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

Виконали:
Студенти групи ФІ-22 мн

Ковальчук Ольга
Коломієць Андрій
Толмачов Євгеній

Київ – 2024

Мета та основні завдання роботи

Дослідження особливостей реалізації криптографічних механізмів протоколів IPSec.

Вимоги

Провести дослідницьку роботу з метою аналізу особливостей реалізації криптографічних механізмів протоколів IPSec. Описати основне призначення протоколів IPSec, їх місце в мережевій моделі OSI та взаємодію зі стеком протоколів TCP/IP та ін.

Дослідити архітектуру стеку протоколів IPSec. Описати призначення, особливості та відмінності криптографічних механізмів протоколів AH, ESP, ISAKMP, IKE, IKEv2, KINK та ін. Проаналізувати концепцію безпечних асоціацій (SA), її особливості та бази даних SPD і SAD (їх призначення та способи заповнення і використання). Дослідити детально особливості структури заголовків протоколів AH і ESP в тунельному та транспортному режимах з повним описанням їх полів та можливих значень. Визначити особливості обробки вхідних та вихідних IPSec-пакетів для кожного з протоколів та режимів.

Дослідити нижній рівень архітектури стеку протоколів IPSec – домен інтерпретації DOI. Визначити зареєстровані алгоритми автентифікації, шифрування, геш-функцій та ін. криптографічних алгоритмів для стеку протоколів IPSec.

Визначити та описати особливості основних схем застосування протоколів IPSec: хост-хост, шлюз-шлюз та хост-шлюз. А також використання протоколів IPSec для побудови VPN-тунелів.

Виконання комп'ютерного практикуму

IP Sec (Internet Protocol Security) — це стандартний набір протоколів Internet Engineering Task Force (IETF) між двома точками зв'язку в мережі IP, які забезпечують автентифікацію даних, цілісність і конфіденційність.

Існує два режими, в яких можна застосовувати IPSec для роботи в мережі, які називаються **транспортним режимом** і **тунельним режимом**. У *тунельним режимі* весь вихідний IP-пакет (заголовок і корисне навантаження (payload)) шифрується, після чого він інкапсулюється в новий IP-пакет. Цей новий пакет має інший IP-заголовок, зазвичай із винятковим джерелом і одержувачем, поміченими на його IP-адресах. Тунельний режим зазвичай використовується у VPN типу «сайт-веб-сторінка», у яких цілі мережі або підмережі повинні безпечно спілкуватися через ненадійну мережу, включаючи Інтернет. Транспортний режим шифрує лише корисне навантаження (payload) автентичного IP-пакета, залишаючи IP-заголовок недоторканим. Зазвичай використовується для наскрізного зв'язку між хостами або гаджетами.

У IPSec розрізняються наступні **компоненти**:

- Два протоколи безпеки: IP Authentication Header (AH) і IP Encapsulating Security Payload (ESP), які забезпечують механізми безпеки для захисту IP-трафіку.
- Протокол керування ключами Internet Key Exchange (IKE), який дозволяє двом вузлам узгоджувати ключі та всі параметри, необхідні для встановлення з'єднання AH або ESP.

Authentication Header (AH)

Протокол AH — це процедура, передбачена в IPSec для забезпечення цілісності та автентифікації IP-датаграм (datagrams). Тобто, він надає одержувачу IP-пакетів засіб для автентифікації джерела даних і перевірки того, що дані не були змінені під час передачі. Однак

він не дає жодної гарантії конфіденційності, тобто передані дані можуть переглядати треті особи.

AH — це заголовок автентифікації, який вставляється між стандартним заголовком IP (як IPv4, так і IPv6) і транспортованими даними, які можуть бути повідомленнями TCP, UDP або ICMP або навіть повною датаграмою IP, як показано на малюнку:

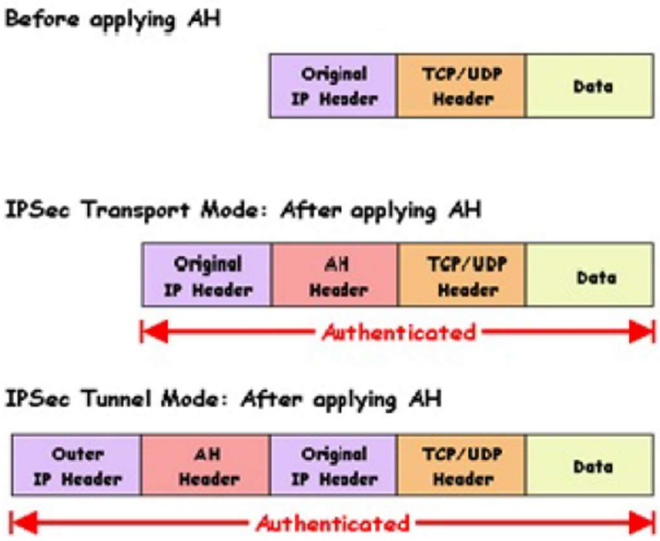
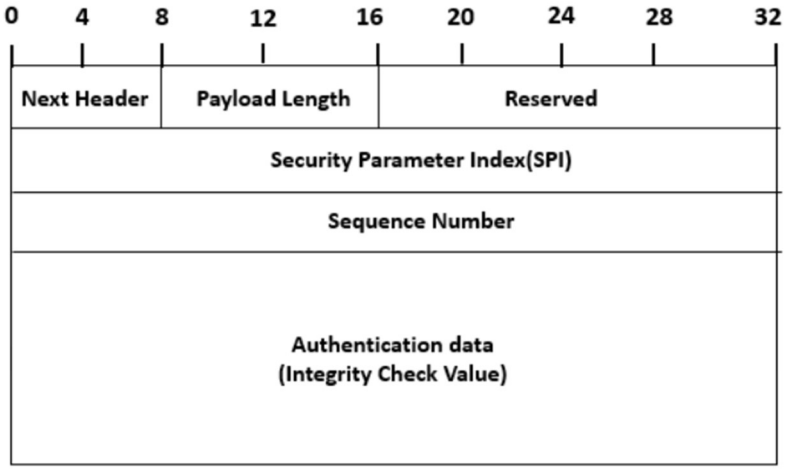


