

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ № 2

з дисципліни:

«ПРОЕКТУВАННЯ, РОЗРОБКА І РЕАЛІЗАЦІЯ КРИПТОГРАФІЧНИХ СИСТЕМ»

Дослідження реалізацій протоколів IPSec

Виконала:

Студентка групи ФІ-22мн

Калитюк Дар'я

КИЇВ 2023

Мета роботи: дослідження особливостей реалізації криптографічних механізмів протоколів IPSec.

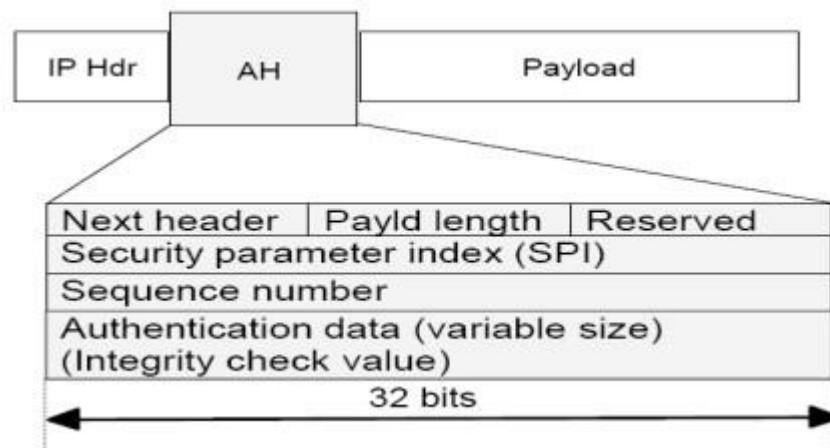
Хід роботи

IPsec — це стек протоколів і стандартів, які визначають механізми забезпечення цілісності і конфіденційності для комунікацій на мережевому рівні, що дозволяє використовувати його для захисту будь-яких протоколів, що базуються на стеку протоколів TCP/IP (ICMP, UDP тощо). IPsec може працювати в двох режимах: тунельному та транспортному. Тунельний режим використовується для захисту всього пакету даних, який включає в себе заголовок та корисне навантаження (payload). Весь пакет обгортається новим заголовком (тунельним заголовком), і такий "запакований" пакет передається через мережу. Тунельний режим широко використовується для створення віртуальних приватних мереж (VPN). Транспортний режим застосовується для захисту самого тіла (payload) IP-пакету, залишаючи незахищеним заголовок оригінального пакету.

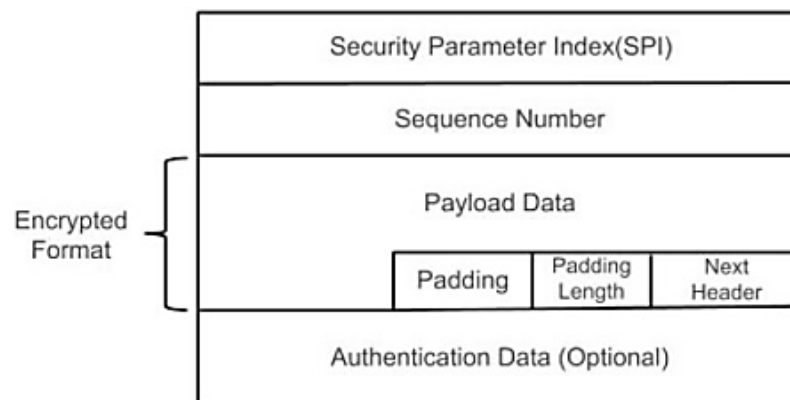
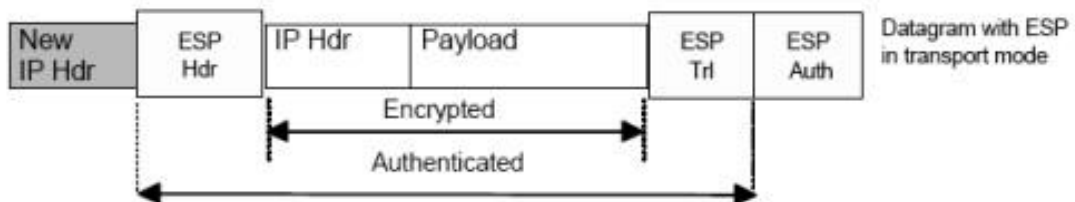
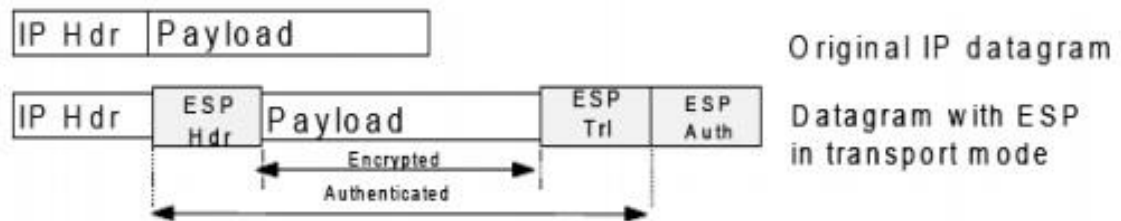
У IPsec використовуються три основні протоколи:

