік направляється на центральний об'єкт через приватну мережу, де забезпечується безпечний доступ до Інтернету. Це зменшує потребу в мережевій інфраструктурі безпеки на віддалених місцях, які захищаються центральною інфраструктурою. Однак такий підхід неефективно використовує пропускну здатність центрального об'єкта, оскільки трафік обробляється двічі. Збільшена затримка погіршує користувацький досвід на віддалених об'єктах через додатковий час при доступі до регіональних ресурсів (рис. 2.7).

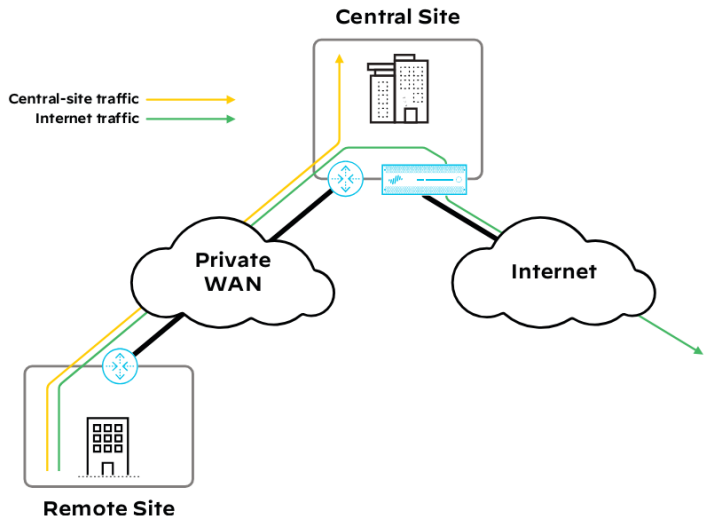


Рис. 2.7 Централізований доступ до Інтернету.

Хмарне Інтернет-підключення, надане клієнтом

У цьому варіанті весь інтернет-трафік перенаправляється через приватну мережу до найближчого хмарного центру з доступом до Інтернету. Ці центри доступу мають ту ж інфраструктуру безпеки, що й центральний об’єкт. Розгортання декількох хмарних центрів у певному регіоні допомагає зменшити затримку, пов'язану з пересиланням трафіку через центральний вузол. Центри доступу зазвичай розташовані в приміщеннях операторів зв'язку або в нейтральних місцях із доступом до транспортних послуг постачальників. Замовник орендує стійку та електроживлення для обладнання безпеки і несе витрати на адміністрування, конфігурацію, утримання та моніторинг (рис. 2.8).

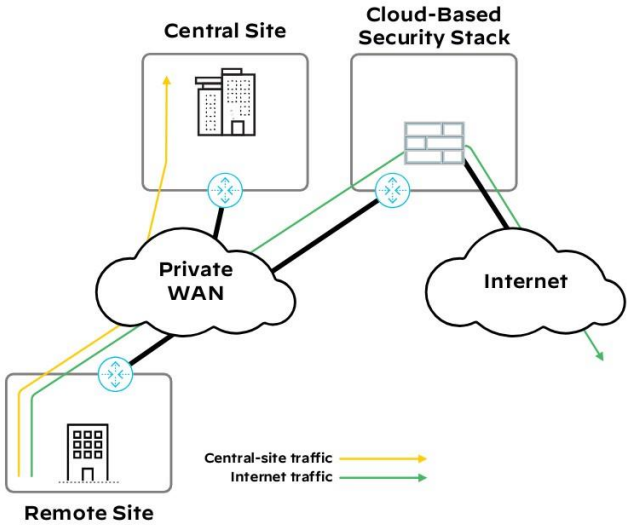


Рис. 2.8 Хмарне Інтернет-підключення, надане клієнтом.

Прямий доступ до Інтернету

Інтернет-трафік, що базується на додатках, надсилається безпосередньо до точки призначення без перетину приватної WAN. Кожна віддалена локація забезпечує місцевий безпечний доступ до Інтернету через власну інфраструктуру безпеки. Такий варіант є витратним з точки зору мережевої безпеки та управління, особливо зі збільшенням кількості віддалених об’єктів. Проте він ефективно використовує пропускну спроможність центрального об’єкта, оскільки вона

застосовується лише для відповідного трафіку. Затримки не впливають на взаємодію користувача при доступі до регіональних ресурсів, незалежно від відстані до центрального місця (рис. 2.9).

Основні причини застосування прямого доступу до Інтернету (DIA) обумовлені вартістю. Компанії нерідко вирішують реалізувати інше рішення щодо безпеки, ніж на центральному об’єкті, або реалізувати лише обмежений набір функцій, що призводить до збільшення ризику для організації. Однак рекомендація Palo Alto Networks полягає в забезпеченні послідовної видимості за допомогою комплексного захисту брандмауера наступного покоління.

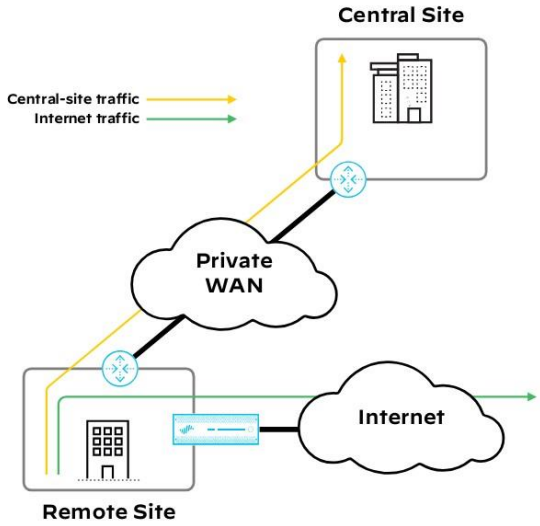


Рис. 2.9 Прямий доступ до Інтернету.

Довірений прямий доступ до Інтернету

Трафік, що базується на додатках для довірених місць розташування та програм SaaS, подорожує безпосередньо до точки призначення без перетину WAN. Організація сама визначає, які програми є довіреними, наприклад, Office 365, G Suite або Box. Кожен віддалений об’єкт надає місцевий безпечний доступ для довіреного інтернет-трафіку через власну інфраструктуру безпеки. Увесь інший інтернет-трафік пересилається на центральний об’єкт через приватну WAN для безпечного доступу до Інтернету, використовуючи ту ж інфраструктуру безпеки. Цей метод забезпечує доступ з низькою затримкою до довірених ресурсів і зменшує загальний обсяг трафіку на центральний об’єкт (рис. 2.10).

Випадок, коли кожен віддалений об’єкт надає місцевий безпечний доступ до довірених місць та програм з власною інфраструктурою безпеки, ґрунтується на інфраструктурі безпеки для належної ідентифікації, класифікації цих місць і програм, а також застосування будь-яких додаткових політик на основі користувачів.

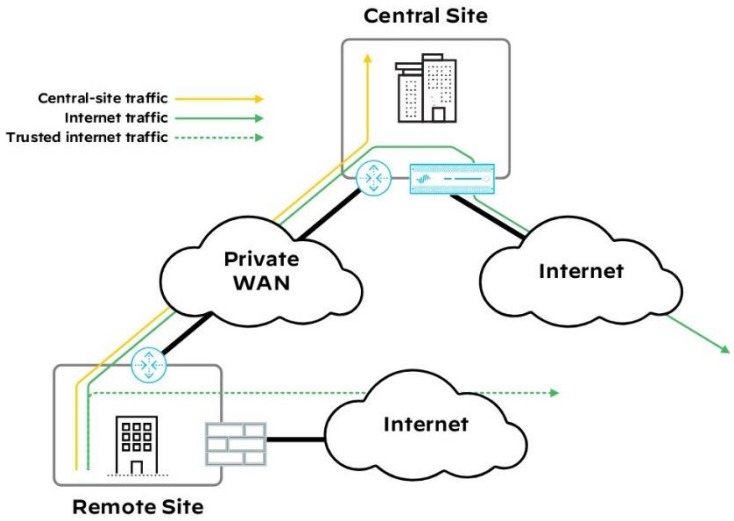


Рис. 2.10 Довірений прямий доступ до Інтернету.

Головною причиною для такого варіанту є вартість, і через це компанії доволі часто застосовують інакше від центрального рішення безпеки на віддаленому об’єкті або встановлюють лише обмежений набір функцій, наприклад, які надаються платформою UTM. Це рішення може здатися більш прийнятним через довіру до обраних додатків, однак все ще може збільшити ризик для організації. Навіть з довіреними додатками ризик потенційної загрози залишається: хакери можуть компрометувати додатки і перетворити їх на платформи для поширення шкідливих програм.

Ключовим принципом архітектури Zero Trust є "ніколи не довіряйте, завжди перевіряйте". Найефективніший спосіб перевірки – інспектування та реєстрація всього трафіку.

2.3 Secure Access Service Edge (SASE)

Коли підприємство розвивається, а технологія змінює місце розташування додатків і спосіб, яким клієнти та співробітники до них звертаються, мережам також необхідно еволюціонувати, щоб підтримувати ці зміни. Цифрова трансформація покращує гнучкість та здатність конкурувати, проте вона також викликає питання щодо того, як з’єднатися з даними та захистити їх на місці або в хмарі. Нова концепція, що здатна описати таке злиття технологій, необхідних для захисту мереж для організацій, – це Secure Access Service Edge (SASE).

SASE описує категорію сервісів та продуктів, що пропонують транспорт та безпеку в об'єднаному хмарно-орієнтованому та керованому рішенні. Основні сервіси включають: WAN edge/SD-WAN, безпечний веб-шлюз, Cloud Access Security Broker (CASB), доступ безпеки мережі Zero Trust, безпеку DNS та брандмауер як сервіс. Елементи в мережі, яка підтримує SASE, включають:

- Об'єднаний WAN edge та безпека мережі забезпечує справжню інтеграцію сервісів з об'єднаними сервісами і видимістю для всіх місць, мобільних користувачів та хмари, а не послідовні ланцюги.
- Хмарно-орієнтована доставка використовує багато точок присутності для зменшення затримки з підтримкою ресурсів у країні або регіоні та регуляторних вимог.
- Підтримка широкого краю мережі – це більше, ніж підтримки доступу на основі коробок, що надає можливість керування хмарним сервісом на основі агентів.
- Ідентифікація та мережеве місцезнаходження забезпечує виконання політики поза IP-адресою за допомогою ідентифікації з реальними умовами, такими як тип пристрою, стан та місцезнаходження.

Перехід до SASE змушує існуючі моделі мереж та безпеки еволюціонувати до інтегрованих, хмарно-доставлених сервісів. Prisma Access надає послугу,

сумісну з SASE, з понад 100 місцями та можливістю повної міграції WAN і сервісів безпеки до архітектури хмарного типу.

2.4 Опції SD-WAN

При впровадженні технології SD-WAN для заміни традиційної WAN, організації включають доступ до Інтернету з віддалених місць як ключовий аспект дизайну. У цьому розділі будуть порівнюватися варіанти дизайну для SD-WAN з DIA.

Автономний SD-WAN з прямим доступом до Інтернету

Віддалений об’єкт підключається до SD-WAN за допомогою відповідного пристрою. Весь трафік додатків центрального місця прямує до точки призначення за допомогою SD-WAN, який забезпечує найбільш оптимальний вибір шляху. Весь трафік додатків, що базуються на Інтернеті, прямує до точки призначення без проходження через SD-WAN і натомість переадресовується на публічну мережу через пристрій SD-WAN (рис. 2.11).

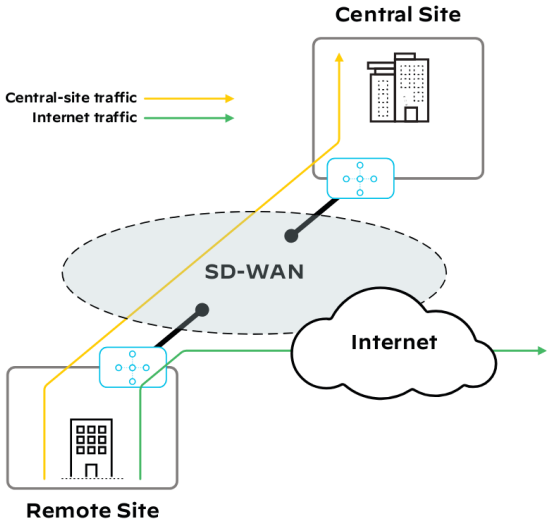


Рис. 2.11 Автономний SD-WAN з прямим доступом до Інтернету.

Кожен віддалений об’єкт надає локальний безпечний доступ до Інтернету, використовуючи лише вбудовані функції безпеки автономного пристрою SD-WAN. На віддаленому об’єкті не розташовані додаткові ресурси з безпеки, що зменшує витрати та спрощує управління. Цей варіант ефективно використовує пропускну здатність центрального об’єкта, оскільки пропускний потік від віддаленого до центрального через SD-WAN споживає пропускну здатність. Затримка між віддаленим місцем і центральним не впливає на користувачів при доступі до регіональних ресурсів, незалежно від відстані.

Можливості надання безпеки пристроїв SD-WAN зазвичай не еквівалентні до комплексного захисту брандмауера наступного покоління. Справа в тому, що автономний пристрій SD-WAN може реалізовувати лише обмежений набір функцій, в результаті чого ризик для організації росте.

SD-WAN з присвяченою безпекою DIA

Цей варіант схожий на попередній, проте тут кожен віддалений об’єкт надає локальний безпечний доступ до Інтернету, використовуючи комплексний захист брандмауера наступного покоління, розгорнутого в лінію з пристроєм SD-WAN (рис. 2.12).

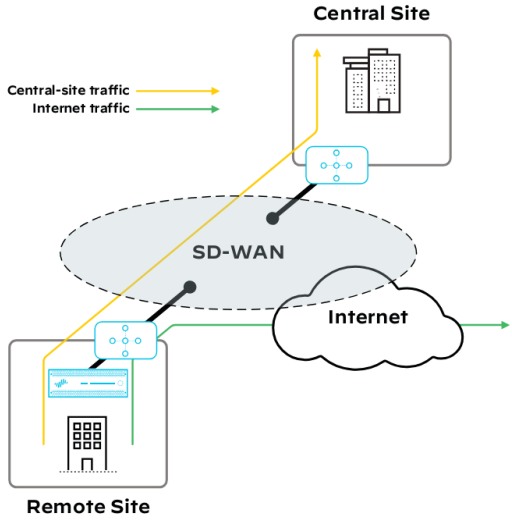


Рис. 2.12 SD-WAN з присвяченою безпекою.