Рис 1. Структура AH датаграми

Формат заголовка автентифікації (AH)

Всього в заголовку автентифікації 6 полів:

1) Наступний заголовок (Next Header)
2) Довжина корисного навантаження (Payload Length)
3) Зарезервований (Reserved)
4) Індекс параметрів безпеки (SPI)
5) Порядковий номер (Sequence Number)
6) Дані автентифікації (Authentication Data)



Формат AH

Розглянемо кожен елемент більш детально.

1) **Next Header**: це 8-розрядне поле використовується для визначення типів заголовків, які слідують безпосередньо за заголовком автентифікації. Наприклад, якщо заголовок ESP

слідує за AH, це поле містить 50 як значення; інакше, якщо інший AH слідує за цим AH, він містить 51 як значення.

2) **Payload Length**: це поле має 8 біт. Довжина корисного навантаження – це довжина заголовка автентифікації, і тут ми використовуємо коефіцієнт масштабування 4. Яким би не був розмір заголовка, розділіть його на 4, а потім відніміть 2. Ми віднімаємо 2, оскільки не враховуємо перші 8 байтів. Наприклад, якщо довжина корисного навантаження дорівнює X. Тоді (X+2)*4 буде вихідною довжиною заголовка автентифікації.

3) **Reserved** – це 16-бітне поле, яке відправник встановлює на «нуль», оскільки це поле зарезервовано для майбутнього використання.

4) **Індекс параметрів безпеки (SPI)**: це поле має 32 біти. Він використовується в поєднанні з адресою джерела та адресою призначення та протоколом IPsec, унікально ідентифікуючи асоціацію безпеки (SA) для трафіку, до якого належить датаграма.

5) **Sequence Number** – це 32-бітове поле без знаку містить значення лічильника, яке збільшується на одиницю для кожного надісланого пакету. Кожному пакету потрібен порядковий номер. Він почнеться з 0 і продовжуватиметься до (2^{32} – 1) і не буде циклу. Скажімо, якщо всі порядкові номери закінчилися, і нічого з них не залишилося, то ми не можемо виконати перенесення, оскільки це заборонено. Отже, ми завершимо з'єднання та знову встановимо з'єднання, щоб відновити передачу решти даних із порядкового номера 0. В основному порядкові номери використовуються для запобігання атаки відтворення.

6) **Authentication Data:** є полем змінної довжини, яке містить значення перевірки цілісності (ICV) для пакета. Використовуючи алгоритм хешування та секретний ключ, відправник створить дайджест повідомлення, який буде надіслано одержувачу. З іншого боку, отримувач використовуватиме той самий алгоритм хешування та секретний ключ. Якщо обидва дайджести повідомлень збігаються, отримувач прийме дані. В іншому випадку одержувач відхилить його, сказавши, що це повідомлення було змінено між ними. Таким чином, дані автентифікації використовуються для перевірки цілісності передачі. Також довжина даних автентифікації залежить від обраного вами алгоритму хешування.

AH використовує алгоритми, відомі як хешовані коди автентифікації повідомлень (**Hashed Message Authentication Codes**, **HMAC)**. Цей алгоритм полягає в застосуванні хеш-функції до комбінації вхідних даних і ключа, а виводом є невеликий рядок символів, який ми називаємо екстрактом. Цей екстракт має наступну властивість: він схожий на особистий слід, пов'язаний з даними та особою, яка їх створила, оскільки вона єдина, хто знає ключ.

Encapsulating Security Payload (ESP)

Основною метою протоколу ESP є забезпечення конфіденційності шляхом визначення способу шифрування даних, які мають бути надіслані, і способу включення цього зашифрованого вмісту в IP-датаграму. Крім того, він може запропонувати цілісність даних і послуги автентифікації, використовуючи механізм, подібний до AH.

Оскільки ESP надає більше функцій, ніж AH, формат заголовка складніший. Цей формат складається із заголовка та хвоста, які оточують дані, що транспортуються. Такими даними може бути будь-який IP-протокол (наприклад, TCP, UDP або ICMP або навіть повний IP-пакет). На рисунку 2 показано структуру датаграми ESP, яка показує, як вміст або корисне навантаження переміщуються в зашифрованому вигляді.