- Заголовок автентифікації (Authentication Header, AH)
- Безпека інкапсульованого корисного навантаження (Encapsulated Security Payload, ESP)
- Обмін ключами в Інтернеті (Internet Key Exchange, IKE)

AH слугує для підтвердження цілісності повідомлення, автентифікації джерела (які забезпечує використання HMAC) і захисту від повторного відтворення (яке забезпечується за допомогою поля порядкового номера із заголовком AH).



Протокол ESP забезпечує конфіденційність даних і автентифікацію. ESP можна використовувати лише з конфіденційністю, лише з автентифікацією або як з конфіденційністю, так і з автентифікацією. Різниця в автентифікації в протоколах AH та ESP полягає в охопленні даних: так, AH автентифікація автентифікує весь пакет, а ESP — його частину.

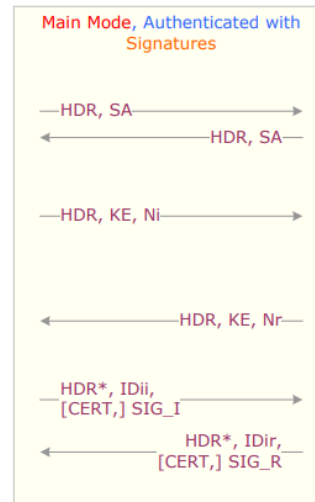
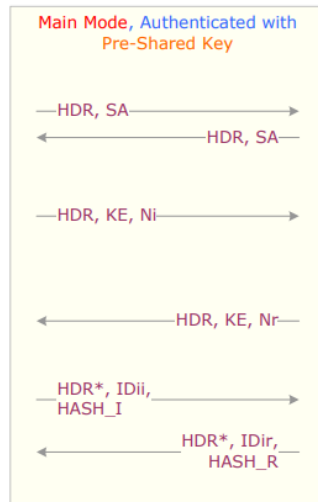


IKE (Internet Key Exchange) - це протокол обміну ключами, який використовується для автоматизації процесу встановлення безпеки в IPSec. В основному, IKE використовується разом з протоколом ISAKMP (Internet Security Association and Key Management Protocol). Протокол IKE включає дві фази роботи: Main mode і Quick (Aggressive) mode. Основна мета першої фази - це узгодження параметрів та обмін ключами для безпеки взаємодії. Друга фаза призначена для встановлення *Security Associations (SA)* для встановлення тунелю для передачі даних. SA визначає наступні елементи: протокол безпеки, алгоритми шифрування та гешування, ключі, атрибути безпеки, ідентифікатори сторін тощо. SA має обмежений "життєвий цикл" (SA Lifetime), після закінчення якого відбувається регенерація ключів і оновлення параметрів безпеки.