Наступне покоління брандмауера забезпечує повний огляд користувачів, додатків і контенту, що перетинає корпоративні мережі, хмару і кінцеві точки. З цим оглядом можна впровадити політику безпеки та вживати заходів. Брандмауер наступного покоління також використовується для зменшення площини атаки на віддаленому об’єкті за допомогою сегментації. Вона розділяє мережі на керовані, безпечні частини, аби зменшити обсяг вимог і стандартів та обмежити витік даних.

Як і попередній, цей варіант продовжує ефективно використовувати пропускну здатність центрального об’єкта, оскільки лише відповідний йому трафік споживає її. Затримка від віддаленого об’єкта до центрального так само не впливає на користувацький досвід при доступі до регіональних ресурсів, незалежно від відстані. Однак у цьому варіанті існують додаткові ресурси безпеки, розташовані на віддаленому об’єкті. Також варто зазначити, що вимога керувати пристроєм SD-WAN і пристроєм безпеки окремо підвищує витрати і ускладнює керування віддаленим об’єктом.

Брандмауер нового покоління SD-WAN з прямим доступом до Інтернету

Цей варіант схожий на попередній, але не вимагає наявності пристрою SD-WAN. Тут брандмауер нового покоління вже надає можливості SD-WAN, і, крім того, забезпечує комплексний захист. Функції SD-WAN на брандмауері нового покоління використовують існуючі розширені засоби безпеки, такі як App-ID, щоб забезпечити інтелектуальний вибір шляху для кожного додатку (рис. 2.13). Крім того, брандмауер інтегрує функції моніторингу стану маршруту та автоматичного перемикання шляхів у разі виявлення проблем з продуктивністю, забезпечуючи надійність і високу якість обслуговування.

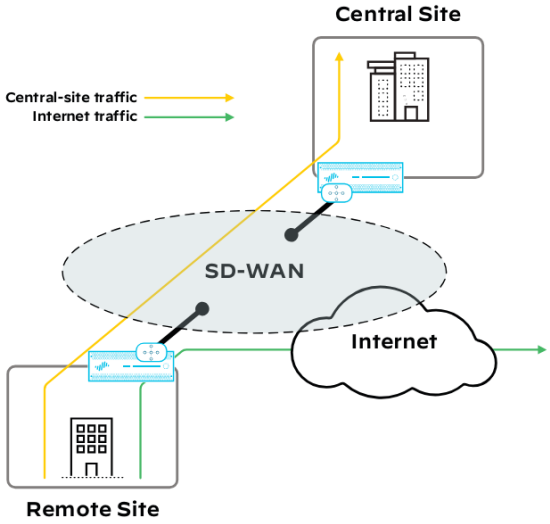


Рис. 2.13 Брандмауер нового покоління SD-WAN.

Next-generation firewall забезпечує повну видимість користувачів, додатків та контенту, які проходять корпоративні мережі, хмари та кінцеві точки. Також цей файрвол можна використовувати для зменшення всіх можливих шляхів, якими зловмисники можуть намагатися проникнути в систему або мережу, на віддаленому об’єкті за допомогою сегментації.

Як і обидва попередні варіанти, цей продовжує ефективно використовувати пропускну спроможність центрального об’єкта, оскільки призначений для нього трафік через SD-WAN споживає пропускну спроможність. Затримки не впливають на використання користувачем регіональних ресурсів, незалежно від відстані. Однак у цьому варіанті існує лише один пристрій на віддаленому місці, який надає функції безпеки та SD-WAN, зменшує витрати і спрощує управління.

Автономний SD-WAN з доступом до Prisma Access DIA

З цим варіантом віддалений об’єкт підключається до Prisma Access за допомогою тунелю IPSec від автономного SD-WAN пристрою. Цей тунель використовується для транспортування всього інтернет-трафіку до Prisma Access. Весь трафік додатків центрального об’єкта подорожує до місця призначення

додатка за допомогою SD-WAN, яке забезпечує оптимальний вибір шляху (рис. 2.14).

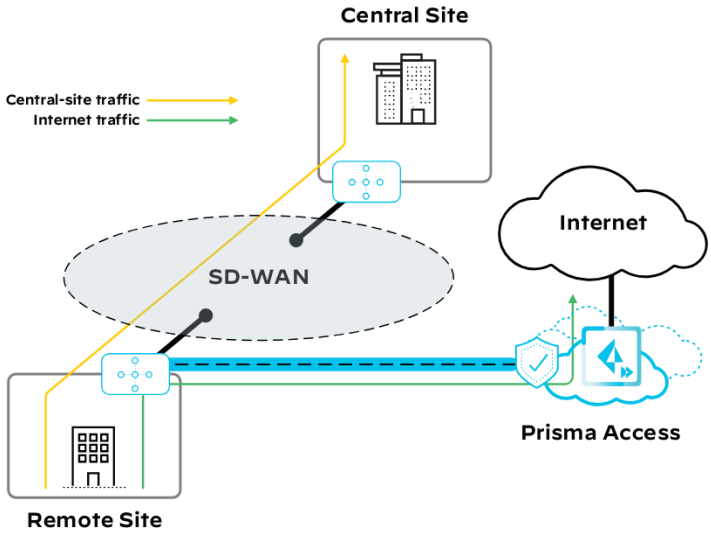


Рис. 2.14 Автономний SD-WAN з Prisma Access DIA.

Prisma Access для мереж надає сервіси безпеки App-ID та запобігання загрозам для віддаленої мережі, дозволяючи безпечне використання поширених додатків та захищений доступ до веб-сайтів. Отже Prisma Access надає прямий доступ до інтернету, без потреби повертати трафік до центрального об’єкта, та точно таку ж безпеку, видимість та контроль, як і next-generation firewall.

3 ДЕТАЛІ ДИЗАЙНУ PALO ALTO NETWORKS

Версія PAN-OS 9.1 вводить ряд нових функцій SD-WAN, що включені до підписки на SD-WAN. Цей розділ надасть докладний огляд можливостей SD-WAN брандмауера нового покоління, а також розгляне дизайнерські аспекти, пов'язані з цими можливостями.

Функції хаба або філії SD-WAN можна налаштувати на пристроях після додавання підписки SD-WAN на будь-який брандмауер нового покоління або модель VM-Series, вказаних у таблиці 3.1 і 3.2. Ці таблиці показують рекомендовану роль філії або хаба для кожної моделі пристрою, проте можна використовувати будь-яку модель пристрою у бажаній ролі, якщо вона відповідає вимогам продуктивності для місця розташування. Для останніх технічних характеристик платформи і продуктивності див. технічний опис SD-WAN.

Табл. 3.1 Характеристики пристрою віддаленого вузла (філії) SD-WAN.

	PA-220/ PA-220R	PA-820	PA-850	PA-3220	PA-3250	PA-3260
Загальна пропускна здатність WAN (рекомендований діапазон)	1-150 Mbps	50-500 Mbps	50-700 Mbps	500-2000 Mbps	1000-3100 Mbps	2000-5000 Mbps
Максимальна кількість тунелів IPSec	1000	1000	1000	2000	3000	3000
Максимальна кількість одночасних сеансів	64,000	128,000	196,000	1,000,000	2,000,000	3,000,000
Максимальна кількість маршрутів IPv4	2500	10,000	10,000	28,000	88,000	88,000

Табл. 3.2 Характеристики пристрою центрального вузла (хаба) SD-WAN.

	PA-5220	PA-5250	PA-5260	VM-300	VM-500
Загальна пропускна здатність IPSec	8 Gbps	16 Gbps	24 Gbps	1.8 Gbps	4 Gbps
Максимальна кількість тунелів IPSec	3000	4000	5000	1000	1000
Максимальна кількість одночасних сеансів	4,000,000	8,000,000	32,000,000	819,200	2,000,000
Максимальна кількість маршрутів IPv4	200,000	200,000	200,000	2000	4000

Додаткові функції мережевого роутера для розпізнаваних застосунків доповнюються функціями маршрутизації з урахуванням додатків в мережах SD-WAN. Підхід до використання SD-WAN і безпеки на інтегрованому віддаленому пристрої веде до більш ефективного управління мережею та безпекою, з меншою ймовірністю помилок у порівнянні з підходом, коли використовуються різні пристрої.

Для забезпечення конфіденційності даних файрволи наступного покоління використовують протокол IPSec для створення тунелів WAN із сильним шифруванням. Вони також розширюють використання декодування в рамках App-ID для швидкого та точного визначення застосунків через WAN. Нові можливості для SD-WAN включають моніторинг стану маршруту за ключовими метриками, такими як затримка, джитер і втрати, а також політики для вибору маршруту та розподілу трафіку для кожного застосунку.

3.1 Нові конструкції для PAN-OS Secure SD-WAN

PAN-OS 9.1 додає кілька нових конструкцій, які необхідні для активації SD-WAN на пристроях:

- Профіль інтерфейсу SD-WAN.
- Віртуальні інтерфейси SD-WAN.

- Профілі якості шляху SD-WAN.
- Профілі розподілу трафіку SD-WAN.
- Правила політики трафіку SD-WAN.

Профіль інтерфейсу SD-WAN

Профіль інтерфейсу SD-WAN визначає тип зв'язку, мітку зв'язку, швидкість завантаження/вивантаження пропускної здатності зв'язку та який моніторинг шляху для зв'язку краще обрати. Після активації SD-WAN для інтерфейсу слід пов'язати профіль з самим інтерфейсом.

Для вибору порядку шляху використовується мітка зв'язку в профілі розподілу трафіку. Мітки зв'язку також групують кілька інтерфейсів для розподілу навантаження сесії або зв’язку в пакеті. Якщо кілька інтерфейсів мають профілі інтерфейсу SD-WAN з тією ж міткою зв'язку, вони логічно об'єднуються для розподілу трафіку.

Плагін Panorama SD-WAN використовує інформацію про тип зв'язку, щоб визначити, які піри (peers) вузлів пристроїв використовуються для покриття мережі зв'язку. Якщо інтерфейс пристрою підключений до будь-якого типу публічного зв'язку (ADSL/DSL, кабельний модем, Ethernet, оптичний волоконний зв'язок, LTE/4G або WiFi), то плагін SD-WAN налаштовує його на підключення до мережі покриття для відповідного типу зв'язку. Якщо пристрій має кілька інтерфейсів з однаковим класом зв'язку, кожен інтерфейс має підключення до мережі покриття.

Мережа покриття складається з точкових тунелів IPSec. Центральні пристрої SD-WAN у вузлах використовують пасивну конфігурацію для тунелів IPSec і не ініціюють з'єднання. Гілкові пристрої SD-WAN на віддалених місцях використовують динамічну конфігурацію пірів для тунелів IPSec до центральних.

Версія програмного забезпечення PAN-OS 9.1 підтримує лише топологію типу "центральний вузол – розгалужені вузли" (hub-and-spoke) для оверлейної мережі. Також підтримується використання кількох центральних вузлів.

Під час вибору типу лінку, метод моніторингу шляху за замовчуванням обирається автоматично. Моніторинг шляху використовується для оцінки стану на основі метрик затримки, втрат і джитера, які обчислюються на основі даних, зібраних з проб трафіку. Моніторинг передбачає, що пристрій Palo Alto Networks SD-WAN завершує IPSec-тунелі на обох кінцях з'єднання.

Коли пристрій налаштований на агресивний режим, він відсилає пакети проб із частотою 5 пакетів на секунду постійно. В розслабленому режимі пристрій відсилає пакети проб з частотою 5 пакетів на секунду протягом 7 секунд, після чого робить паузу на 60 секунд перед відновленням. Метод моніторингу шляху можна перевизначити. Агресивний режим швидко виявляє погіршені шляхи, але споживає більше пропускної здатності. Розслаблений режим споживає менше пропускної здатності, але потребує більше часу для виявлення погіршеного шляху. Частоту відсилання проб можна налаштувати для обох режимів, а період очікування – лише для розслабленого.

Якщо потрібно змінити стандартні частоти зондування, слід налаштувати пороги втрат пакетів, які розраховуються на основі частоти зондування. Зменшення частоти може затримати виявлення втрат, тому важливо відповідно зменшити поріг втрат пакетів, щоб підвищити ймовірність виявлення втрат. Наприклад, при стандартній частоті зондування 5 зондів/с і порозі втрат 5%, зменшивши частоту зондування до 2 зондів/с, потрібно зменшити поріг втрат до 2%.

Однією з основних переваг SD-WAN є можливість переміщувати потоки трафіку з пошкоджених шляхів на кращі через пристрої. В ідеалі, коли деградований шлях відновлюється, пристрій має відновлювати й потоки на нього. Щоб уникнути ризику мимовільного перемикання маршрутів (path flapping – коли трафік постійно переміщується з одного шляху на інший), пристрій SD-WAN застосовує час очікування відновлення. Таймер очікування переконується, що шлях залишався здоровим протягом 120 секунд, перш ніж SD-WAN пристрої відновлюють потоки на нього. Час очікування можна налаштувати самостійно.

Зазвичай Palo Alto Networks рекомендує використовувати унікальний профіль інтерфейсу SD-WAN та мітку зв'язку для кожного фізичного інтерфейсу. Цей підхід дає найбільшу кількість деталей для створення політик SD-WAN. Проте, якщо є набір функціонально еквівалентних фізичних інтерфейсів, можна використовувати одну мітку зв'язку для всього набору інтерфейсів. Цей підхід дозволяє симулювати зв'язок лінків і спрощує конфігурацію, необхідну для базового розподілу навантаження.

Віртуальний інтерфейс SD-WAN

Віртуальний інтерфейс SD-WAN (VIF) можна налаштувати для включення фізичних інтерфейсів з підтримкою SD-WAN та інтерфейсів тунелів IPSec як членів групи. Всі вони повинні бути одного типу (рис. 3.1).

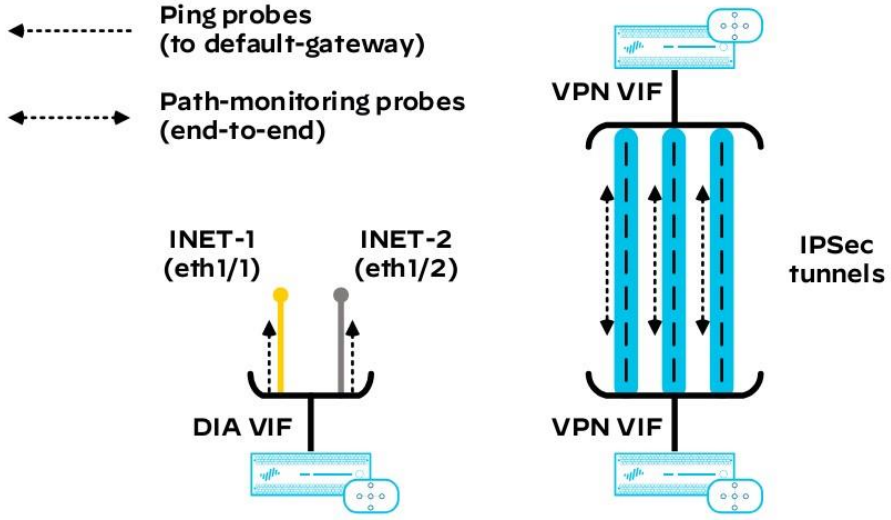


Рис. 3.1 Віртуальний інтерфейс SD-WAN.

