Cloud Protection Suite для Hybrid Mesh Firewall: Інформаційний матеріал

Cloud Protection Suite - це ваш шлях до Hybrid Mesh Firewall

Що таке Hybrid Mesh Firewall?

Гібридний сітковий брандмауер (Hybrid Mesh Firewall) – це термін, розроблений аналітичною компанією Gartner. За своєю суттю, це інтегрована платформа безпеки з централізованим хмарним керуванням, призначена для захисту застосунків та інфраструктури за допомогою брандмауерів будь-якого формфактора.

У своєму "Посібнику з ринку платформ гібридних сіткових брандмауерів" за 2024 рік (2024 Market Guide for Hybrid Mesh Firewall Platforms) Gartner описує його як брандмауер, що підтримує різноманітні варіанти розгортання. Це включає апаратні та віртуальні пристрої, хмарні рішення та моделі "як послуга" (as-a-service), які об'єднані єдиною хмарною площиною керування. Така платформа передбачає інтеграцію з конвеєрами безперервної інтеграції/безперервної доставки (CI/CD), нативну інтеграцію з хмарними середовищами та розширені можливості запобігання загрозам. Ці можливості поширюються на захист пристроїв Інтернету речей (IoT) та протидію атакам на основі DNS. Окрім основних функцій, Gartner також визначає "опціональні" можливості, такі як безпечний віддалений доступ, агентна або безагентна мікросегментація, а також інтеграція з XDR (розширене виявлення та реагування) та SASE (безпечний доступ до сервісів на периферії мережі), серед іншого.

Важливо зазначити, що починаючи зі звітного циклу "Магічного квадранта" (Magic Quadrant) 2025 року, Gartner замінює свій звіт "Мережеві брандмауери" (Network Firewall) на новий звіт "Магічний квадрант для платформ гібридних сіткових брандмауерів" (Magic Quadrant for Hybrid Mesh Firewall Platforms). Компанія Cisco активно бере участь у підготовці цього майбутнього звіту.

Гібридний сітковий брандмауер від Cisco

Компанія Cisco розвиває та розширює визначення гібридного сіткового брандмауера, надане Gartner. У своєму баченні Cisco включає можливості для захисту вразливостей застосунків від експлуатації, а також здатність захищати процеси розробки та розгортання моделей штучного інтелекту (ШІ) для застосунків, що використовують технології ШІ.

Гібридний сітковий брандмауер від Cisco – це високорозподілена архітектура безпеки, оптимізована для сегментації за принципом нульової довіри (zero-trust). Вона призначена для захисту застосунків та інфраструктури в різноманітних середовищах, таких як центри обробки даних, хмарні платформи, корпоративні мережі (кампуси) та середовища Інтернету речей (IoT). Ця архітектура об'єднує брандмауери різних формфакторів (апаратні, віртуальні, "як послуга" та хмарно-нативні), засоби мікросегментації, технології захисту від експлойтів та захисту моделей ШІ. Все це керується через єдину хмарну площину управління.