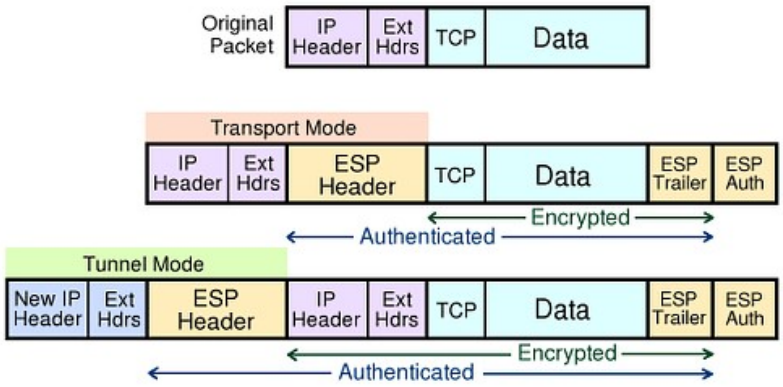
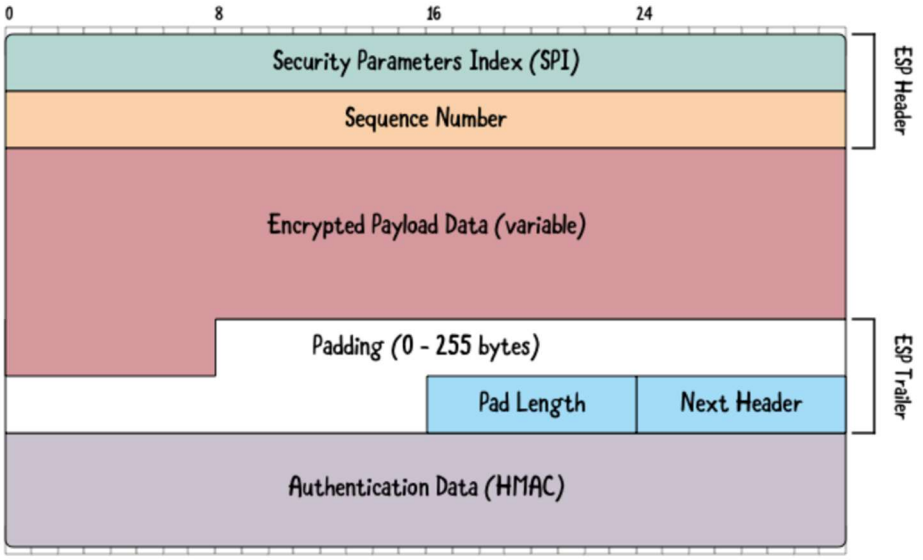


Рис 2. Структура ESP

Формат ESP



1) **SPI:** 32-розрядне значення, яке встановлює асоціацію безпеки для цього пакета.
2) **Sequence Number**: монотонно зростаюче число для кожного надісланого пакета, щоб запобігти атакам відтворення.
3) **Encrypted Payload Data**: дані/контент, захист яких забезпечується методом шифрування.
4) **Padding**: до 255 байт заповнення
5) **Pad Length:** кількість байтів pad, що безпосередньо передують цьому полю.
6) **Next Header**: тип заголовка безпосередньо після AH. IP – 4, TCP – 6, UDP – 17 тощо.
7) **Authentication Data**: MAC пакета, обчислений за допомогою SHA-1 або HMAC. Дані автентифікації є необов'язковим полем, яке можна застосувати, лише якщо вибрано SA. Це служить меті забезпечення цілісності

Internet Key Exchange (IKE)

IPsec використовує IKE як протокол за замовчуванням для керування та передачі алгоритмів, ключів і протоколів, а також для перевірки обох сторін. Він використовується для встановлення асоціацій безпеки. Важливою концепцією IPSec є ***асоціація безпеки (SA):*** це односпрямований канал зв'язку, який з'єднує два вузли, через які захищені датаграми проходять через попередньо узгоджені криптографічні механізми. Ідентифікуючи лише один

односпрямований канал, з'єднання IPSec складається з двох SA, по одному для кожного значення зв'язку. Поки що передбачалося, що обидва кінці асоціації безпеки повинні знати ключі, а також іншу інформацію, необхідну для надсилання та отримання датаграм AH або ESP. Як зазначено вище, необхідно, щоб обидва вузли узгодили як криптографічні алгоритми, які будуть використовуватися, так і параметри керування. Цю операцію можна виконати за допомогою ручної конфігурації або деякого протоколу керування, який відповідає за автоматичне узгодження необхідних параметрів; Ця операція називається *узгодженням SA*.

IETF визначив протокол IKE для виконання як функції автоматичного керування ключами, так і встановлення відповідних SA. Важливою особливістю IKE є те, що його утиліта не обмежується IPSec, а є стандартним протоколом керування ключами, який може бути корисним в інших протоколах, таких як OSPF або RIPv2. IKE — це гібридний протокол, який є результатом інтеграції двох взаємодоповнюючих протоколів: ISAKMP і Oakley. ISAKMP узагальнено визначає протокол зв'язку та синтаксис повідомлень, які використовуються в IKE, тоді як Oakley визначає логіку безпечного обміну ключем між двома частинами, які раніше не були відомі.

IKE v1 (1998 р)

Оригінальна версія IKE встановлює захищені канали зв'язку в два етапи: етап 1 і етап 2 (або фаза).