VIF виконує кілька ключових функцій на пристрої SD-WAN:

- Надає віртуальний інтерфейс 3-го рівня для використання як призначеного інтерфейсу таблиці маршрутизації IP та відокремлює фізичні або тунельні інтерфейси від рішень маршрутизації IP на тому ж рівні.
- Генерує проби моніторингу шляху для кожного члена групи.

- Дозволяє фізичним членам групи інтерфейсів підтримувати специфічний для інтерфейсу основний шлюз без потреби у спеціальному записі в таблиці маршрутизації IP.
- Виконує інтелектуальний розподіл трафіку між інтерфейсами членів групи, залежно від профілю розподілу трафіку.

У більшості випадків плагін Panorama SD-WAN автоматично створює SD-WAN VIF.

На всіх пристроях SD-WAN плагін створює один VIF, що включає фізичні інтерфейси як члени групи. Цей VIF зазвичай використовується для прямого доступу до Інтернету (DIA) і часто називається DIA VIF. Плагін також створює статичний маршрут за замовчуванням з цим VIF як призначенням, використовуючи маршрутну метрику 5. Кожен з фізичних інтерфейсів-членів групи повинен мати власний шлюз за замовчуванням, який або статично налаштовується, або призначається як опція DHCP (табл. 3.3).

Табл. 3.3 VIF, створені плагіном SD-WAN.

	Конфігурація DIA VIF	**Конфігурація VPN VIF**
Центральний об’єкт	Один VIF для прямого доступу до Інтернету (DIA), який включає всі фізичні інтерфейси, увімкнені для SD-WAN, як члени групи	Один VIF VPN для кожного віддаленого об’єкта. Кожен включає всі IPSec-тунелі до певного віддаленого місця як члени групи
Віддалений об’єкт	Один VIF для прямого доступу до Інтернету (DIA), який включає всі фізичні інтерфейси, увімкнені для SD-WAN, як члени групи	Один VIF VPN для кожного центрального об’єкта. Кожен включає всі IPSec-тунелі до певного центрального місця як члени групи

Плагін SD-WAN автоматично включає приватні інтерфейси, такі як MPLS, як членів групи DIA VIF. Тоді необхідно виключити приватні інтерфейси з профілю розподілу трафіку SD-WAN для DIA.

Іноді потрібно вручну створити VIF з фізичними інтерфейсами як членами групи перед завершенням конфігурації SD-WAN за допомогою плагіна Panorama SD-WAN. У цих випадках, при налаштуванні статичного маршруту за

замовчуванням з вручну створеним VIF як інтерфейсом призначення, використовується маршрутна метрика більше 5, аби цей маршрут був менш затребуваний порівняно зі статичним маршрутом за замовчуванням, створеним плагіном.

DIA VIF, як і інші VIF, виконує моніторинг шляхів, але не має явного піра для зондування. Коли створюється DIA VIF, він відправляє ping-зонди до шлюзів за замовчуванням для кожного інтерфейсу. Принаймні один зі шлюзів за замовчуванням повинен відповісти, а якщо ні, DIA VIF буде вважатися відключеним. Пристрої SD-WAN не збирають жодних метрик продуктивності з ping-зондів.

Варто перевірити, щоб шлюзи за замовчуванням для фізичних інтерфейсів відповідали на ICMP echo запити. Якщо цього не сталось, DIA VIF позначає фізичний інтерфейс як DOWN і не використовує його для пересилання трафіку.

На центральних SD-WAN хаб-пристроях плагін створює VPN VIF для кожного віддаленого місця з IPSec тунелями, що підключаються як члени групи для VIF. На віддалених SD-WAN пристроях плагін створює відповідно VPN VIF для кожного центрального об’єкта з IPSec тунелями, що так само підключаються як члени групи для VIF. Кожен IPSec тунель для VPN VIF вважається потенційним шляхом до місця-призначення.

VPN VIF виконують моніторинг шляхів, відправляючи зонди моніторингу шляхів через тунель. Вони відправляються через кожен активний IPSec тунель до віддаленого піра. Пристрої SD-WAN збирають дані зондів моніторингу шляхів, використовуваних для розрахунку метрик продуктивності шляху.

Після того, як IPSec тунель для VPN VIF переходить у стан UP і моніторинг шляху активний, DIA VIF призупиняє моніторинг шляху через ping. Кожен фізичний інтерфейс-член групи в VIF успадковує стан моніторингу шляху IPSec тунелю, який виходить з цього інтерфейсу. Якщо з інтерфейсу виходить декілька тунелів, для стану моніторингу шляху фізичний інтерфейс-член групи використовує середнє значення всіх тунелів.

Пристрій SD-WAN використовує VIF для спрощення IP-маршрутизації. За відсутності VIF, коли на пристрої є кілька шляхів до пункту призначення, віртуальний маршрутизатор має кілька записів у таблиці маршрутизації. Найкращий шлях встановлюється в таблицю пересилання, або при ввімкненні ECMP маршрутизатор виконує розподіл навантаження по шляхах, встановлюючи кілька маршрутів у таблицю пересилання. Метод розподілу навантаження можна обрати, але слід враховувати, що жоден з них не використовує метрики продуктивності в реальному часі, які пропонує SD-WAN.

При використанні VIF віртуальний маршрутизатор потребує лише одного запису в таблицях маршрутизації і пересилання. Після того, як трафік пересилається на VIF, він визначає, яким шляхом йти на основі політики SD-WAN, профілю розподілу трафіку та умов в реальному часі кожного шляху. VIF може додавати активні членські інтерфейси, коли їх стан змінюється на UP, і видаляти неактивні, коли їх стан змінюється на DOWN. При цьому віртуальний маршрутизатор не зазнає змін у своїх таблицях маршрутизації і пересилання.

При використанні двох інтерфейсів з DHCP-адресами та серверами, що надають маршрутизатори за замовчуванням, існують два рівноцінні шляхи через різні інтерфейси. SD-WAN автоматично вирішує цю проблему. Якщо налаштувати пристрій SD-WAN так, щоб стандартний маршрут не був у таблиці маршрутизації, DIA VIF зберігає кожен шлюз інтерфейсів за замовчуванням. DIA VIF можна використовувати як інтерфейс призначення для маршруту за замовчуванням без зазначення IP-адреси наступного кроку для статичного маршруту. Після створення VPN VIF та активних тунелів, пристрої SD-WAN можуть застосовувати політики SD-WAN та вибирати найкращі шляхи для кожного додатка на основі поточних умов реального часу SD-WAN.

Профілі якості маршрутів SD-WAN

Кожен профіль якості маршрутів SD-WAN (Path-Quality profile – PQP) складається з набору впорядкованих метрик і порогів, потрібних для оптимальної

продуктивності додатка. Зазвичай використовується унікальний PQP для кожного набору критичних для бізнесу і чутливих до затримок додатків. PQP є одним із ключових компонентів під час вибору маршруту SD-WAN.

Моніторингові проби маршрутів SD-WAN використовуються для обчислення метрик PQP для маршруту. Кожен IPSec тунель у VPN VIF вимірює та обчислює свої метрики незалежно.

Метрики, які використовує кожен PQP:

- Затримка – час затримки у двох напрямках для пакета даних, відправленого через тунель SD-WAN (вимірюється у мс). За замовчуванням вона обчислюється кожні 200 мс за допомогою рухомого вікна, що включає останні три вимірювання.
- Джитер – відхилення затримки в порівнянні з середньою затримкою для пакета даних, відправленого через тунель SD-WAN (вимірюється у мс). За замовчуванням обчислюється так само, як і затримка.
- Втрата пакетів – відсоток втрачених пакетів у порівнянні з загальною кількістю відправлених пакетів через тунель SD-WAN. Обчислюється кожні 200 мс за допомогою рухомого вікна, що включає останні 100 вимірювань.

Основна функція PQP полягає у визначенні кваліфікований (працює нормально) чи некваліфікований (працює у погіршеному режимі) шлях. Вторинна функція полягає у визначенні, який шлях використовувати, коли декілька з них є кваліфікованими, і чи вважаються вони еквівалентними за алгоритмом вибору шляху.

Поріг для кожної метрики вважається максимальним верхнім лімітом. Якщо пристрій SD-WAN вимірює значення будь-якої метрики PQP для шляху, і значення перевищує налаштований поріг, шлях вважається некваліфікованим. Це спричиняє вибір пристроєм альтернативного кваліфікованого шляху.

Якщо набір шляхів є кваліфікованими, алгоритм вибору шляху пристрою SD-WAN враховує чутливість метрик для визначення найкращого доступного шляху.

Можна вибрати одну з трьох налаштувань чутливості, щоб встановити важливість метрики: низьку, середню або високу. Якщо налаштувати якусь метрику на більшу чутливість, алгоритм вибору шляху спочатку враховує її. Якщо ж всі метрики мають однакове значення, алгоритм вибору шляху спочатку враховує втрату пакетів, потім затримку, а потім джитер.

Профілі розподілу трафіку SD-WAN

Правило політики SD-WAN визначає критерії, використовувані алгоритмом вибору шляху SD-WAN. Кожне правило політики включає PQP і профіль розподілу трафіку (Traffic Distribution Profile – TDP), що одночасно оцінюються для визначення шляху для додатка.

При налаштуванні TDP замість імен профілів інтерфейсу SD-WAN використовуються мітки ланцюжка. Якщо використовувати унікальні профілі та мітки для кожного фізичного інтерфейсу, мітка відповідатиме всім шляхам, що походять від цього інтерфейсу. Можна використовувати мітки для того, щоб розрізняти фізичні інтерфейси у політиці SD-WAN. Якщо використовувати спільну мітку ланцюжка SD-WAN, призначену для кількох фізичних інтерфейсів, вона відповідатиме всім шляхам, що походять від будь-якого з фізичних інтерфейсів. У цьому випадку відрізнити фізичні інтерфейси у політиці SD-WAN неможливо.

SD-WAN TDP використовується як частина політики SD-WAN для визначення методу розподілу трафіку, що використовує алгоритм вибору шляху для додатка. Цей алгоритм використовує метрики шляху, пороги та чутливості, визначені в PQP. При налаштуванні TDP можна обрати один з наступних методів розподілу трафіку:

- Найкращий доступний шлях – цей метод розподілу трафіку вимагає створення списку дозволених міток ланцюжків. Алгоритм вибору шляху використовує виключно PQP для вибору найкращого шляху зі списку дозволених і відповідають міткам ланцюжків. Для вибору доступні лише кваліфіковані шляхи. Якщо таких декілька, алгоритм використовує

значення чутливості, призначені для метрик, щоб визначити пріоритет. Цей метод зазвичай обирається, коли вартість шляху не є фактором для додатка.

- Пріоритет зверху вниз – цей метод розподілу трафіку вимагає створення пріоритетного списку дозволених міток ланцюжків. Алгоритм вибору шляху обирає кваліфікований шлях, що відповідає мітці ланцюжка з найвищим пріоритетом. Цей метод зазвичай використовується, коли є значна різниця в вартості між шляхами. Низький пріоритет призначається шляхам з високою вартістю міток ланцюжків, щоб більш дорогі шляхи використовувалися лише коли шляхи з низькими вартостями некваліфіковані.
- Ваговий розподіл сеансів – цей метод розподілу трафіку вимагає створення списку дозволених міток ланцюжків і призначення відсоткової ваги кожному елементу в ньому. Загальний відсоток, виділений на всі мітки ланцюжків, повинен дорівнювати 100. При використанні цього методу алгоритм вибору шляху виконує розподіл сеансів по шляхам для кожної мітки ланцюжка, при умові, що шляхи не повинні бути кваліфіковані.

При налаштуванні кількох фізичних інтерфейсів з однаковим профілем інтерфейсу SD-WAN та міткою ланцюжка, необхідно скорегувати поведінку цих методів розподілу трафіку. Якщо алгоритм вибору шляху обирає спільну мітку ланцюжка, він розподіляє сесії рівномірно по всім шляхах. Крім поведінки різних методів розподілу трафіку, яка раніше обговорювалася, алгоритм вибору шляху також має нечітко визначену поведінку для наступних випадків:

- Кілька фізичних інтерфейсів з однією міткою ланцюжка SD-WAN.
- Відсутні кваліфіковані шляхи.
- Немає відповідного правила SD-WAN політики.
- Всі VIF відключені.

Правила політики SD-WAN

Правила політики SD-WAN схожі на правила політики безпеки, що значно спрощує конфігурацію. Обидва типи правил відповідають за джерело зони/адреси/користувача, призначення зони/адреси та додаток/службу. Однак правила безпеки оцінюються перед застосуванням політики SD-WAN. Якщо додаток дозволяється правилом безпеки, то політика SD-WAN обробляє його. Правила політики SD-WAN не обробляються для відхилені додатків або потоків.

Коли визначається, що додаток відповідає правилу політики SD-WAN, алгоритм вибору шляху оцінює кожний шлях з TDP і порівнює з реальними умовами шляху та порогами у PQP для визначення оптимального.

Palo Alto Networks SD-WAN автоматично вмикає функцію симетричного повернення (symmetric return), щоб уникнути асиметричних потоків трафіку. Потрібно налаштувати правило SD-WAN тільки на об’єкті, який ініціює з'єднання. Якщо з'єднання ініціюється з віддаленого до центрального об’єкта, а правило SD-WAN на віддаленому призначає потік шляхом SD-WAN, а центральний пристрій автоматично використовує той самий шлях для зворотного трафіку.

3.2 Керування розгортанням SD-WAN за допомогою Panorama

Використання Panorama для центрального керування політикою забезпечує актуальну конфігурацію брандмауера. Panorama спрощує конфігурацію політики через групи пристроїв та стек шаблонів. Брандмауери в одній групі отримують спільний набір правил. Panorama дозволяє керувати всіма брандмауерами, створюючи ієрархію конфігурації. Групи на нижчому рівні включають політику груп на вищому, що дозволяє налаштовувати однорідні набори правил для всіх брандмауерів і конкретних місць розгортання, таких як хмара.

Конфігурація SD-WAN спрощується за допомогою мінімум двох наборів шаблонів та груп пристроїв. Краще використовувати один набір для центральних пристроїв-хабів та другий для віддалених місць. Якщо віддалені місця згруповані у

кількох регіонах, можна розмістити пристрої віддалених місць у додаткових шаблонах та групах пристроїв.