Encryption Algorithm : 3DES-CBC
 Hash Algorithm : SHA
 Authentication Method : Pre-Shared Key
 DH Group : 1024-bit MODP
 Life Type : Seconds
 Life Duration : 3600

ISAKMP HDR
 Initiator Cookie : CKY-I
 Responder Cookie : CKY-R
 Next Payload : 4 (KE)
 Exchange Type : 2 (Main Mode)
 Flags : -
 KE Payload
 Next Payload : 10 (NONCE)
 Key Exchange Data : g^{ax} (DH Public Value)
 NONCE Payload (Ni)
 Next Payload : 0
 Nonce Data : nonce_i

$hash_i = \text{prf}(\text{SKEYID}, g^{ax} | g^{bx} | \text{CKY-I} | \text{CKY-R} | \text{SAI}_b | \text{IDi}_b)$
 ISAKMP HDR
 Initiator Cookie : CKY-I
 Responder Cookie : CKY-R
 Next Payload : 5 (ID)
 Exchange Type : 2 (Main Mode)
 Flags : Encrypted
 ID Payload (IDi)
 Next Payload : 8 (HASH)
 ID Type : 1 (ID_IPV4_ADDR)
 Protocol ID : -
 Port : -
 Identification Data : id_isakmp_i
 HASH Payload (HASH_I)
 Next Payload : 0
 Hash Data : hash_i



Encryption Algorithm : 3DES-CBC
 Hash Algorithm : MD5
 Authentication Method : Pre-Shared Key
 DH Group : 1024-bit MODP
 Life Type : Seconds
 Life Duration : 3600

ISAKMP HDR
 Initiator Cookie : CKY-I
 Responder Cookie : CKY_R
 Next Payload : 4 (KE)
 Exchange Type : 2 (Main Mode)
 Flags : -
 KE Payload
 Next Payload : 10 (NONCE)
 Key Exchange Data : g^{ax} (DH Public Value)
 NONCE Payload (Nr)
 Next Payload : 0
 Nonce Data : nonce_r

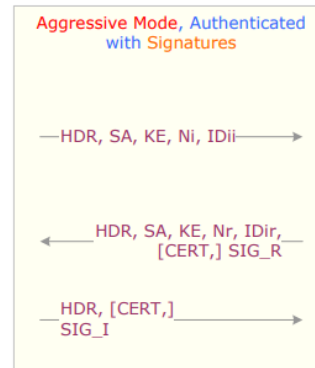
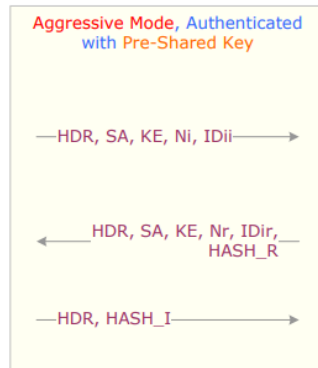
$hash_r = \text{prf}(\text{SKEYID}, g^{ax} | g^{bx} | \text{CKY-I} | \text{CKY-R} | \text{SAI}_b | \text{IDr}_b)$
 ISAKMP HDR
 Initiator Cookie : CKY-I
 Responder Cookie : CKY-R
 Next Payload : 5 (ID)
 Exchange Type : 2 (Main Mode)
 Flags : Encrypted
 ID Payload (IDr)
 Next Payload : 8 (HASH)
 ID Type : 1 (ID_IPV4_ADDR)
 Protocol ID : -
 Port : -
 Identification Data : id_isakmp_r
 HASH Payload (HASH-R)
 Next Payload : 0
 Hash Data : hash_r

$\text{SKEYID} = \text{prf}(\text{pre-shared-key}, \text{Ni}_b | \text{Nr}_b)$

$\text{SKEYID}_d = \text{prf}(\text{SKEYID}, g^{ax} | \text{CKY-I} | \text{CKY-R} | 0)$
 $\text{SKEYID}_a = \text{prf}(\text{SKEYID}, \text{SKEYID}_d | g^{ax} | \text{CKY-I} | \text{CKY-R} | 1)$
 $\text{SKEYID}_e = \text{prf}(\text{SKEYID}, \text{SKEYID}_a | g^{ax} | \text{CKY-I} | \text{CKY-R} | 2)$

$hash_1 = \text{prf}(\text{SKEYID}_a, \text{M-ID} | \text{SA} | \text{Ni} | \text{KE})$

$hash_3 = \text{prf}(\text{SKEYID}_a, 0 | \text{M-ID} | \text{Ni}_b | \text{Nr}_b)$



$hash_2 = \text{prf}(\text{SKEYID}_a, \text{M-ID} | \text{Ni}_b | \text{SA} | \text{Nr} | \text{KE})$