На **<u>етапі 1</u>** автентифіковане з'єднання між хостом і користувачем встановлюється за допомогою спільного ключа або цифрового сертифіката. Мета полягає в тому, щоб захистити зв'язок, який відбувається на етапі 2. Алгоритм обміну ключами Діффі-Хеллмана створює безпечний канал зв'язку автентифікації. Цей метод цифрового шифрування використовує числа, доведені до певних ступенів, для створення ключів дешифрування. Результатом узгодження мають бути ключі сеансу та одна двонаправлена SA.

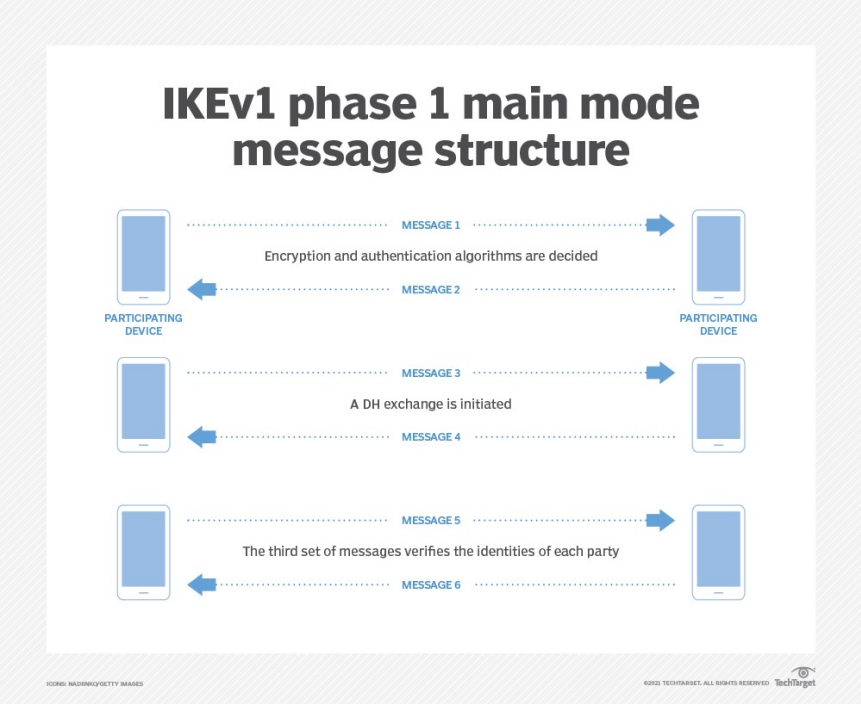
Фаза 1 працює в одному з двох режимів: ***основний режим*** або ***агресивний режим***. **Основний режим** полягає в тому, що обидві сторони надсилають три двосторонні обміни, що загалом дорівнює шести повідомленням. Перші два повідомлення підтверджують алгоритми шифрування та автентифікації. Другий набір із двох повідомлень починає обмін ключами Діффі-Хеллмана, де обидві сторони надають випадкове число. Третій набір повідомлень перевіряє особистість кожної сторони.

Агресивний режим виконує те саме завдання, що й основний режим, але робить це лише за два обміни трьома повідомленнями. У той час як основний режим захищає особистість обох сторін шляхом їх шифрування, агресивний режим цього не робить.

<u>Етап 2</u> IKE узгоджує SA для захисту даних, які передаються через IPsec, використовуючи захищений канал, створений на етапі 1. Результатом є мінімум дві односпрямовані SA. Обидві сторони також обмінюються пропозиціями щодо визначення того, який параметр безпеки використовувати в SA.

Етап 2 працює лише в одному режимі: швидкому. Швидкий режим надає три ресурси: ідентифікатори проксі-сервера, повну секретність (PFS) і захист від повторного відтворення. Ідентифікатори проксі кожного учасника надаються один одному. PFS надає ключі незалежно від попередніх ключів. Захист від повторів — це метод захисту від атак відтворення.

Основний і агресивний режими, виявлені у фазі 1, <u>застосовуються лише</u> до IKE v1, а не до IKE v2.



Приклад структури основного режиму IKE v1.

IKE v2 (2005 р, оновлений у 2014 р)

IKEv2 узгоджує та автентифікує IPsec SA і забезпечує безпечні канали зв'язку VPN між пристроями. Ця версія не включає фази 1 або 2, як її попередниця, але обмін повідомленнями все ще узгоджує тунель IPsec. Перше з чотирьох повідомлень – це переговори щодо визначення атрибута безпеки. Друге повідомлення – кожна сторона засвідчує свою особу. Третє включає створення додаткових SA. Четверте повідомлення видаляє зв'язки SA, виявляє активність тунелю IPsec і повідомляє про помилки.

Удосконалення IKEv2 порівняно з IKEv1 такі:

- вимагає меншої пропускної здатності;
- вимагає менше криптографічних механізмів для захисту пакетів;
- вимагає лише одного початкового механізму обміну чотирма повідомленнями;
- підтримує мобільні платформи, включаючи смартфони;
- підтримує захист трафіку Stream Control Transmission Protocol (SCTP);
- забезпечує більшу стійкість до атак типу DoS;
- оснащений вбудованим обходом Network Address Translation (NAT), необхідним для підтримки маршрутизаторів, які виконують трансляції;
- автоматично визначає, чи працює тунель IPsec, щоб IKE міг автоматично відновити з'єднання, якщо потрібно;
- вмикає фрагментацію повідомлень і дозволяє IKE v2 працювати в областях, де фрагменти IP можуть бути заблоковані, а SA може не встановити;
- дозволяє змінювати ключі для створення нових ключів для SA.