Панорама та плагін SD-WAN

Крім традиційних можливостей Panorama, базованих на групах пристроїв та стеках шаблонів, плагін SD-WAN для Panorama також надає розширену конфігурацію, моніторинг та звітність для SD-WAN.

Після додавання центральних та віддалених пристроїв до Panorama та прив’язування їх до відповідних стеків шаблонів та груп пристроїв, конфігурацію пристроїв за допомогою плагіна SD-WAN для Panorama завершується.

При додаванні пристроїв до плагіна SD-WAN потрібно визначити тип вузла: центральний (hub) або віддалений (branch). Це визначає налаштування IPSec-пірів. Рекомендується ввімкнути динамічну маршрутизацію з BGP, надавши ідентифікатор маршрутизатора BGP, IPv4-адресу петлевого зворотного зв'язку та номер автономної системи BGP. На центральних вузлах потрібно також надати список IPv4-префіксів для оголошення BGP; на віддалених пристроях це не є обов'язковим.

Після додавання пристроїв та створення кластера VPN SD-WAN, конфігурація плагіна SD-WAN завершена. Кожен VPN-кластер є логічним об'єднанням центральних та віддалених пристроїв. Плагін SD-WAN використовує VPN-кластери як верхній рівень для моніторингу та звітності SD-WAN. Необхідно призначати кожен пристрій до кластера VPN. Якщо залишити його непризначеним, плагін SD-WAN не створить і не надішле конфігурацію SD-WAN.

Плагін SD-WAN спрощує та автоматизує кілька важливих завдань SD-WAN через процес, відомий як AutoVPN. Під час виконання плагіном SD-WAN AutoVPN виконуються наступні завдання:

- Створення попередньо визначених зон безпеки та необхідних інтерфейсів.
- Створення SD-WAN VIFs та конфігурація IPSec-тунелів.

- Конфігурація BGP та статичних маршрутів.

Плагін SD-WAN автоматично створює конфігурації AutoVPN щоразу, як до нього додаються нові пристрої. Palo Alto Networks не рекомендує виконувати локальні заміни елементів конфігурації, керовані плагіном SD-WAN.

Крім завдань конфігурації, перерахованих вище, плагін SD-WAN також надає централізовані можливості моніторингу та звітності для SD-WAN. Моніторингова панель надає статистику продуктивності додатків та лінків для SD-WAN VPN-кластерів на основі кожного місця.

Моніторинг продуктивності додатків включає список усіх спостережуваних додатків для кожного об’єкта, відповідність правил політики SD-WAN та міток лінків, статус здоров'я додатків та загальну кількість сеансів (посічених/загалом). Екран продуктивності додатків відображає додатки як “посічені” тільки коли пристрій SD-WAN не може визначити шлях, що відповідає визначеним пороговим значенням додатка в PQP.

Моніторинг продуктивності лінків включає список шляхів для кожного місця (IPSec тунель або фізичний інтерфейс), мітку лінка, тип, статус лінка та здоров'я шляху (затримка/відхилення/втрата пакетів). Можна вказати інтервал часу для панелі або налаштувати його для дослідження попередніх подій.

Збір логів за допомогою Panorama

Можливості моніторингу та звітності для SD-WAN вимагають збору та зберігання журналів трафіку за допомогою Panorama в одиночній або конфігурації на основі колектора журналів.

Можна використовувати один з двох варіантів режиму розгортання для Panorama, що дозволяє розділити функції управління та збору логів (рис. 3.2).

- Режим Panorama. Panorama керує як політикою, так і функціями управління логами для всіх пристроїв.

- Режим колектора журналів. Один або кілька Колекторів збирають і управляють журналами з керованих пристроїв. Це передбачає, що інше розгортання Panorama працює тільки в режимі Panorama або управління.

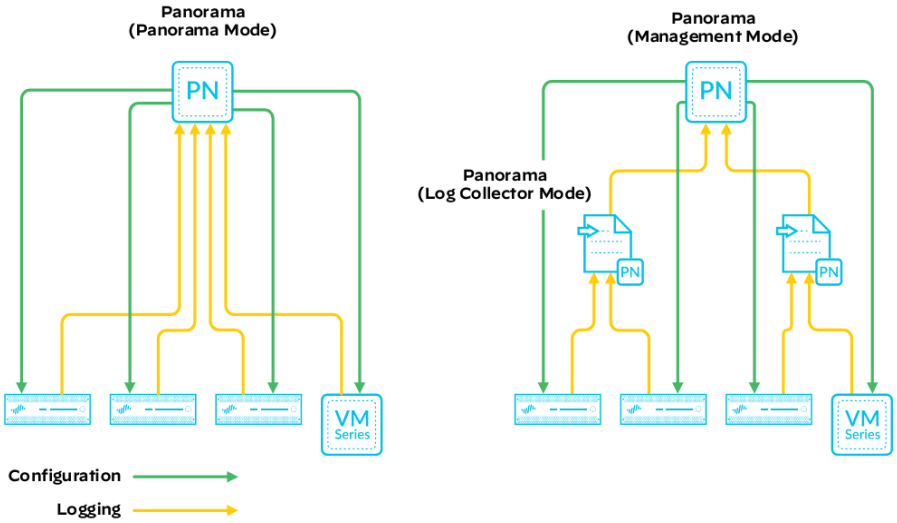


Рис. 3.2 Режими Panorama.

Розділення управління та збору логів дозволяє розгортанню Panorama відповідати вимогам щодо масштабованості, організаційних та географічних потреб.

Потрібно мати один або кілька управлінських колекторів логів (які можуть включати Panorama). На Panorama додається кожен колектор логів до групи колекторів. При додаванні нових SD-WAN пристроїв до Panorama потрібно призначати кожен пристрій до групи колекторів.

На SD-WAN пристроях необхідно надсилати логи конфігурації, системні та трафіку до Panorama, інакше екрани моніторингу SD-WAN на Panorama будуть неповними.

Для надсилання логів трафіку потрібно створити профіль пересилання і посилатися на нього в кожному з правил політики безпеки. Якщо цей профіль не увімкнути, то трафік, що відповідає цьому правилу політики безпеки, не буде моніторитися.

Керування пристроями

Всі пристрої SD-WAN керуються та моніторяться за допомогою Panorama та плагіна Panorama SD-WAN. За замовчуванням використовують інтерфейс управління пристрою для спілкування з Panorama, що підходить для місць з існуючим підключенням до Panorama. Альтернативний метод – використання інтерфейсу даних пристрою, що потребує додаткової конфігурації, але дозволяє керувати віддаленими місцями через WAN без існуючого підключення.

Якщо планується керування пристроями, використовуючи інтерфейси даних через публічну мережу, то потрібно призначити публічну IP-адресу для Panorama та кожного колектора логів.

Керування пристроями центрального об'єкта

Panorama зазвичай розгортається на центральному об'єкті для керування мережевими межами. Після підключення інтерфейсів управління до внутрішньої мережі додаткова конфігурація не потрібна. За замовчуванням інтерфейс управління використовується для взаємодії з Panorama та функцій керування (DNS, NTP, логування, оновлення). Слід також створити правила політики безпеки для контролю трафіку до Інтернету та дозволу хмарних застосунків площини керування (рис. 3.3).

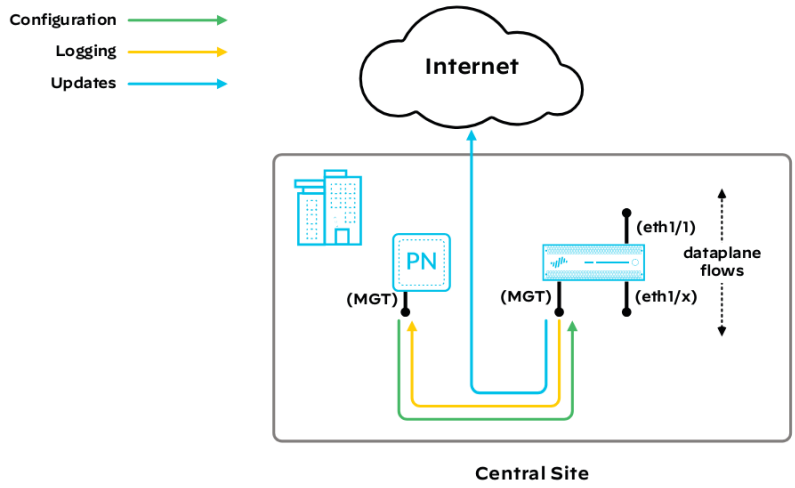


Рис. 3.3 Керування пристроями центрального об'єкта.

Якщо розгортається новий пристрій, можна домовитися про проведення початкової конфігурації пристрою на місці за допомогою технічного персоналу. Початкові завдання конфігурації потребують прямого підключення до пристрою SD-WAN. Після цього можна завершити залишкові завдання централізовано, використовуючи Panorama.

Керування пристроями на віддалених об'єктах

Керувати пристроєм на віддаленому об'єкті складніше ніж тим, що на центральному. Якщо є існуюча out-of-band (OOB) мережа, призначена для керування пристроями, то можна використовувати той самий підхід, про який йшлося раніше для пристроїв на центральних об'єктах (рис. 3.4).

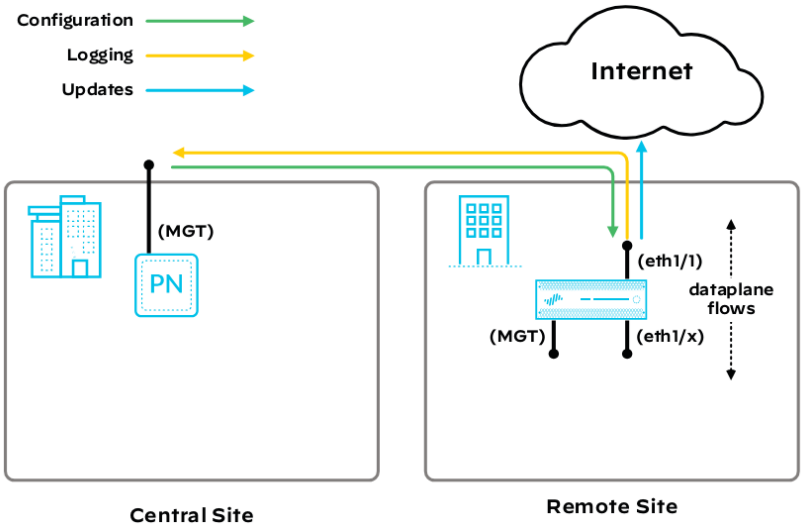


Рис. 3.4 Керування пристроями на віддалених об'єктах.

Для віддалених місць без OOB мережі управління доступні такі методи:

- Ручна конфігурація пристрою, виконана технічним персоналом на місці. Цей метод передбачає створення сервісних маршрутів, правил NAT та правил політики безпеки для пристрою. Після завершення основної конфігурації можна підключити пристрій до мережі, і він зініціює контакт з Panorama. Залишкові завдання дороблюються централізовано, використовуючи Panorama.

- Завантаження конфігурації через USB. Після створення та перевірки працюючої конфігурації віддаленого пристрою, можна використовувати її як базову конфігурацію для спрощення та автоматизації процесу.
- Централізоване вивантаження. Після створення та перевірки працюючої конфігурації віддаленого пристрою, персонал центрального об’єкта виконує конфігурації пристроїв SD-WAN для кожного віддаленого пристрою. Після завершення цього процесу пристрій повертається у віддалений об’єкт. Технічному персоналу на місці не потрібно виконувати жодної конфігурації, лише увімкнути пристрій та підключити його до мережі, аби ініціювати контакт з Panorama. Залишкові завдання виконуються централізовано, використовуючи Panorama, як і в минулому методі.

3.3 Зони безпеки

Кожен пристрій SD-WAN потребує конкретного набору зон безпеки. Деякі з них потрібно створити вручну, використовуючи шаблони Panorama. Плагін SD-WAN для Panorama використовує декілька зон, тому їх назви повинні точно відповідати. Необхідно створити всі зони заздалегідь, якщо є потреба посилатися на них у політиках безпеки та NAT в межах груп пристроїв Panorama. Якщо цього не зроблено, плагін SD-WAN створює будь-які потрібні зони, які ще не існують. Крім того, важливо переконатися, що всі правила політики та NAT правильно налаштовані для нових зон, щоб уникнути порушень безпеки або проблем з трафіком.

Центральний об’єкт

Як мінімум, кожний центральний об’єкт повинен включати зони, перелічені в таблиці 3.4. Рисунок 3.5 візуалізує ці зони і показує як вони взаємодіють між собою.

Табл. 3.4 Обов'язкові зони для центральних пристроїв SD-WAN.

Назва зони	Тип зони	Використання SD-WAN
zone-internal	Layer 3	Необхідно для петельних інтерфейсів пристрою, які використовуються для SD-WAN. Назва зони повинна точно відповідати.
zone-to-branch	Layer 3	Необхідно для тунелів SD-WAN та VPN VIF до віддалених місць. Назва зони повинна точно відповідати.
zone-public	Layer 3	Необхідно для інтерфейсів, що виходять в WAN та DIA VIF. Назву зони можна вибрати.
zone-private	Layer 3	Необхідно для інтерфейсів, що виходять в LAN на центральних місцях. Назву зони можна вибрати.

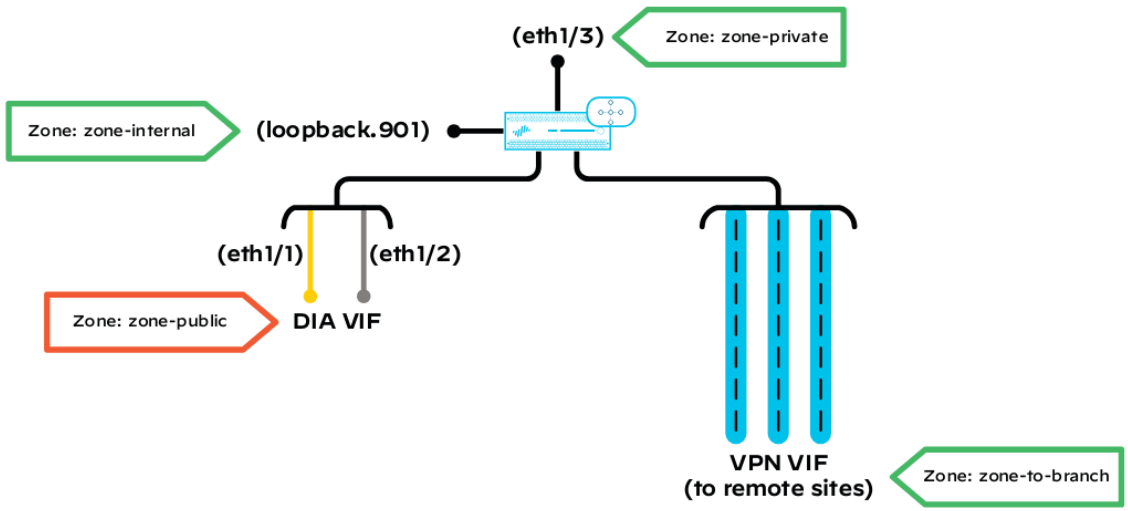


Рис. 3.5 Центральні зони безпеки об’єкта.

