МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря Сікорського»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Проектування, розробка і реалізація криптографічних систем

“Дослідження реалізацій протоколів IPSec”

Виконали:

Студенти групи ФІ-22мн
Бондаренко Андрій
Яценко Артем

Київ – 2023

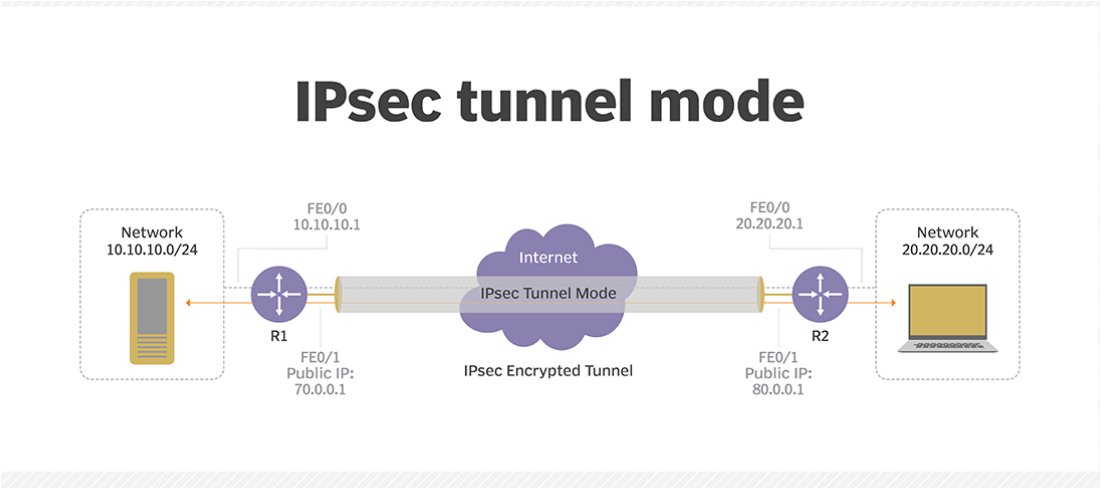
Мета: дослідження особливостей реалізації криптографічних механізмів протоколів IPSec.

Хід роботи

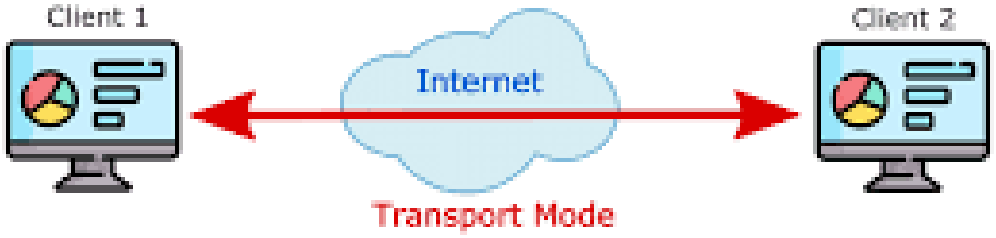
IPSec (Internet Protocol Security) - це стек протоколів і стандартів, що використовуються для захисту інтернет-зв'язку. Він працює на мережевому рівні, забезпечуючи як шифрування даних, так і автентифікацію, щоб гарантувати безпечну передачу даних. По суті, IPSec підвищує безпеку стандартного Інтернет-протоколу шляхом автентифікації джерела пакетів даних і шифрування самих даних. Це робить його особливо ефективним у VPN, де життєво важливо зберігати конфіденційність і цілісність даних, що передаються через незахищені мережі, такі як Інтернет. Розроблений у 1990-х роках Робочою групою з розробки інтернету (Internet Engineering Task Force, IETF), IPSec широко використовується для захищеного доступу віддалених користувачів до мереж, захисту з'єднань між сайтами та підвищення безпеки мобільного зв'язку.

IPsec працює в одному з двох режимів: **тунельний** або **транспортний**. Тунельний режим IPsec використовується переважно для забезпечення безпечного зв'язку між мережами, наприклад, у VPN, що з'єднують різні сайти. В цьому режимі, весь IP-пакет, включаючи як заголовок, так і корисне навантаження (payload), шифрується. Це створює віртуальний "тунель" між двома роутерами через публічну мережу, гарантуючи, що дані залишаються конфіденційними та недоступними для сторонніх під час транзиту. Щоб забезпечити доставку шифрованого пакета, IPsec додає новий IP-заголовок, що направляє пакет через тунель. При досягненні кінцевої точки тунелю, шифрування знімається, і оригінальний IP-пакет

передається до кінцевого пункту призначення.



А у транспортному режимі IPsec шифрується лише корисне навантаження (payload) IP-пакету, тоді як заголовок пакета залишається незмінним та видимим. Цей режим часто використовується для захищеного кінцевого до кінцевого з'єднання, наприклад, між клієнтом та сервером. Оскільки заголовок IP залишається незашифрованим, проміжні роутери можуть визначити кінцеве місце призначення пакету, що дозволяє ефективну маршрутизацію без додаткових тунельних протоколів. Транспортний режим відомий своєю ефективністю у використанні пропускної здатності мережі порівняно з тунельним режимом, зробивши його вибором для сценаріїв використання, де необхідно оптимізувати продуктивність.



Протоколи IPSec безпечно передають пакети даних. Пакет даних - це певна структура, яка форматує і готує інформацію для передачі мережею. Він складається з заголовка, корисного навантаження і трейлера.

- Заголовок - це попередній розділ, який містить інструкцію для маршрутизації пакета даних до правильного місця призначення.
- Корисне навантаження - це термін, який описує фактичну інформацію, що міститься в пакеті даних.

- Трейлер - це додаткові дані, що додаються до хвоста корисного навантаження, щоб вказати на кінець пакета даних.