Kerberized Internet Negotiation of Keys (KINK)

Kerberized Internet Negotiation of Keys (KINK) — це протокол, розроблений для встановлення безпечного та масштабованого керування ключами між комунікуючими об'єктами в централізовано керованому середовищі, підтримуючи послідовні політики безпеки. Цілі безпеки включають конфіденційність, автентифікацію та захист від повторного

відтворення повідомлень керування ключами, зосереджуючись на уникненні вразливості відмови в обслуговуванні. Протокол націлений на низьку обчислювальну вартість, низьку затримку та невелику площу, зводячи до мінімуму використання операцій із відкритим ключем.

KINK використовує механізм автентифікації Kerberos, відомий своєю ефективністю в автентифікації клієнт-сервер за допомогою надійної сторонньої моделі. Клієнти отримують квитки від Центру розповсюдження ключів (KDC) для автентифікації, а KINK використовує цю властивість для розповсюдження ключів для асоціацій безпеки (SA) IPsec.

Працюючи як протокол команд/відповідей, KINK може створювати, видаляти та підтримувати IPsec SA. Кожна команда або відповідь включає загальний заголовок і корисні навантаження тип-довжина-значення, причому тип обмежує корисні навантаження, що обмінюються. На відміну від IKE, KINK не має стану, усуваючи потребу у жорсткому зберіганні стану для кожної команди чи відповіді.

KINK використовує механізми Kerberos для взаємної автентифікації та захисту від відтворення, забезпечуючи конфіденційність для корисних навантажень після корисного навантаження Kerberos AP-REQ під час встановлення SA. Протокол пом'якшує атаки на відмову в обслуговуванні, вимагаючи автентифікованих обмінів перед будь-якими операціями з відкритим ключем або встановленням стану. KINK також підтримує використання механізмів Kerberos User-to-User, особливо у випадках, коли немає спільного ключа між сервером і KDC, як це видно в однорангових вузлах IPsec, які використовують PKINIT для початкової автентифікації.

KINK безпосередньо повторно використовує корисні навантаження швидкого режиму IKE з деякими незначними змінами та пропусками. У більшості випадків обміни KINK - це одна команда та її відповідь. Додаткове третє повідомлення потрібне під час створення SA, лише якщо відповідач відхиляє першу пропозицію від ініціатора або хоче внести ключові матеріали (секретні ключі (невизначеного) формату, довжини та кількості). KINK також забезпечує зміну ключа та виявлення мертвих однорангових вузлів.

Security Association Database (SAD)

База даних асоціації безпеки (SAD) — це центральне сховище, що містить усі активні SA для вхідного та вихідного трафіку, причому кожен запис визначає параметри для конкретного SA.

Зазвичай запис SA містить таку інформацію:

Індекс параметра безпеки	унікальний ідентифікатор, згенерований творцем SA, який використовується для розрізнення SA протоколу IPsec, що завершується на тому самому вузлі призначення.
Адреса призначення	адреса вузла призначення, до якого застосовується цей запис SA.
Лічильник	для генерування порядкових номерів.
Вікно Anti-Replay	лічильник і інформація про співставлення, щоб визначити, чи пакет відтворюється повторно.
IP-протокол безпеки	тип протоколу IP-безпеки, який використовується для обробки пакетів. Можна вказати або Authentication Header (AH), або Encapsulating Security Payload (ESP).

Алгоритм	алгоритм, який використовується протоколом безпеки IP, визначеним параметром протоколу безпеки IP.
Ключ	ключ, який використовується алгоритмом, указаним у параметрі Algorighm.
Термін служби SA	виражається або в часі, або в кількості байтів. Після закінчення терміну служби SA потрібно замінити новим SA та новим SPI, інакше SA припиняється.
Режим роботи протоколу IPsec	Тунельний режим або Транспортний режим.

The Security Policy Database (SPD)

База даних політики безпеки (SPD) містить набір правил, які визначають, чи підлягає пакет обробці IPsec, і керують деталями обробки. Кожен запис у SPD представляє політику, яка визначає, як буде оброблятися набір трафіку, охопленого цією політикою. Будь-який вхідний або вихідний пакет обробляється одним із трьох способів: відхилення, виконання обробки IPsec або обхід обробки IPsec. Запис політики SPD містить SA або специфікацію пакета SA для трафіку, який підлягає обробці IPsec. Пакет SA відноситься до набору SA, які слід застосовувати в порядку, коли обробляється відповідний трафік.

Зіставлення пакета із записом політики здійснюється за допомогою селектора, який функціонує як ключ пошуку. *Селектор* — це набір полів IP і протоколу верхнього рівня, які відображають потік трафіку в політиці безпеки в SPD.