Віддалений об’єкт

Мінімальний набір зон для кожного віддаленого об’єкта повинен включати перераховані в таблиці 3.5. При необхідності можна використовувати додаткові приватні зони для сегментації на віддаленому місці. Рисунок 3.6 візуалізує як ці зони виглядають. Для кожної зони також слід налаштувати відповідні політики безпеки, щоб забезпечити належний рівень захисту та контролю трафіку. Це дозволить ефективно управляти мережевими ресурсами та зберегти дані на віддалених об’єктах.

Табл. 3.5 Обов'язкові зони для віддалених пристроїв SD-WAN.

Назва зони	Тип зони	Використання SD-WAN
zone-internal	Layer 3	Необхідно для петлевого інтерфейсу пристрою, який використовується для SD-WAN. Ім'я зони повинно точно відповідати.
zone-to-branch	Layer 3	Необхідно для тунелів SD-WAN та VPN VIF до центральних місць. Ім'я зони повинно точно відповідати.
zone-public	Layer 3	Вимагається для інтерфейсів, що виходять у світ та DIA VIF. Можна вибрати ім'я зони.
zone-private	Layer 3	Вимагається для інтерфейсів, що виходять у локальну мережу на віддалених об’єктах. Можна вибрати ім'я зони.

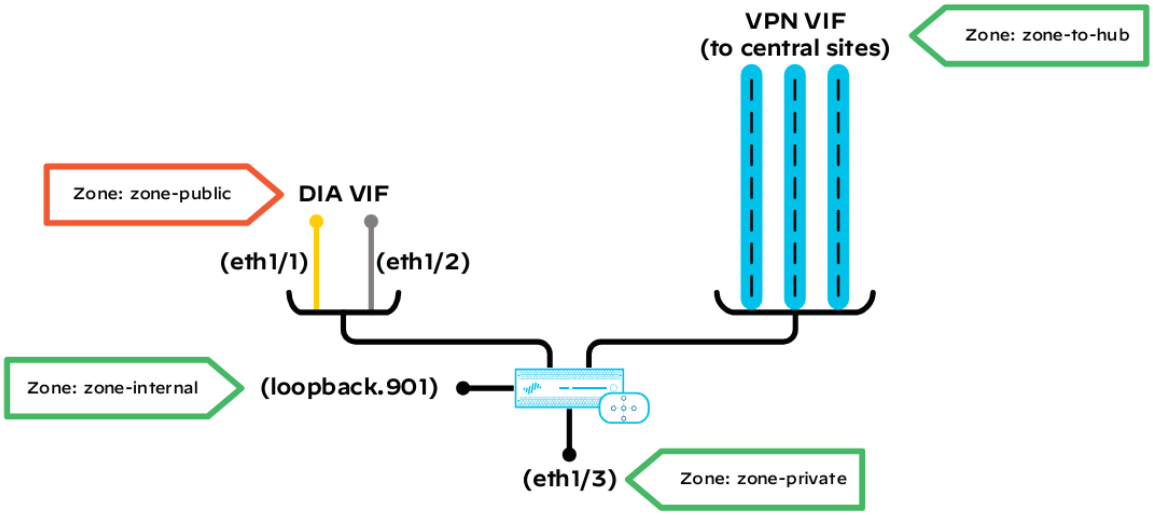


Рис. 3.6 Віддалені зони безпеки об’єкта.

3.4 Оверлей AutoVPN

Плагін SD-WAN для Panorama використовує інформацію про тип зв'язку для визначення, які пристрої-піри використовуються для оверлейної мережі. Якщо було вказано інтерфейс пристрою як підключений до будь-якого публічного типу зв'язку (ADSL/DSL, кабельний модем, Ethernet, оптичний кабель, LTE/4G або WiFi), то плагін SD-WAN конфігурує підключення до оверлейної мережі цього

типу зв'язку. Якщо у пристрою є кілька інтерфейсів з однаковим класом зв'язку, кожен інтерфейс має підключення до оверлейної мережі.

Під час виконання AutoVPN плагін SD-WAN створює оверлейну мережу між кожним набором пірів. На кожному пірі VPN VIF завершує оверлейну мережу, яка складається з набору тунелів до кожного піра. Кількість потрібних тунелів залежить від типів зв'язку SD-WAN інтерфейсів джерела тунелю. Плагін SD-WAN використовує клас зв'язку для типу зв'язку, вказаного в Таблиці 3.2, для визначення пірів тунелів.

Якщо є два WAN-з'єднання на кожному місці, одне публічне (ADSL/DSL), а інше приватне (MPLS), то плагін SD-WAN створює один тунель між публічними інтерфейсами та другий тунель між приватними. Плагін SD-WAN не створює тунелів між публічними та приватними інтерфейсами.

Плагін SD-WAN автоматично включає приватні інтерфейси, наприклад MPLS, як члени групи DIA VIF. Якщо приватна мережа не має шляху до Інтернету, треба виключити приватні інтерфейси з відправки трафіку DIA і використовувати їх для завершення тунелів. Варто налаштовувати профіль розподілу трафіку для DIA, що включає лише інтерфейси, підключені до публічних мереж.

Шлях SD-WAN відповідає тунелю всередині VPN VIF. Пристрої SD-WAN виконують моніторинг шляху для кожного шляху (рис. 3.7).

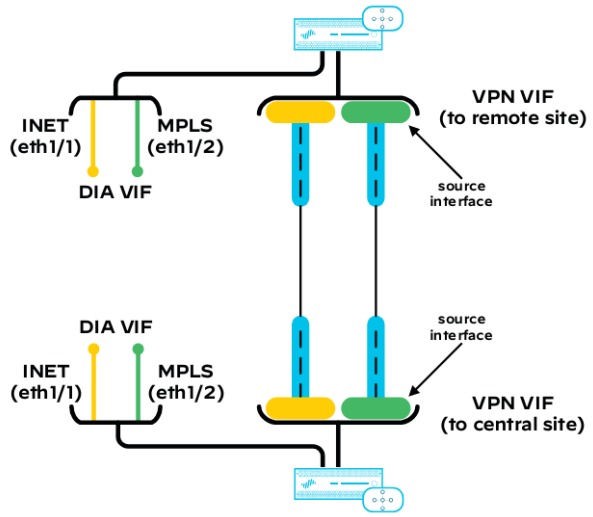


Рис. 3.7 AutoVPN (MPLS та Internet).

Якщо є два публічні WAN-з'єднання на кожному об’єкті (ADSL/DSL та кабельний модем), плагін SD-WAN створює повну сітку тунелів між публічними інтерфейсами (рис. 3.8).

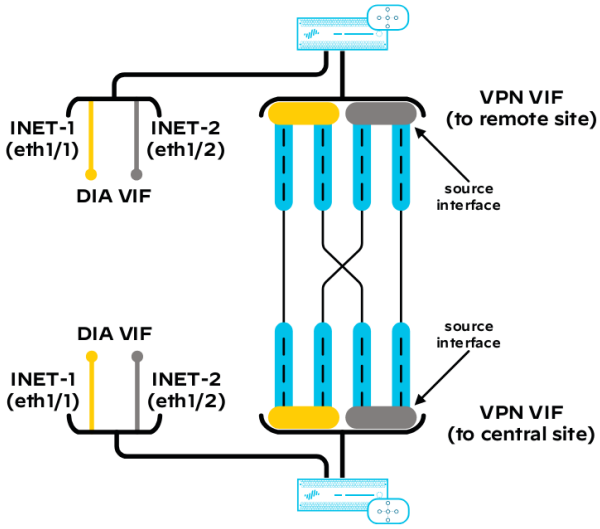


Рис. 3.8 AutoVPN (подвійний Інтернет).

Якщо є три WAN-з'єднання на кожному об’єкті: два публічних (ADSL/DSL і кабельний модем) і одне приватне (MPLS), плагін SD-WAN створює повну сітку тунелів між публічними інтерфейсами та один тунель між приватними. Плагін SD-WAN не створює тунелі між публічними та приватними інтерфейсами (рис. 3.9).

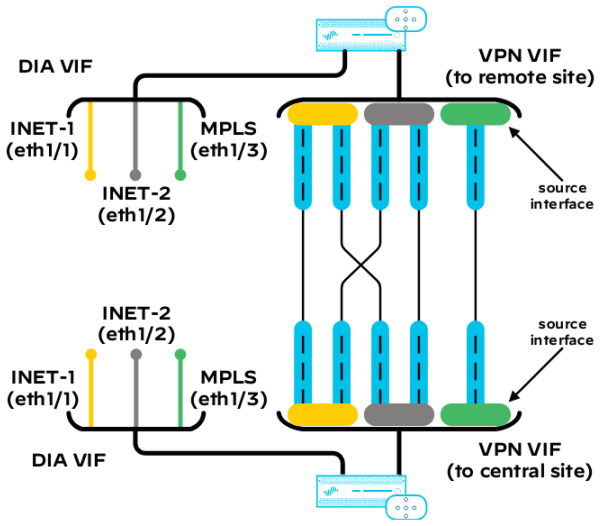


Рис. 3.9 SD-WAN (MPLS і подвійний Інтернет).

3.5 Маршрутизація SD-WAN

Маршрутизація трафіку до та від обладнання LAN рівня 3 на об’єктах не залежить від методу маршрутизації в мережі SD-WAN. Для забезпечення маршрутизації по мережі SD-WAN необхідно передавати інформацію про маршрутизацію з SD-WAN до обладнання LAN. Кожен вузол або об’єкт у мережі SD-WAN повинен також повідомляти інші вузли про свої маршрути, щоб забезпечити правильну маршрутизацію трафіку, враховуючи унікальні маршрути кожного місця.

Компанія Palo Alto Networks рекомендує використовувати послідовні блоки IP-маршрутів в організації, аби узагальнити IP-маршрути. Цей підхід спрощує конфігурацію маршрутизації для мережі SD-WAN.

Маршрутизація на центральних об’єктах

На центральних об’єктах налаштовується маршрутизація на обладнанні LAN рівня 3, щоб направляти трафік до віддалених об’єктів на LAN-інтерфейс пристрою SD-WAN. Можна використати статичну маршрутизацію, OSPF або BGP на обладнанні LAN. У разі статичної маршрутизації необхідно включити всі префікси віддалених об’єктів або узагальнені маршрути, що відповідають їх префіксам. При використанні BGP або OSPF потрібно налаштувати той же протокол на пристрої SD-WAN та створити профіль перерозподілу для віртуального роутера (на пристрої SD-WAN), включаючи префікси віддалених об’єктів або узагальнені маршрути. Пристрій SD-WAN потім оголошує вказані у профілі перерозподілу префікси на обладнання LAN.

На кожному центральному об’єкті також потрібно сконфігурувати маршрутизацію на пристрої SD-WAN, щоб відправляти призначений для об’єкта трафік на найближчий інтерфейс пристрою LAN рівня 3. Можна використовувати статичну маршрутизацію, OSPF або BGP на пристрої SD-WAN. В такому випадку потрібно включити або всі префікси центральних місць, або узагальнені маршрути,

що відповідають префіксам центральних. Якщо використовується BGP або OSPF, також потрібно сконфігурувати той же протокол на обладнанні LAN рівня 3 та оголосити префікси центральних об’єктів або узагальнені маршрути на пристрій SD-WAN.

Для оголошення префіксів об’єктів через мережу SD-WAN використовується BGP між пристроями SD-WAN. У рамках цього процесу AutoVPN з плагіном SD-WAN конфігурує список IPv4-префіксів для оголошення BGP. Цей список повинен включати префікси центральних об’єктів або узагальнені маршрути.

Маршрутизація на віддалених об’єктах

У багатьох організаціях віддалені місця є відносно невеликими і можуть мати лише кілька мережевих пристроїв. Загальна топологія мережі для віддаленого місця – це пристрій SD-WAN, підключений безпосередньо до комутатора LAN рівня 2. У такій топології пристрій SD-WAN відповідає за всю маршрутизацію на віддаленому об’єкті.

BGP використовується між пристроями SD-WAN для оголошення притаманних об’єкту префіксів по всій мережі SD-WAN. У рамках процесу AutoVPN з плагіном SD-WAN активується BGP на віддаленому місці. Процес AutoVPN автоматично налаштовує пристрій SD-WAN для перерозподілу прямо підключених маршрутів з його інтерфейсів, орієнтованих на LAN. Також можна сконфігурувати список IPv4-префіксів для оголошення BGP.

Маршрутизація між віддаленими об’єктами

Якщо необхідно включити маршрутизацію для трафіку між віддаленими місцями, потрібно це явно налаштувати. Конфігурація маршрутизації BGP, створена плагіном SD-WAN, оголошує префікси центрального об’єкта до всіх і префікси віддаленого до центральних. Якщо потрібно прокласти маршрут трафіку між віддаленими місцями, необхідно визначити центральний об’єкт як транзитний

і налаштувати його для оголошення одного або декількох зведених маршрутів на пристрої віддаленого місця (рис. 3.10).

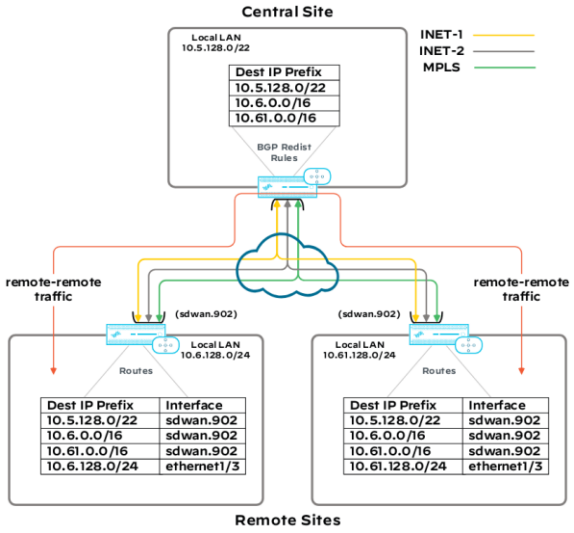


Рис. 3.10 Маршрутизація між віддаленими об’єктами.