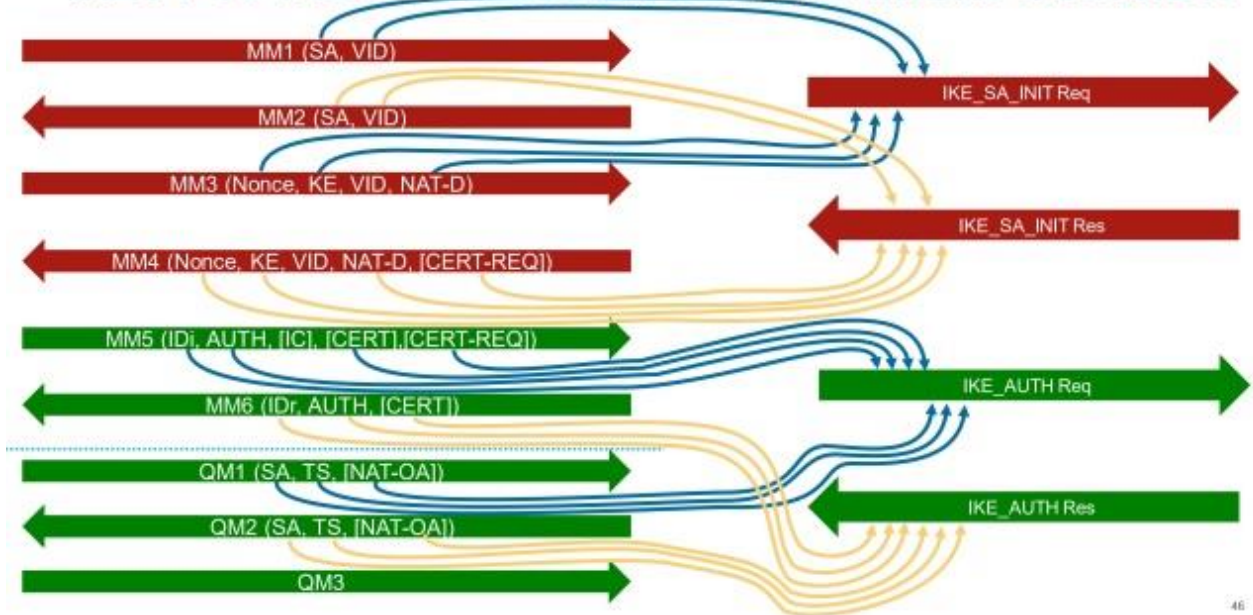
Основні відмінності IKEv2 від IKEv1:

- Зменшення кількості обмінів для встановлення SA;
- вбудована підтримка обходу трансляції мережевих адрес NAT-T;
- підтримка MOBIKE (Mobility and Multi-homing Protocol);
- підтримка EAP (Extensible Authentication Protocol) автентифікації;
- підтримка протоколу IPv6;
- певний рівень захисту від DoS атак;

Kerberosized Internet Negotiation of Keys (KINK):

- централізоване управління політиками безпеки;
- автентифікацію однорангових користувачів виконує довірена третя сторона – Центр Розподілу Ключів;