Можливі поля для створення селектора:

• Адреса джерела

• Адреса призначення

• Протокол транспортного рівня

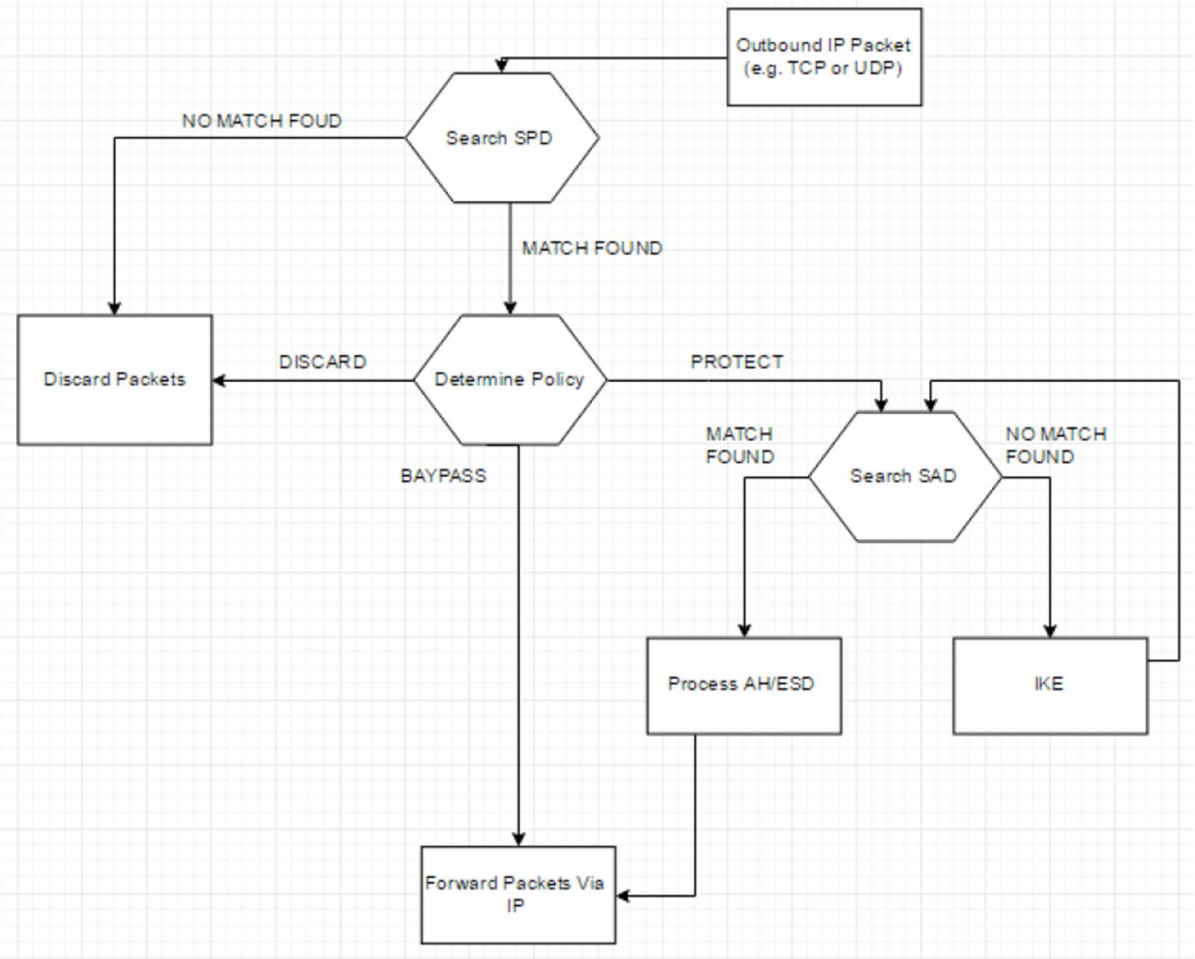
• Порти протоколу джерела та призначення

• Ідентифікатор користувача або ім’я системи, представлене ім’ям X.500 або FQDN.

Загалом кожен **запис політики в SPD** містить таку інформацію: Діапазон адрес джерела Адреса джерела пакета.

Оскільки SA застосовується до певного напрямку потоку трафіку, кожна політика безпеки в SPD має атрибут напрямку, який вказує, чи застосовується політика до вхідного чи вихідного трафіку.