3.6 Захист місць

Крім захисту користувацького трафіку, реалізація SD-WAN передбачає створення політик безпеки для підтримки функцій управління контрольним пакетом, таких як віддалене управління, DNS, NTP, протоколи маршрутизації та оновлення служб безпеки. Належно функціонуючий контрольний пакет необхідний для пристроїв SD-WAN, щоб забезпечити пересилання користувацького трафіку та забезпечити послідовну видимість та комплексний захист.

Політики контрольного пакета

Центральні пристрої SD-WAN використовують свої інтерфейси для віддаленого управління, DNS, NTP та оновлень служб безпеки. Однак потрібно створити правила політики безпеки для дозволу BGP від і до інших пристроїв SD-WAN.

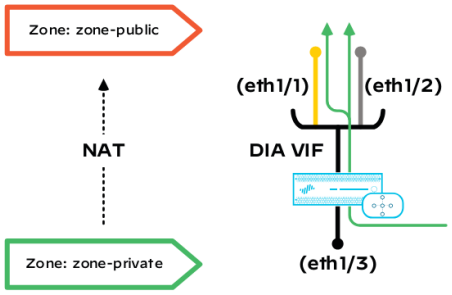
Пристрої SD-WAN налаштовуються на віддалених місцях для використання їхніх інтерфейсів даних для віддаленого управління, DNS, NTP та оновлень служб безпеки через маршрути обслуговування. Налаштування включає створення петлевого інтерфейсу для маршрутів обслуговування та правил політики NAT для кожного інтерфейсу даних WAN. Правила NAT перекладають IP-адреси петлевого інтерфейсу в IP-адреси інтерфейсів даних WAN. Також створюються правила політики безпеки для доступу до віддаленого управління, DNS, NTP та оновлень служб безпеки через зону zone-public.

Також потрібно створити правила політики безпеки для дозволу BGP від і до центральних пристроїв SD-WAN. Можна використовувати плагін SD-WAN , щоб автоматично згенерувати правила BGP для груп пристроїв SD-WAN, або створити правила BGP вручну за уподобаннями.

Політики DIA

Політики DIA необхідні лише на пристроях SD-WAN на віддалених місцях. Це передбачає, що доступ до Інтернету на центральних об’єктах не забезпечується через пристрої SD-WAN.

У рамках конфігурації DIA створюється набір правил політики NAT – по одному для кожного з інтерфейсів даних WAN. Кожне правило NAT перекладає трафік з зони zone-private в IP-адресу інтерфейсу даних WAN. Крім того, потрібно створити необхідні правила політики безпеки для дозволу доступу додаткам до зони zone-public (рис. 3.11).



Name	Original Packet			Translated Packet
	Source Zone	Destination Zone	Destination Interface	Source Translation
DIA-NAT-eth1_1	zone-private	zone-public	ethernet1/1	dynamic-ip-and-port ethernet1/1
DIA-NAT-eth1_2	zone-private	zone-public	ethernet1/2	dynamic-ip-and-port ethernet1/2

Рис. 3.11 Правила політики NAT для SD-WAN DIA.

Правила безпеки між об'єктами

Трафік між об'єктами SD-WAN потребує лише правил політики безпеки і не потребує жодних правил NAT. Однак, оскільки кожна сесія повинна проходити через кілька пристроїв SD-WAN, потрібно створити взаємодоповнюючі правила політики безпеки для кожного пристрою на шляху руху трафіку. Усі вони використовують тип правила Universal, за винятком наступних випадків:

- Трафік від центрального об'єкта до віддаленого. На центральному треба створити правила політики безпеки для дозволу трафіку додатків зі зони-private до зони-to-branch. На віддаленому – правила політики безпеки для дозволу трафіку додатків зі зони-to-hub до зони-private.
- Трафік від віддаленого об'єкта до центрального. На віддаленому треба створити правила політики безпеки для дозволу трафіку додатків зі зони-private до зони-to-hub. На центральному – правила політики безпеки для дозволу трафіку додатків зі зони-to-branch до зони-private.
- Трафік між віддаленими об'єктами. На вихідному віддаленому треба створити правила політики безпеки для дозволу трафіку додатків зі зони-private до зони-to-hub. На центральному – правила політики безпеки з типом правила intrazone, для дозволу трафіку додатків із зони-

to-branch. Ці правила неявно включають зону призначення зони-to-branch. На віддаленому об’єкті призначення треба створити правила політики безпеки для дозволу трафіку додатків зі зони-to-hub до зони-private.

4 МОДЕЛІ ПРОЄКТУВАННЯ SD-WAN

Цей розділ описує, як Palo Alto Networks Secure SD-WAN та CloudGenix SD-WAN дозволяють організаціям розширити свій периметр безпеки, щоб включити віддалені місця, забезпечити конфіденційність даних для мережевого трафіку в межах організації та забезпечити інспекцію і видимість для всього трафіку, що входить і виходить з мережі.

Для побудови SD-WAN та захисту зовнішніх підключень, Palo Alto Networks надає широкий набір пропозицій, з яких можна обрати:

- Брандмауер нового покоління з PAN-OS Secure SD-WAN
- CloudGenix Autonomous SD-WAN з ION
- Prisma Access

Є багато способів використання концепцій для побудови SD-WAN та захисту трафіку DIA, описаних у попередніх розділах. У цій роботі включено дві конкретні моделі проєктування. Основна відмінність між ними полягає в тому, як кожна з них забезпечує комплексний захист для трафіку на віддалених об’єктах.

PAN-OS Secure SD-WAN

Ця модель проєктування використовує брандмауер нового покоління як для центральних, так і для віддалених об’єктів. Вони з’єднуються, використовуючи вбудовані засоби SD-WAN брандмауера нового покоління. А Panorama використовується для централізованого управління всіма пристроями.

Модель описує топологію мережі з двома центральними об’єктами і кількома віддаленими в одному регіоні. Усі об’єкти мають два підключення до громадської мережі, забезпечені стандартним передавальним Ethernet. SD-WAN з'єднує місця в топології «центр-вилив» і забезпечує вибір шляху для кожної програми через всі можливі. Кожен віддалений об’єкт налаштований для DIA, і трафік DIA ділить обидва підключення до громадської мережі.

Також можна використовувати брандмауер нового покоління для надання сегментації з метою зменшення обсягу відповідності, обмеження виливання даних та зменшення поверхні атаки.

Ця модель об'єднує функції SD-WAN та безпеки на одному пристрої віддаленого об’єкта, що зменшує складність і вартість. Завдяки розгортанню брандмауера нового покоління на кожному місці, можна забезпечити видимість та інспекцію для всіх користувачів і програм у кожному сегменті мережі. Незалежно від вибору між апаратним пристроєм та віртуальними форм-факторами, можна самостійно управляти та розгортати пристрої. Palo Alto Networks рекомендує дану модель, якщо безпека має високий пріоритет для організації.

CloudGenix з Prisma Access

Ця модель проєктування використовує пристрої CloudGenix ION як для центральних, так і для віддалених місць. Вони з’єднуються за допомогою захищеної програмної тканини CloudGenix SD-WAN – AppFabric. Всі пристрої централізовано керуються за допомогою порталу CloudGenix. Конфігурація Prisma Access керується, використовуючи плагін хмарних послуг для Panorama.

Дана модель описує топологію мережі з двома центральними об'єктами та кількома віддаленими в одному регіоні. Усі об'єкти мають два підключення до громадської мережі через стандартний Ethernet. Для з'єднання використовується AppFabric, яка підтримує різні топології в залежності від вимог. SD-WAN забезпечує вибір шляху для кожної програми. Для трафіку DIA кожен віддалений об'єкт, підключений до Prisma Access, розглядається як сторонній кінцевий пункт. Пристрої ION використовують інтерфейси VPN сторонніх постачальників для побудови IPSec-тунелів до з'єднань віддаленої мережі Prisma Access. Трафік DIA розподіляється між обома підключеннями до громадської мережі.

У цій моделі пристрої ION надають брандмауер з урахуванням додатків та зон на кожному віддаленому місці. Крім того, Prisma Access доповнює можливості

ION на місці та надає додаткову видимість та інспекцію для трафіку DIA. Пристрої ION також підтримують автоматичне виведення з ладу та розгортання.

Функції SD-WAN розділяються від функцій безпеки для віддалених об’єктів. Вартість та складність залишаються низькими, оскільки обидві функції керуються та надаються з хмари. Для трафіку DIA Prisma Access надає таку ж безпеку, видимість та контроль, що й брандмауер нового покоління на віддаленому місці.

Palo Alto Networks рекомендує дану модель, якщо для організації важливі автоматичне виведення з ладу та розгортання пристроїв на віддалених місцях, а також всебічна безпека для DIA та хмарних додатків. Ця модель також забезпечує глибоку видимість і продуктивність додатків, що працюють через SD-WAN.

4.1 Модель проєктування PAN-OS Secure SD-WAN

У цій моделі кожен об’єкт підключається до SD-WAN і надає доступ до центральних офісів та локацій дата-центру. Модель передбачає, що центральні об’єкти вже підключені один до одного (рис. 4.1). SD-WAN забезпечує дві основні функції у цій моделі проєктування:

- З'єднання між центральними та віддаленими об’єктами за допомогою VPN VIFs та IPSec-тунелів.
- Прямий доступ до Інтернету з віддалених місць за допомогою DIA VIFs.

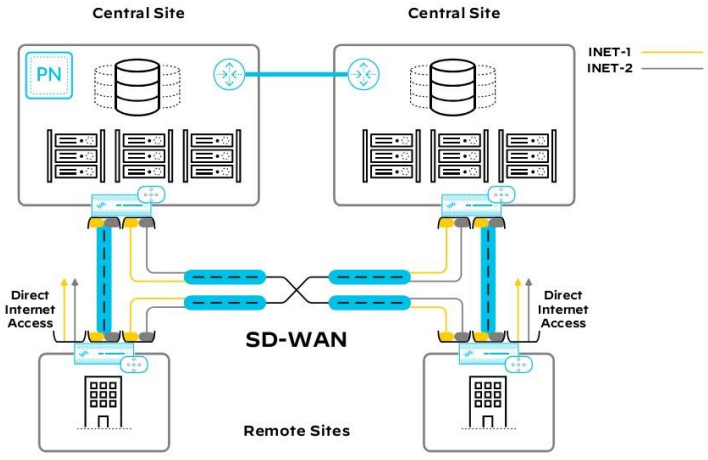


Рис. 4.1 Модель проєктування PAN-OS Secure SD-WAN.

SD-WAN захищає внутрішній корпоративний трафік за допомогою VPN VIFs, що забезпечують інтелектуальний контроль маршрутизації з вибором шляху для кожного додатка. IPSec-тунелі через публічні мережі гарантують конфіденційність даних за допомогою надійного шифрування. SD-WAN також забезпечує вибір шляху для кожного додатка та розподіл навантаження для трафіку через публічні мережі.

На всіх локаціях мережевий брандмауер наступного покоління надає повну видимість користувачів, додатків та контенту для всього мережевого трафіку. На віддаленому об’єкті також можна використовувати мережевий брандмауер наступного покоління для зменшення поверхні атаки за допомогою сегментації.

У цій моделі мережеві брандмауери наступного покоління використовуються в якості пристроїв SD-WAN як на центральних, так і на віддалених локаціях. Panorama використовується для централізованої конфігурації, управління та моніторингу SD-WAN. Кожен пристрій спочатку додається до Panorama як керований, а потім додається до плагіну SD-WAN Panorama як пристрій SD-WAN.

Ця модель передбачає, що інші (не показані) пристрої інфраструктури безпеки надають доступ до Інтернету на центральних місцях.

Пристрої центральних об’єктів

Ця модель інтегрує пристрої центральної вузлової точки SD-WAN в існуючі мережі на центральних місцях. Для керування пристроями необхідно підключити порт управління до існуючої мережі, яка має доступ до Panorama.

На центральних місцях кожен пристрій SD-WAN налаштовується як вузол. Пристрої на кожному місці підключаються до приватної мережі і двох публічних. На інтерфейсах, які підключаються до публічних, потрібно використовувати публічні IP-адреси зі статичним призначенням адреси кожного інтерфейсу, що мають шлюз наступного кроку. BGP слід налаштувати на віртуальний

маршрутизатор для кожного пристрою задля обміну інформацією маршрутизації з пірами в приватній мережі.

При додаванні пристрою до плагіну SD-WAN, для кожного пристрою SD-WAN центрального місця треба включити повний список префіксів або зведені префікси. Якщо необхідно дозволити трафік віддаленого місця до такого ж, треба вибрати один з центральних об’єктів як транзитний і включити зведені префікси віддаленого в список префіксів для пристрою транзитного об’єкта.

Пристрої SD-WAN на центральних об’єктах використовують BGP для розповсюдження своїх списків префіксів до всіх інших. На Panorama створюються правила політики безпеки для дозволу BGP від і до інших пристроїв SD-WAN.

На Panorama слід створити набір політик SD-WAN для керування додатками, ініційованими з центральних місць. Кожна політика повинна включати зону-джерело zone-private та зону-призначення zone-to-branch. Для керування сесіями, що ініціюються з центрального місця за допомогою політики SD-WAN, потрібно лише налаштувати політику SD-WAN на цьому місці.

Політики SD-WAN застосовуються лише до одного кроку маршрутизації SD-WAN і ефективні для контролю потоків між місцями типу "віддалений об’єкт – центральний об’єкт" або "центральний до віддаленого". Щоб контролювати ці потоки, потрібно застосувати політики SD-WAN, які відповідають потоку як на віддаленому об’єкті, так і на центральному.

Пристрої віддалених об’єктів

Ця модель об'єднує функції SD-WAN та безпеки на одному пристрої, що зменшує складність і витрати. Оскільки мережевий екран нового покоління розгортається на кожному об’єкті, можна забезпечити видимість та інспекцію для всіх користувачів та додатків у кожному сегменті мережі.

На віддалених об’єктах кожен пристрій SD-WAN налаштовується як відділ. Пристрої на кожному місці підключаються до приватної мережі і двох публічних. На інтерфейсах, підключених до публічних мереж, можна використовувати

публічні або приватні IP-адреси за допомогою пристрою NAT. Можна також налаштувати кожний публічний інтерфейс з використанням автоматичного призначення адреси за допомогою DHCP або статичного призначення адреси, за умови, що кожен інтерфейс має шлюз наступного кроку.

Пристрої SD-WAN на віддалених місцях використовують BGP для оголошення своїх прямо-підключених LAN-мереж та вчаться маршрутам від пристроїв хабів SD-WAN на центральних. Якщо є додаткові префікси для додавання, треба вказати їх у списку префіксів для об'єкта. На Panorama створюються правила політики безпеки для дозволу BGP від та до пристроїв хабів SD-WAN на центральних об'єктах.