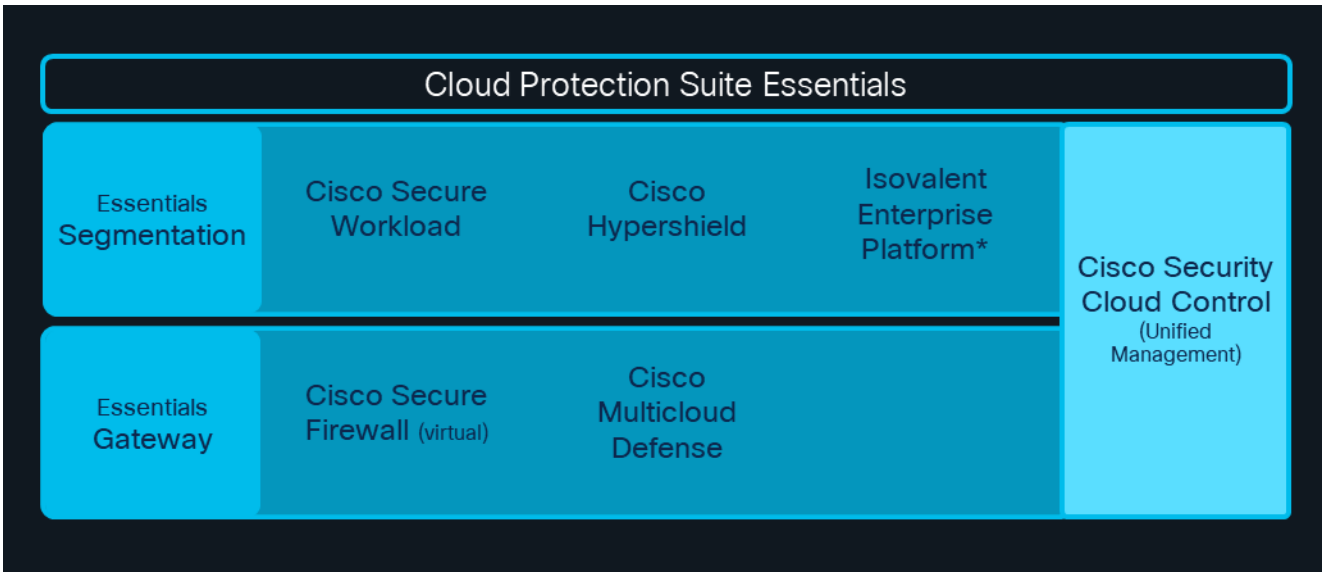
Гібридний сітковий брандмауер пропонує просту та гнучку модель впровадження та використання ключових програмних технологій, об'єднаних у пакеті Cisco Cloud Protection Suite.

AM BITS

cisco Partner Gold Integrator

Пакет Cisco Cloud Protection Suite

Нову версію пакета Cisco Cloud Protection Suite було запущено в лютому 2025 року. Рівень "Essentials" (Базовий) тепер складається з двох стартових опцій, які можна використовувати як незалежно, так і в комбінації, залежно від потреб клієнта: "Essentials Segmentation" (Базова сегментація) та "Essentials Gateway" (Базовий шлюз). До складу обох опцій входить Cisco Security Cloud Control – єдина консоль управління.



* На даний момент доступ до Isovalent Enterprise Platform через консоль управління Security Cloud Control не надається.

Модель ліцензування пакета Cloud Protection Suite поєднує в собі простоту та гнучкість, що забезпечує легке впровадження рішення гібридного сіткового брандмауера (Hybrid Mesh Firewall) від Cisco.

Essentials Segmentation (Базова сегментація): Ліцензується на основі кожного робочого навантаження (per workload), мінімальна кількість – 25 ліцензійних прав.

- Ліцензії можуть бути розподілені між однією або декількома опціями. Наприклад, маючи 100 ліцензій на робоче навантаження, 50 з них можна виділити для Secure Workload, а інші 50 – для Isovalent.
- Клієнти можуть легко переміщувати ліцензії в межах опції сегментації. Наприклад, клієнт може почати зі 100 ліцензій Secure Workload, а згодом, у міру зміни потреб, перейти на Hypershield.

Essentials Gateway (Базовий шлюз): Ліцензується на основі кожного віртуального брандмауера (per virtual Firewall), мінімальна кількість – 10 ліцензійних прав.

- Кожна ліцензія на віртуальний брандмауер включає 720 годин роботи шлюзу на місяць та ліцензію FTDv30 (Firepower Threat Defense virtual).
- Ліцензії для шлюзу включають права на моніторинг загроз, управління політиками (через хмарний центр управління брандмауерами – Cloud Delivered Firewall Management Center) та реєстрацію подій (через систему аналітики безпеки та реєстрації – Security Analytics and Logging).
- Усі продукти керуються через єдину консоль Security Cloud Control.