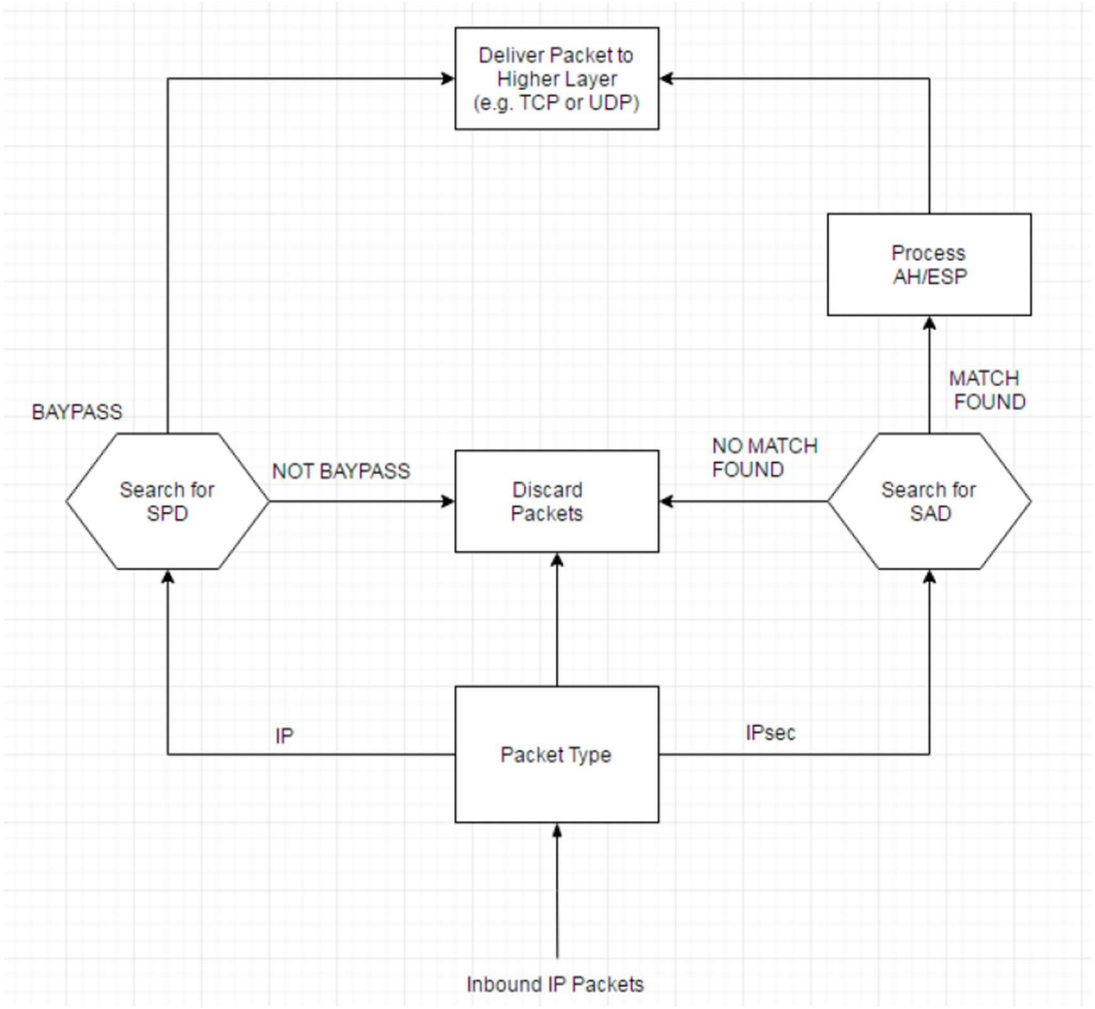
Схема роботи IP Sec для вихідних пакетів



Порядок дій:

1) IPSec знаходить перший збіг (на основі srcAddress,srcPort,dstAddress,dstPort) у Базі даних політики безпеки (SPD)
2) Якщо політика вимагає захисту, IPSec зіставляє пакет із правильною асоціацією безпеки (SA) у Базі даних асоціації безпеки (SAD)
3) Якщо SA не існує, IPSec викликає службу IKE, щоб створити пару SA
4) Якщо SA існує, пакет зашифровано/автентифіковано

Схема роботи IP Sec для вхідних пакетів



Для вхідних пакетів IPSec:

- IPSec шукає вхідний SA у SAD на основі SPI (індекс параметрів безпеки) (цим обмінюються відправник і одержувач під час початкового узгодження, і він міститься в пакеті IPSec)
- IPSec обробляє (дешифрує/автентифікує) пакет на основі SA

Для вхідних пакетів не IPSec:

- IPSec знаходить першу відповідну політику в SPD і перевіряє, чи дія є BYPASS; якщо ні, пакет відкидається.

Рівні архітектури IPSec

Верхній рівень –протоколи захисту віртуального каналу і узгодження параметрів захисту

 Протоколи AH та ESP не залежать від конкретних алгоритмів шифрування й автентифікації. Можуть застосовуватись різні:

- методи автентифікації
- типи ключів
- алгоритми шифрування та розподілу ключів

 Протоколи AH та ESP зареєстровані організацією IANA (Internet Address Naming Authority) під номерами 51 та 50, відповідно