На Panorama створюються набори політик SD-WAN для контролю додатків, ініційованих з віддалених місць. Кожна політика має включати джерело зони-приватної та призначення зони-хаб. Для контролю сеансів, ініційованих з віддаленого об'єкта за допомогою політики SD-WAN, потрібно налаштувати політику лише на цьому об'єкті. Для кожної політики SD-WAN необхідно вибрати PQP і TDP та зазначити їх у правилі політики. Де можливо, слід використовувати вбудовані PQP для спрощення конфігурації. Також потрібно включити PQP для політик SD-WAN, які контролюють трафік DIA, навіть якщо DIA VIF не виконує моніторингу шляху з кінця в кінець. DIA VIF успадковує стан моніторингу шляху тунелів IPSec від джерел, що є членами інтерфейсів.

Для підтримки трафіку DIA треба налаштувати кожний публічний інтерфейс для виконання NAT. На Panorama необхідно створити набір правил політики NAT – одне для кожного з публічних інтерфейсів. Кожне правило NAT перетворює трафік з приватної зони на IP-адресу публічного. Крім того, потрібно створити необхідні правила політики безпеки для дозволу додатків доступу до публічної зони.

Якщо потрібно, можна створити кілька приватних зон безпеки для надання сегментації на віддаленому місці. Цей підхід дозволяє розділити мережу на декілька захищених, що зменшить обсяг вимог з відповідності та обмежить

викидання даних. Можна також створити необхідні правила політики безпеки для дозволу додатків від та до кожної додаткової зони безпеки (рис. 4.2).

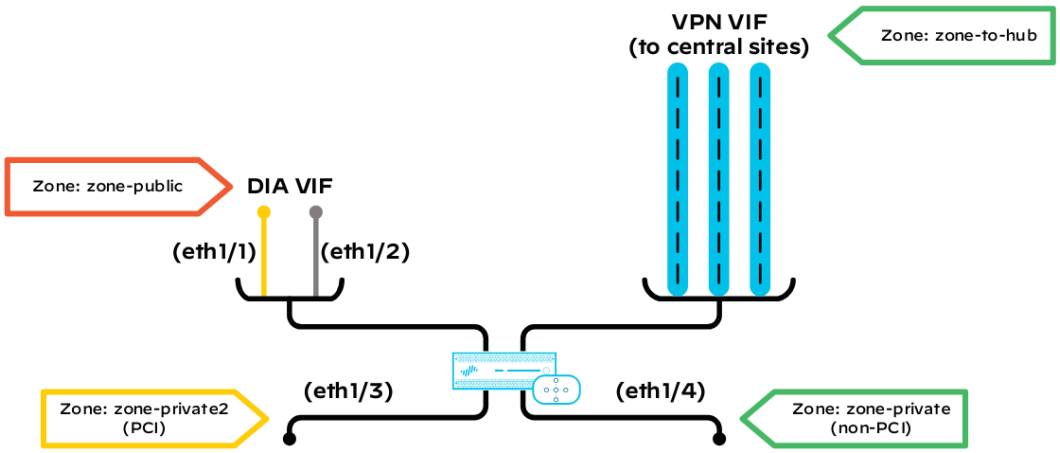


Рис. 4.2 Сегментація віддаленого об’єкта.

Взаємодія між об’єктами

Плагін SD-WAN встановлює VPN-тунелі між об’єктами. Для цього потрібно мати щонайменше один пристрій SD-WAN типу «хаб» на центральному місці та щонайменше один пристрій SD-WAN типу «гілка» на віддаленому. Плагін SD-WAN генерує конфігурацію, яка створює оверлейну мережу для публічної мережі та для кожного типу приватної мережі в організації. Якщо у будь-якого пристрою SD-WAN є кілька інтерфейсів, підключених до тієї ж оверлейної мережі, то для неї між центральним і віддаленим об’єктом створюється повна мережа VPN-тунелів.

У цій моделі всі місця знаходяться в одному логічному регіоні. Плагін SD-WAN налаштовується з одним VPN-кластером, що відповідає регіону. VPN-кластер є найвищим рівнем організаційної структури для групування, що використовується моніторинговою панеллю. У межах кластера можна порівнювати продуктивність об’єктів, переглядати статистику продуктивності застосунків та статистику продуктивності зв'язків на об’єкті.

Після завершення процесу AutoVPN і надання згенерованої плагіном конфігурації, пристрої SD-WAN на віддалених місцях ініціюють з'єднання IPSec з центральними та починають застосовувати політики SD-WAN, надані з Panorama.

Налаштування політик застосунків SD-WAN

Компанія Palo Alto Networks рекомендує моніторити трафік мережі, а потім використовувати зібрану інформацію для розробки політики застосунків SD-WAN для організації. У разі відсутності налаштованих політик, трафік перенаправляється через SD-WAN за допомогою традиційної маршрутизації разом із циклічним розподілом навантаження.

Потрібно налаштувати політики SD-WAN для відповідності застосункам і явно розподілити трафік по публічних мережах. Ці політики створюються і застосовуються до пристроїв SD-WAN на джерелах трафіку. Оскільки для налаштування цих політик використовуються шаблони Panorama, потрібно створити окремі політики для кожної групи пристроїв Panorama – один набір політик для центральних пристроїв і ще один для віддалених.

4.2 Модель проєктування CloudGenix3 Prisma Access

У цій моделі кожен об’єкт підключається до CloudGenix AppFabric та забезпечує доступ до центральних місць розташування та дата-центрів. Ця модель передбачає, що центральні місця вже мають з'єднання через існуюче громадське або приватне WAN-з'єднання. На всіх об’єктах потрібно використовувати пристрій ION у якості місцевого. Після завершення основної конфігурації пристрою об’єкт переходить у режим керування.

Однією з ключових відмінностей від моделі PAN-OS Secure SD-WAN є те, що Prisma Access використовується для захисту трафіку DIA, і кожен віддалений об’єкт підключається безпосередньо до Prisma за допомогою з'єднань VPN від третіх сторін (рис. 4.3).

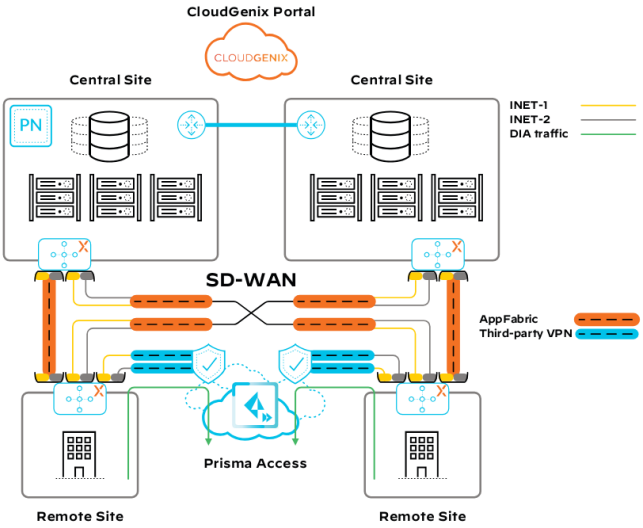


Рис. 4.3 Модель проєктування CloudGenix3 Prisma Access.

Усі аспекти CloudGenix SD-WAN керуються через CloudGenix Portal. Для Prisma Access, Panorama та Cortex™ Data Lake управління всіма політиками та моніторингом здійснюється централізовано, а інфраструктурою Prisma Access управляє Palo Alto Networks.

SD-WAN захищає внутрішній корпоративний трафік за допомогою AppFabric, що використовує IPSec-тунелі через громадські мережі для забезпечення конфіденційності даних за допомогою надійного шифрування. Пристрої ION автоматично вибирають найкращий шлях WAN для додатків на основі бізнес-політики та аналізу метрик продуктивності у реальному часі та WAN-зв'язків.

Ця модель передбачає, що інші (не показані) пристрої інфраструктури безпеки надають доступ до Інтернету на центральних місцях.

Пристрої центральних об’єктів

У цій моделі ION-пристрої інтегруються в існуючі мережі на центральних місцях. Пристрої на кожному місці підключаються до приватної та двох громадських мереж. Для управління пристроєм треба підключити порт контролера ION до існуючої мережі з доступом до Інтернету. Пристрій підключається до

CloudGenix Portal і з'являється як неналаштований. На CloudGenix Portal для кожного центрального місця створюється об’єкт і конфігурується як дата-центр. Потім для нього налаштовується та призначається пристрій.

IP-адресу треба налаштувати для кожного інтерфейсу та призначити мітку лінії. Можна використовувати як статично призначені, так і призначені через DHCP IP-адреси. Palo Alto Networks рекомендує використовувати статично призначені IP-адреси для підключень на центральних об’єктах. Пристрої ION можна розмістити за пристроєм NAT. Тоді треба вказати громадські IP-адреси при конфігурації інтерфейсів.

BGP налаштовується для кожного пристрою, щоб обмінюватися маршрутною інформацією з пірами на приватній мережі.

Пристрої віддалених об’єктів

У цій моделі ION-пристрої розгортаються в нових мережах на віддалених місцях. Вони підключаються до приватної мережі та двох громадських мереж. Для управління пристроєм треба підключити порт інтернету ION до громадських мереж. Пристрій підключається до CloudGenix Portal і з'являється як неналаштований. На CloudGenix Portal для кожного віддаленого місця створюється об’єкт і конфігурується як філія. Потім пристрій налаштовується та призначається для нього.

IP-адреса налаштовується для кожного інтерфейсу та призначається мітка лінії. Можна використовувати як статично призначені, так і призначені через DHCP IP-адреси. Palo Alto Networks рекомендує використовувати статично призначену IP-адресу для підключення до приватної мережі та IP-адреси, призначені через DHCP, для підключень до громадських.

Підключення об’єктів

CloudGenix Portal автоматично конфігурує AppFabric між об’єктами після переходу їх у режим управління. У цей момент портал також надсилає політику

безпеки та додатків на всі об’єкти. За замовчуванням AppFabric будує топологію «центр-і-вилив», що підтримує зв'язок між віддаленими місцями через центральний об’єкт.

Налаштування політик застосунків SD-WAN

Palo Alto Networks рекомендує відстежувати аналітику мережі, а потім використовувати зібрану інформацію для розробки політики додатків SD-WAN для організації. У випадку впровадження на базі вже існуючої інфраструктури існує можливість спершу впровадити пристрої ION в режим аналітики, який лише відстежує трафік. Однак, у випадку створення нової інфраструктури, пристрої переходять в режим управління.

Політики SD-WAN потрібно налаштовувати у відповідності додаткам, явно розподіляти трафік додатків через громадські мережі та вказати, які з них відправляти на Prisma Access.

Підключення віддалених об’єктів до Prisma Access

Політики застосунків CloudGenix можуть витісняти політики маршрутизації за напрямком. Замість того, щоб просто налаштовувати типовий маршрут до Prisma Access, він вважається за набір сторонніх кінцевих точок. Потім створюються політики, що відповідають застосункам і їм призначаються кінцеві точки Prisma Access.

Є два варіанти керування інтеграцією від CloudGenix SD-WAN до Prisma Access. У невеликих розгортаннях, зазвичай менше 20 місць, інтеграцією керується з Prisma Access вручну, використовуючи як Panorama, так і CloudGenix Portal. У великих розгортаннях інтеграцію автоматизується з Prisma Access через API за допомогою платформи CloudGenix CloudBlades. CloudBlade надає абстрактний шар між CloudGenix Portal та певним хмарним сервісом, чим спрощує інтеграцію з цим сервісом. CloudBlade для Prisma Access мереж надає можливість автоматично налаштувати CloudGenix Portal, пристрої ION, Panorama та Prisma Access.

Опція налаштування вручну

На Panorama, для кожного віддаленого об’єкта створюється підключення до мережі Prisma Access на місці, що найближче до віддаленого. Якщо використовується активне/активне підключення, створюється додаткове підключення до мережі Prisma Access на місці, що наступне за віддаленим. Опція активне/активне споживає вдвічі більше ліцензованої пропускної здатності Prisma Access, оскільки обидва зв'язки налаштовані як основні тунелі.

На CloudGenix Portal, для кожного віддаленого об’єкта створюється та налаштовується VPN сторонніх виробників від інтерфейсу до найближчого місця розташування Prisma Access. Якщо використовується активне/активне підключення, створюється та налаштовується додатковий VPN сторонніх виробників з цього інтерфейсу до наступного найближчого місця розташування Prisma Access.

Після створення підключень VPN сторонніх виробників, пов'язана політика SD-WAN налаштовується для направлення інтернету та хмарних застосунків до Prisma Access. Також необхідно налаштувати правила політики безпеки на Prisma Access для пов'язаних застосунків. Додаткові конфігурації можуть бути потрібні для забезпечення належної роботи мережі та безпеки даних.

Опція налаштування через CloudBlade

CloudBlade Prisma Access автоматизує сторонні компоненти VPN параметра ручного налаштування, що робить цю опцію дуже масштабованою. Вона передбачає розгортання контейнера Docker на місці або в контейнері публічного хмарного середовища для забезпечення зв'язку між CloudBlade Prisma Access та Panorama. На CloudGenix Portal також потрібно надати регіональні теги Prisma Access для інтерфейсів пристроїв на віддалених об’єктах. CloudBlade керує як конфігурацію VPN сторонніх виробників, так і підключення до Prisma Access.

Після створення підключень VPN сторонніх виробників, налаштовується пов'язана політика SD-WAN для направлення інтернету та хмарних застосунків до

Prisma Access. Також потрібно налаштувати правила політики безпеки на Prisma Access для пов'язаних застосунків. Необхідно враховувати, що цей процес може вимагати додаткових налаштувань та ручних дій зі сторони адміністратора для забезпечення правильної роботи мережі та безпеки даних.

ВИСНОВКИ

1. Palo Alto Networks надає організаціям кілька варіантів розгортання SD-WAN. Окрім широкого огляду WAN, було детально розглянуто технічні аспекти PAN-OS Secure SD-WAN і описано найкращі методи інтеграції CloudGenix з Prisma Access. Враховуючи аналіз, можна визначити, яка пропозиція є найбільш ефективною у відповідності до бізнес-вимог якоїсь певної організації.

2. Модель проєкту PAN-OS Secure SD-WAN консолідує функції SD-WAN і функції безпеки на одному пристрої на віддалених об’єктах, що зменшує складність і витрати. Усі об’єкти в організації отримують переваги від комплексних функцій безпеки наступного покоління мережевого брандмауера. Видимість та інспекція надається всім користувачам і застосункам у кожному сегменті мережі, включаючи потоки трафіку до центральних місць, хмарних застосунків і Інтернету.