IKEv1 vs IKEv2 – Session Establishment Overview



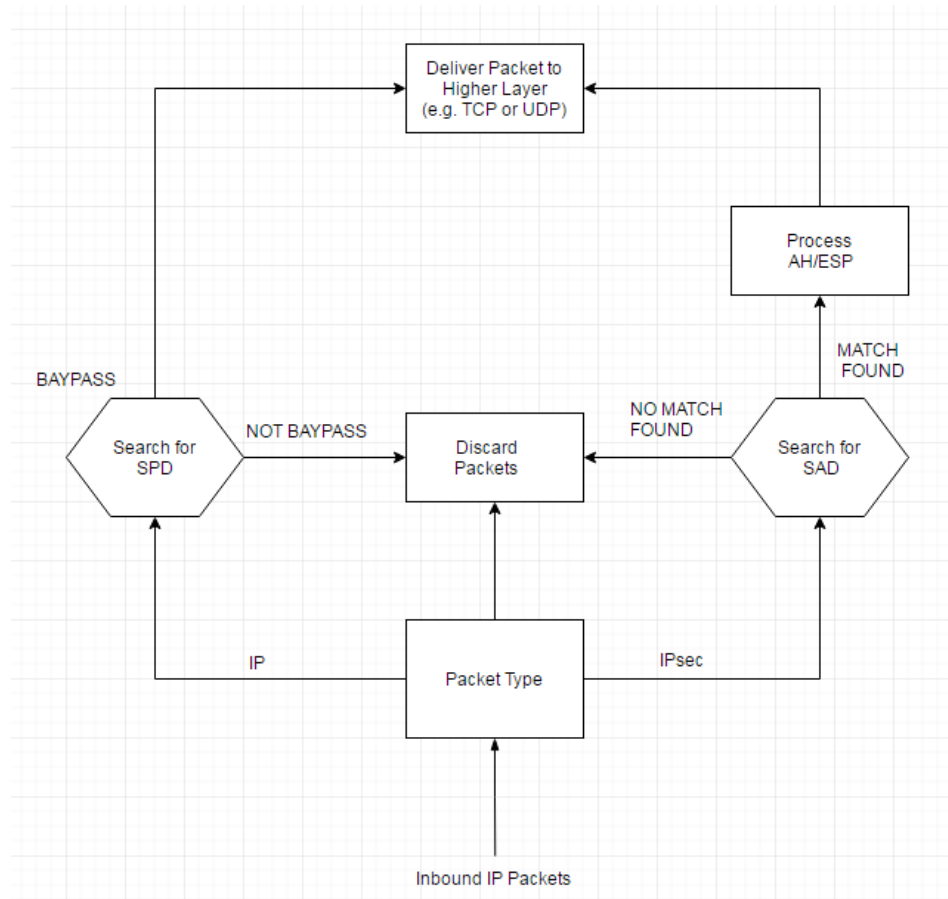
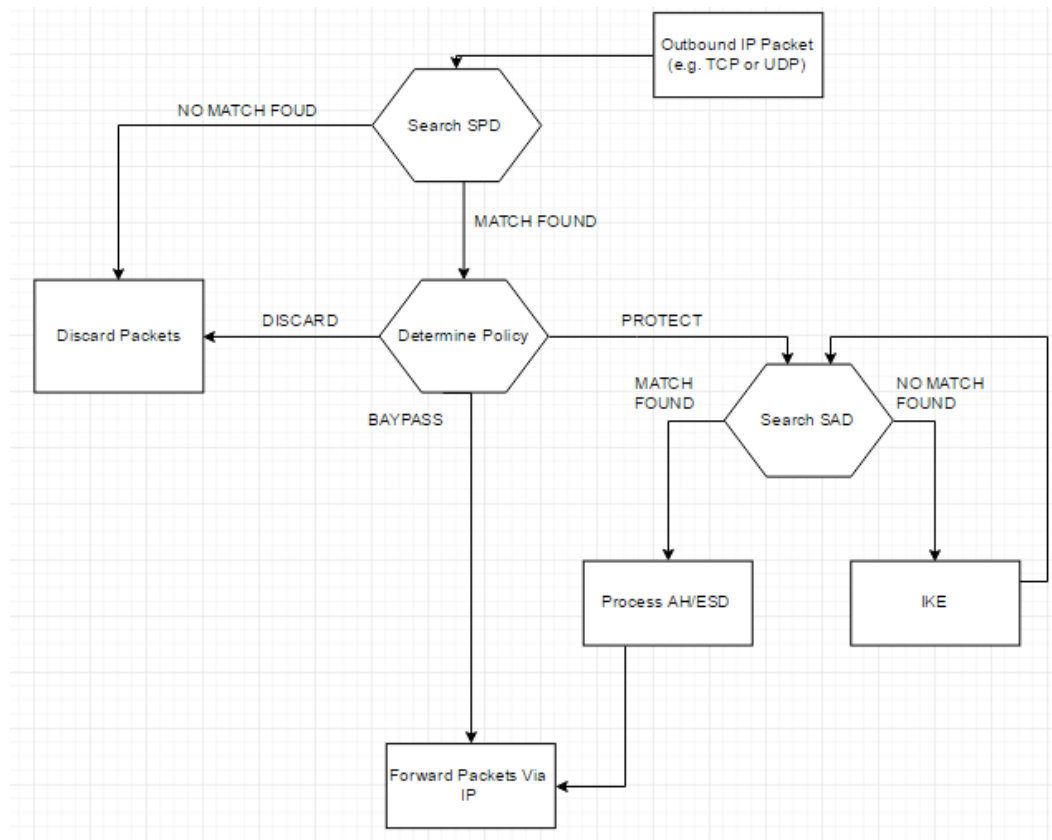
Security Association Database (SAD) – це таблиця, яка зберігає інформацію про активні SA вхідного та вихідного трафіку. SAD заповнюється динамічно під час процесу встановлення безпеки, зокрема, після встановлення SA. Кожна SA ідентифікується трьома параметрами:

- Security Parameters Index, SPI
- Destination Address
- Ідентифікатор протокола безпеки (ESP або AH)

В SAD зберігаються наступні дані:

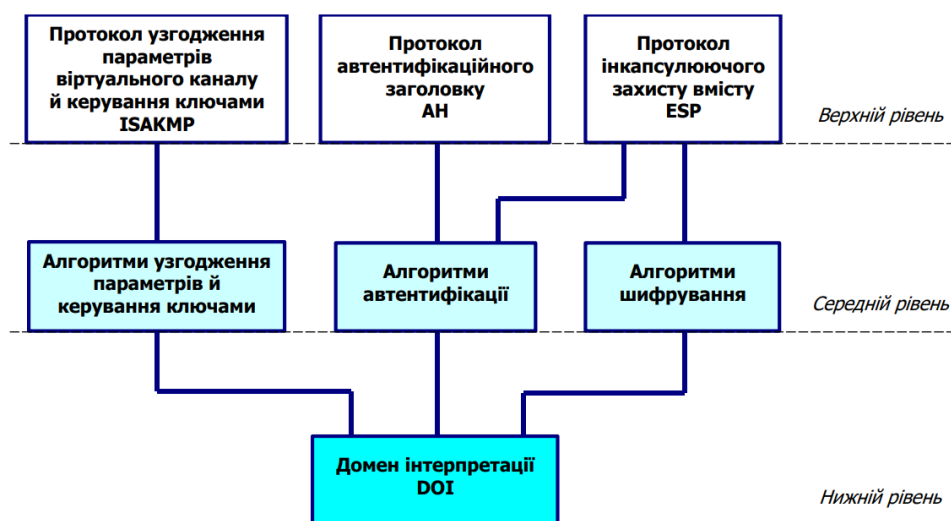
- Security Parameter Index
- Destination Address
- Sequence Number
- Anti-Replay Window
- IP Security Protocol
- Algorithm
- Key
- SA Lifetime
- IPSec

Security Policy Database (SPD) є впорядкованим набором правил і політик безпеки. SPD фільтрує IP-трафік, щоб визначити, як потрібно обробляти пакети. Для вихідних пакетів SPD і SAD визначають, який рівень захисту застосовувати. Для вхідних пакетів SPD допомагає визначити, чи прийнятний рівень захисту пакета.



Архітектура засобів захисту IPsec:

- Верхній рівень: протоколи захисту віртуального каналу і узгодження параметрів захисту;
- Середній рівень: криптографічні алгоритми, що використовуються в протоколах АН та ESP, алгоритми узгодження і керування ключами, які використовує протокол IKE;
- Нижній рівень: домен інтерпретації (DOI) – база даних, яка містить інформацію про усі протоколи і алгоритми, що застосовуються в IPsec, а також про їхні параметри, ідентифікатори тощо.



Криптографічні алгоритми в IPsec

Обмін ключами	Автентифікація	Гешування	Шифрування
DH, ECDH	PSA, PSK, ECDSA	HMAC – SHA2	AES-GCM, ChaCha20-Poly1305

Особливості основних схем застосування протоколів IPsec для встановлення VPN-тунелю:

Тип з'єднання	Особливості	Приклад використання
Хост-хост	Кожен хост є кінцевим пунктом VPN-тунелю. Обидва хости повинні бути налаштовані для підтримки IPsec.	Забезпечення безпеки комунікації між конкретними комп'ютерами.
Шлюз-шлюз	VPN-тунель між двома мережами через їхні шлюзи. Кожен шлюз повинен підтримувати IPsec.	Безпечне з'єднання двох віддалених мереж через Інтернет.
Хост-шлюз	Один чи кілька хостів підключаються до центрального шлюзу. Кожен хост та шлюз повинні підтримувати IPsec.	Забезпечення безпеки комунікації між індивідуальним комп'ютером та центральним шлюзом, наприклад, в корпоративних мережах або VPN.