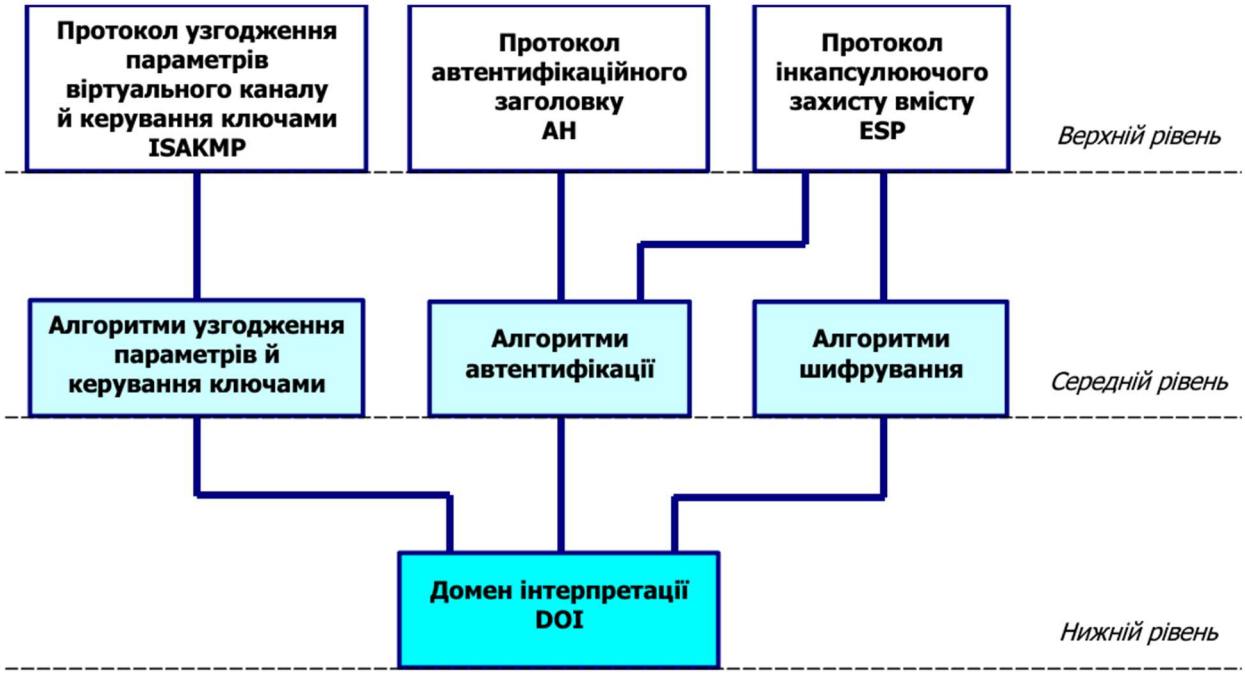
Середній рівень –криптографічні алгоритми, що використовуються в протоколах AH та ESP, а також певні алгоритми узгодження і керування ключами, які використовує протокол ISAKMP

Нижній рівень–так званий "домен інтерпретації" (Domain of Interpretation, DOI)

 Це, фактично, база даних, яка містить інформацію про усі протоколи і алгоритми, що застосовуються в IPSec, а також про їхні параметри, ідентифікатори тощо

 Наявність такої бази пояснюється тим, що відкрита архітектура IPSec припускає застосування протоколів і алгоритмів, які не розроблялись для неї чи з урахуванням її вимог

 Необхідною умовою застосування сторонніх алгоритмів автентифікації або шифрування (наприклад, тих, що відповідають національним стандартам) є реєстрація їх у домені інтерпретації



Криптографічні алгоритми в IPsec

Шифрування	HMAC-SHA1/SHA2 для захисту цілісності та автентичності. TripleDES-CBC для конфіденційності AES-CBC і AES-CTR для конфіденційності. AES-GCM і ChaCha20-Poly1305 забезпечують ефективну конфіденційність і автентифікацію.
Обмін ключами	Diffie–Hellman, ECDH (Діффі-Хелман на еліптичних кривих)
Автентифікація	RSA, ECDSA (Elliptic Curve Digital Signature Algorithm),

	PSK (pre-shared key), EdDSA (Edwards-curve Digital Signature Algorithm)

Основні схеми застосування протоколів IPSec для встановлення VPN тунелю

Хост-хост (host-to-host):

- Кожен хост є кінцевим пунктом VPN тунелю.
- Потрібно, щоб обидва хости бути налаштовані для підтримки IPSec.

Використовується для: забезпечення безпеки комунікації між конкретними комп'ютерами.

Шлюз-шлюз (network-to-network):

- VPN−тунель між двома мережами через їхні шлюзи.
- Потрібно, щоб кожен шлюз підтримував IPSec.

Використовується для: безпечне з'єднання двох віддалених мереж через Інтернет.

Хост-шлюз (host-to-network):

- Один/декілька хостів підключаються до центрального шлюзу.
- Потрібно, щоб кожен хост та шлюз підтримував IPSec.

Використовується для: забезпечення безпеки комунікації між індивідуальним комп'ютером та центральним шлюзом (наприкл. в корпоративних мережах).

Джерела інформації

1. Al-khatib, A. A., & Hassan, R. (2018). Impact of IPSec Protocol on the Performance of Network Real-Time Applications: A Review. *Int. J. Netw. Secur.*, *20*(5), 811-819.
2. IP security (IPSec): https://www.geeksforgeeks.org/ip-security-ipsec/
3. IPsec (Internet Protocol Security) Tunnel and Transport Modes: https://www.geeksforgeeks.org/ipsec-internet-protocol-security-tunnel-and-transport-modes/
4. Authentication Header: https://www.educba.com/authentication-header/
5. Internet Protocol Authentication Header: https://www.geeksforgeeks.org/internet-protocol-authentication-header/
6. Encapsulating Security Payload: https://comp38411.jtang.dev/docs/ip-security/encapsulating-security-payload/
7. What is Encapsulating Security Payload: https://www.geeksforgeeks.org/what-is-encapsulating-security-payload/
8. Internet Key Exchange (IKE): https://www.techtarget.com/searchsecurity/definition/Internet-Key-Exchange
9. Kerberized Internet Negotiation of Keys (KINK) protocol:

   https://www.rfc-editor.org/rfc/rfc4430.html
10. Security Association Database:

    https://what-when-how.com/ipv6-advanced-protocols-implementation/security-association-database-ipv6-and-ip-security/
11. Архітектура засобів захисту IPSec: https://comsys.kpi.ua/upload/14.pdf