3. Модель проєкту CloudGenix з Prisma Access поєднує передові можливості SD-WAN від CloudGenix SD-WAN з хмарно-орієнтованими комплексними можливостями безпеки від Prisma Access. Функції SD-WAN і безпеки пристроїв ION доповнюються додатковою хмарно-доставленою безпекою. Видимість та інспекція забезпечується для всіх користувачів і застосунків усюди, включаючи потоки трафіку до центральних місць, хмарних застосунків та Інтернету.

4. Обидві моделі надають послідовну безпеку, незалежно від місця розташування користувачів та застосунків. Вибір між цими моделями залежить від конкретних бізнес-потреб організації та рівня безпеки, який бажано досягти.

ПЕРЕЛІК ПОСИЛАНЬ

1. Prisma SD-WAN Security Architecture. URL: https://www.paloaltonetworks.com/resources/whitepapers/prisma-sd-wan-security-architecture
2. PAN-OS Secure SD-WAN deployment guide. URL: https://www.paloaltonetworks.com/resources/guides/pan-os-secure-sd-wan-deployment-guide
3. Palo Alto Networks reference architectures. URL: https://www.paloaltonetworks.com/resources/reference-architectures
4. Palo Alto Networks Prisma SD-WAN. URL: https://www.paloaltonetworks.com/sase/sd-wan
5. The Industry’s Best SD-WAN with Integrated Security: CloudGenix & Prisma Access. URL: https://www.paloaltonetworks.com/resources/webcasts/cloudgenix-prisma-access
6. SASE for Securing Internet: Deployment Guide. URL: https://www.paloaltonetworks.com/resources/guides/sase-securing-internet-deployment-guide
7. Palo Alto Networks SD-WAN Reference Architecture Guide, June 2020
8. Rohan Naggi, Rachna Srivastava, Tim Van Herck, Steven Woo. SD-WAN The Networking Blueprint for Modern Businesses, 2018

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Презентація
до кваліфікаційної роботи на здобуття освітнього ступеня бакалавра
на тему: «**Розробка системи захисту глобальних програмно-визначених мереж на основі технології Palo Alto Networks**»

Виконала: студентка Кравець А.А.
Керівник: Гніденко М.П.

Мета роботи, об'єкт та предмет дослідження

Мета роботи – аналіз моделей та стратегій SD-WAN від Palo Alto Networks, вивчення концепцій і сервісів для WAN та віддалених місць, а також дослідження методів маршрутизації та захисту в SD-WAN.

Об'єкт дослідження – програмно-апаратні рішення для управління широкосмуговими мережами (WAN) та захисту віддалених місць, які пропонує Palo Alto Networks.

Предмет дослідження – архітектурні моделі SD-WAN, методи маршрутизації, стратегії безпеки, управління розгортанням та інтеграція з хмарними сервісами у рамках рішень від Palo Alto Networks.

Вступ

У сучасному цифровому світі безпека мережі є однією з найважливіших проблем. Одним з передових рішень у цій галузі є використання технології від компанії Palo Alto Networks. У процесі дослідження буде розглянуто основні проблеми надання безпеки SDN і досліджено прототип системи захисту, який буде використовувати ключові можливості технології Palo Alto Networks.

У рамках роботи буде описана референтна архітектура, а саме як SD-WAN дозволяє організаціям ефективніше використовувати свої WAN-зв'язки та отримувати можливість відстежувати й контролювати трафік користувачів на віддалених об’єктах і WAN-трафік організації, що направляється в інший віддалений об’єкт, великий кампус або центр обробки даних.

01 МОДЕЛІ ТА СТРАТЕГІЯ SD-WAN ВІД PALO ALTO NETWORKS

Модель дизайну безпеки SD-WAN на основі PAN-OS

- ***Брандмауери наступного покоління***: Вбудовані функції гарантії безпеки та SD-WAN у PAN-OS.
- ***PAN-OS 9.1***: Інтелектуальний вибір шляху на основі існуючої безпеки.
- ***App-ID™***: Видимість і контроль застосунків для детального управління трафіком.
- ***Panorama™***: Конфігурація та моніторинг пристроїв; створення оверлейної мережі IPSec, динамічна маршрутизація.
- ***Комплексний захист***: Безпечний доступ до ресурсів, блокування шкідливого ПЗ, послідовна безпека для локальних і хмарних середовищ.

01 МОДЕЛІ ТА СТРАТЕГІЯ SD-WAN ВІД PALO ALTO NETWORKS

Модель дизайну SD-WAN від CloudGenix

- ***Придбання CloudGenix***: Прискорення розвитку безпечного доступу до сервісів на межі.
- ***CloudGenix ION***: Автоматичне встановлення VPN-з'єднань, політика на основі бізнес-наміру, динамічний вибір шляху для застосунків.
- ***Портал управління CloudGenix***: Автоматична аутентифікація, безконтактне розгортання та встановлення.
- ***Реальний час аналізу***: Визначення відповідного шляху для застосунків.

01 МОДЕЛІ ТА СТРАТЕГІЯ SD-WAN ВІД PALO ALTO NETWORKS

Стратегія Palo Alto Networks щодо SD-WAN

- ***Дві архітектури SD-WAN***: PAN-OS Secure SD-WAN та CloudGenix SD-WAN.
- ***Prisma Access***: Безпека та запобігання загрозам для віддалених мереж.
- ***Управління через Panorama***: Повний набір функцій PAN-OS, прямий доступ до інтернету.
- ***Інтеграція CloudGenix SD-WAN та Prisma Access***: Незавантажений віддалений об'єкт з комплексною безпекою.

02 КОНЦЕПЦІЇ ТА СЕРВІСИ ДЛЯ WAN І ВІДДАЛЕНИХ МІСЦЬ

Огляд WAN

- ***MPLS VPN***: Приватні мережі з гарантованою пропускною здатністю, що забезпечують надійне та безпечне з'єднання між філіями та центром обробки даних.
- ***Internet VPN***: Віртуальні приватні мережі, що використовують інтернет для створення захищених тунелів, забезпечуючи доступ до корпоративних ресурсів через громадські мережі.
- ***Висока доступність WAN***: Застосування резервних каналів та методів автоматичного перемикання для забезпечення безперервної роботи мережі у випадку збою основного каналу.
- ***Програмно-визначена WAN***: Інтелектуальне управління трафіком на основі політик, що використовує різні типи підключень (MPLS, інтернет) задля оптимального вибору шляху для кожного застосунку.

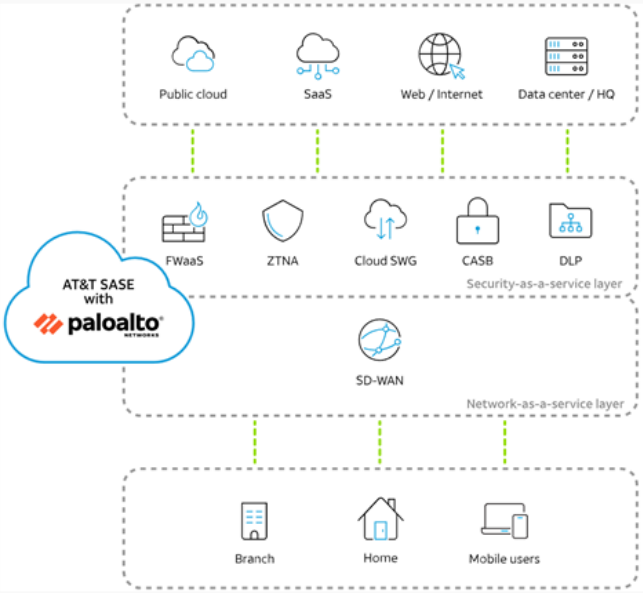
02 КОНЦЕПЦІЇ ТА СЕРВІСИ ДЛЯ WAN І ВІДДАЛЕНИХ МІСЦЬ

Опції доступу до Інтернету для віддалених місць

- ***Централізований доступ***: Весь трафік прямує через центральний об’єкт. Збільшує затримку та витрати.
- ***Хмарне підключення***: Трафік прямує до хмарного центру. Зменшує затримку, додаткові витрати.
- ***Прямий доступ (DIA)***: Прямує безпосередньо до точки призначення. Зменшує затримку, підвищує витрати на безпеку.
- ***Довірений прямий доступ***: Довірений трафік йде напряму, інший через центральний об’єкт. Зменшує затримку для довірених ресурсів.
- ***Безпека***: Послідовна видимість та інспекція трафіку. Використання архітектури Zero Trust.

Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE) – це нова концепція, що поєднує в собі технології для захисту мережі і даних в умовах цифрової трансформації. SASE пропонує об'єднане хмарно-орієнтоване рішення, яке включає в себе WAN edge/SD-WAN, безпечний веб-шлюз, CASB, Zero Trust, безпеку DNS та брандмауер як сервіс. Це забезпечує інтеграцію та видимість для всіх місць, мобільних користувачів та хмари. Prisma Access від Palo Alto Networks – це приклад рішення, сумісного з SASE, яке надає повну міграцію WAN і сервісів безпеки до архітектури хмарного типу.



02 КОНЦЕПЦІЇ ТА СЕРВІСИ ДЛЯ WAN І ВІДДАЛЕНИХ МІСЦЬ

Опції SD-WAN

- ***Автономний SD-WAN з прямим доступом до Інтернету***: коли SD-WAN пристрої використовуються без проксі або NAT для надання прямого доступу до Інтернету з віддалених місць.
- ***SD-WAN з присвяченою безпекою DIA***: використовує прямий доступ до Інтернету (DIA), але з додатковими заходами безпеки, такими як фірмовий брандмауер.
- ***Брандмауер нового покоління SD-WAN з прямим доступом до Інтернету***: комбіноване рішення, яке поєднує в собі брандмауер нового покоління та SD-WAN для надання безпеки та управління мережею.
- ***Автономний SD-WAN з доступом до Prisma Access DIA***: використовує Prisma Access для безпеки та керування доступом до Інтернету.

03 ДЕТАЛІ ДИЗАЙНУ PALO ALTO NETWORKS

1. ***Нові конструкції для PAN-OS Secure SD-WAN*** – оновлені архітектурні рішення для надання безпеки та управління SD-WAN.
2. ***Керування розгортанням SD-WAN за допомогою Panorama*** – управління і розгортання мережі SD-WAN через інтерфейс Panorama.
3. ***Зони безпеки*** – визначені області мережі з різними рівнями безпеки для захисту мережі від несанкціонованого доступу.
4. ***Оверлей AutoVPN*** – автоматизований VPN для підключення різних мереж та пристроїв до SD-WAN.
5. ***Маршрутизація SD-WAN*** – інтелектуальне керування маршрутами для оптимізації трафіку в SD-WAN.
6. ***Захист місць*** – заходи для безпеки віддалених місць і користувачів мережі.

04 МОДЕЛІ ПРОЄКТУВАННЯ SD-WAN

Для побудови SD-WAN та захисту зовнішніх підключень, Palo Alto Networks надає широкий набір пропозицій, з яких можна обрати:

- *Брандмауер нового покоління з PAN-OS Secure SD-WAN*
- *CloudGenix Autonomous SD-WAN з ION*
- *Prisma Access*

Є багато способів використання концепцій для побудови SD-WAN та захисту трафіку DIA. У цій роботі включено дві конкретні моделі проєктування. Основна відмінність між ними полягає в тому, як кожна з них забезпечує комплексний захист для трафіку на віддалених об’єктах.

04 МОДЕЛІ ПРОЄКТУВАННЯ SD-WAN

Модель проєктування PAN-OS Secure SD-WAN

У цій моделі кожен об’єкт підключається до SD-WAN і надає доступ до центральних офісів та локацій дата-центру. Модель передбачає, що центральні об’єкти вже підключені один до одного (рис. 4.1). SD-WAN забезпечує дві основні функції у цій моделі проєктування:

- З'єднання між центральними та віддаленими об’єктами за допомогою VPN VIFs та IPSec-тунелів.
- Прямий доступ до Інтернету з віддалених місць за допомогою DIA VIFs.

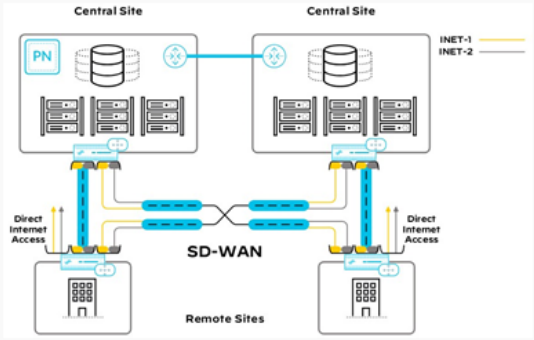


Рис. 4.1 Модель проєктування PAN-OS Secure SD-WAN.

04 МОДЕЛІ ПРОЄКТУВАННЯ SD-WAN

Модель проєктування CloudGenix3 Prisma Access

У цій моделі кожен об’єкт підключається до CloudGenix AppFabric та забезпечує доступ до центральних місць розташування та дата-центрів.

Однією з ключових відмінностей від моделі PAN-OS Secure SD-WAN є те, що Prisma Access використовується для захисту трафіку DIA, і кожен віддалений об’єкт підключається безпосередньо до Prisma за допомогою з'єднань VPN від третіх сторін (рис. 4.3).

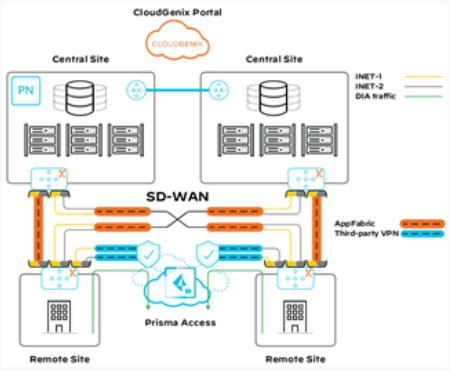


Рис. 4.3 Модель проєктування CloudGenix3 Prisma Access.

Висновки

1. Palo Alto Networks пропонує кілька варіантів розгортання SD-WAN, включаючи PAN-OS Secure SD-WAN. Вибір найкращого варіанту залежить від бізнес-вимог конкретної організації.

2. Модель проєкту PAN-OS Secure SD-WAN об'єднує функції SD-WAN і безпеки на одному пристрої на віддалених об'єктах, що спрощує управління і зменшує витрати.

3. Модель проєкту CloudGenix з Prisma Access поєднує передові можливості SD-WAN від CloudGenix з хмарно-орієнтованими можливостями безпеки від Prisma Access.

4. Обидві моделі забезпечують послідовну безпеку для користувачів та застосунків незалежно від їх місця розташування. Вибір між ними залежить від бізнес-потреб та рівня безпеки.