Додаткові можливості гібридного сіткового брандмауера (Complementary Hybrid Mesh Firewall capabilities):

- Рішення Cisco AI Defense для захисту моделей штучного інтелекту (ШІ) потребує окремої покупки; воно не входить до складу Cloud Protection Suite.
- Рішення Cisco Secure Access (FWaaS – Брандмауер як послуга) потребує окремої покупки; воно не входить до складу Cloud Protection Suite.

AM BITS

cisco Partner
Gold Integrator

Сценарії впровадження

1. Зменшення площі атаки за допомогою сегментації

- Запобігання несанкціонованому переміщенню даних та захист застосунків у центрах обробки даних (ЦОД) та хмарних середовищах.
- Макросегментація в межах ЦОД або між віртуальними приватними хмарами (VPC).
- Інтелектуальна зонна сегментація зменшує площу атаки без використання агентів та забезпечує картування залежностей застосунків і оркестрацію політик.
- Агентна мікросегментація для традиційних робочих навантажень (сервери bare-metal, віртуальні машини та контейнери) локально (on-premises) та в хмарних середовищах.
- Хмарно-нативні безпека, мережеві функції та спостережливість (observability) для сучасних середовищ Kubernetes.
- (У майбутньому) Автономна сегментація – це ШІ-нативне рішення, яке самостійно виконує сегментацію та постійно адаптується на основі аналізу поведінки процесів, змін у файлах та вивчених переваг політик.

2. Зупинка загроз та усунення вразливостей застосунків

- Запобігання вхідним атакам та витоку даних.
- Виявлення загроз у зашифрованому трафіку без зниження продуктивності.
- Вибіркове розшифрування трафіку на основі встановленого порогу ризику.
- Захист від відомих загроз та варіантів загроз "нульового дня" за допомогою Snort IPS та SnortML.
- Виявлення, пріоритезація та усунення вразливостей застосунків, а також застосування точкових компенсаційних заходів контролю.

3. Усунення архітектурних та операційних складностей

- Спрощення адміністративних операцій завдяки єдиному входу (single sign-on), автоматизованому наданню ресурсів (provisioning) та керуванню доступом на основі ролей (RBAC) через єдину хмарну платформу управління.
- Підвищення продуктивності за допомогою ШІ-асистента та оптимізація політик на основі аналітичних даних, отриманих за допомогою AIOps (використання ШІ для автоматизації IT-операцій).
- Зменшення накладних витрат завдяки хмарно-незалежній автоматизації та оркестрації для розгортання шлюзів, включаючи конфігурацію, автоматичне масштабування та самовідновлення.
- Захист існуючих інвестицій у безпеку завдяки плавній міграції між рішеннями в міру зміни бізнес-вимог.
- Скорочення часу на управління наявними або новими ліцензійними правами.

4. Цільові клієнти

- Галузі: Охорона здоров'я, виробництво, банківська справа/фінансові послуги, комунальні підприємства (енергетика), транспорт.
- Профіль клієнта:
- Організації з понад 1000 співробітниками (великі комерційні організації (commercial-select), корпоративний сектор (enterprise), державний сектор).

- Організації з гібридними середовищами (локальна інфраструктура та одна або декілька хмар).

- Існуючі клієнти, що використовують Identity Services Engine (ISE), Secure Firewall, мережеві рішення Cisco для центрів обробки даних (Cisco DC Networking) та комутаційну інфраструктуру Cisco (Cisco Switching Infrastructure).

AM BITS

Cisco Partner
Gold Integrator

Джерела:

- Hybrid Mesh Firewall FAQ
- Hybrid Mesh Firewall BDM
- Hybrid Mesh Firewall webpage
- Cloud Protection Suite webpage
- Cloud Protection Suite Ordering Guide
- Cloud Protection Suite Calculator