Деякі протоколи IPSec наведені нижче.

The Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) складається з шести частин, як описано нижче. Перші дві частини не зашифровані, але вони автентифіковані. Ці частини виглядають наступним чином:

- Індекс параметрів безпеки (SPI) - це довільне 32-бітне число, яке вказує пристрою, що отримує пакет, яку групу протоколів безпеки використовує відправник для зв'язку. Ці протоколи включають конкретні алгоритми і ключі, а також термін дії цих ключів.

- Порядковий номер - це лічильник, який збільшується на 1 кожного разу, коли пакет надсилається на ту саму адресу і використовує той самий SPI. Порядковий номер вказує, який пакет є яким, і скільки пакетів було надіслано з однаковою групою параметрів. Порядковий номер також захищає від атак повтору. Атака повтору передбачає, що зловмисник копіює пакет і надсилає його в неправильній послідовності, щоб збити з пантелику пристрої, які взаємодіють між собою.

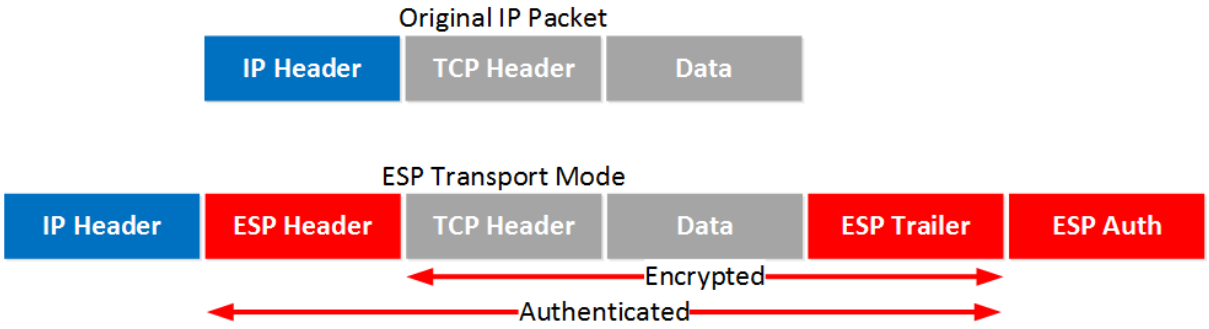
Решта чотири частини ESP шифруються під час передачі мережею. Ці частини є наступними:

- Дані корисного навантаження - це фактичні дані, які переносяться пакетом.
- Padding, від 0 до 255 байт даних, дозволяє певним типам алгоритмів шифрування вимагати, щоб дані були кратними певній кількості байт. Padding також гарантує, що текст повідомлення закінчується на межі чотирьох байт (архітектурна вимога в IP).
- Поле Pad Length (Довжина padding) вказує, яку частину корисного навантаження становить padding, а не дані.

- Поле Next Header, як і стандартне поле IP Next Header, визначає тип даних, що передаються, і протокол.

ESP додається після стандартного IP-заголовка. Оскільки пакет має стандартний IP-заголовок, мережа може маршрутизувати його за допомогою стандартних IP-пристроїв. Як результат, IPsec сумісний з IP-маршрутизаторами та іншим обладнанням, навіть якщо воно не призначене для використання IPsec. ESP може підтримувати будь-яку кількість протоколів шифрування. Користувач сам вирішує, які з них використовувати. Для кожної особи, з якою користувач спілкується, можна використовувати різні протоколи. Однак IPsec визначає базовий шифр DES-Cipher Block Chaining mode (CBC) за замовчуванням, щоб забезпечити мінімальну функціональну сумісність між мережами IPsec. Можливості шифрування ESP призначені для симетричних алгоритмів шифрування. IPsec використовує асиметричні алгоритми для таких спеціалізованих цілей, як узгодження ключів для симетричного шифрування.

Коли ми використовуємо транспортний режим, ми використовуємо оригінальний IP-заголовок і вставляємо заголовок ESP. Ось як це виглядає:



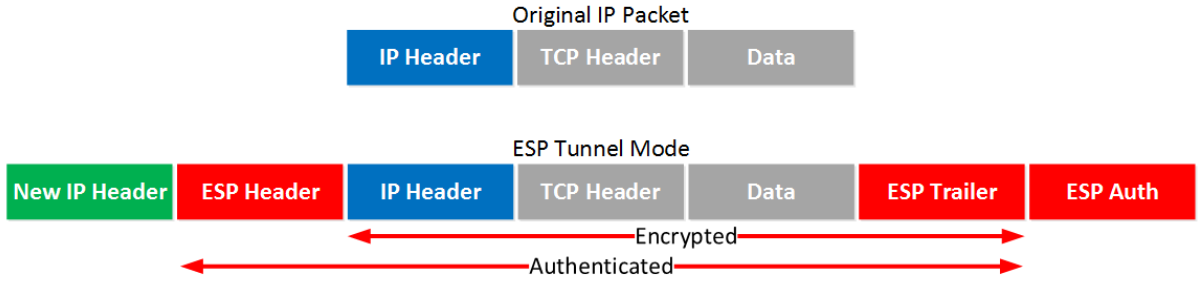
Як можна побачити, ми додаємо заголовок ESP і трейлер. Наш транспортний рівень (наприклад, TCP) і корисне навантаження будуть зашифровані. Він також пропонує автентифікацію, але, на відміну від AH, не для всього IP-пакету.

```
Frame 1: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface 0
Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 152
    Identification: 0x0042 (66)
  Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: Encap Security Payload (50)
  Header checksum: 0x219e [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Encapsulating Security Payload
    ESP SPI: 0x36cb42df (919290591)
    ESP Sequence: 1
```

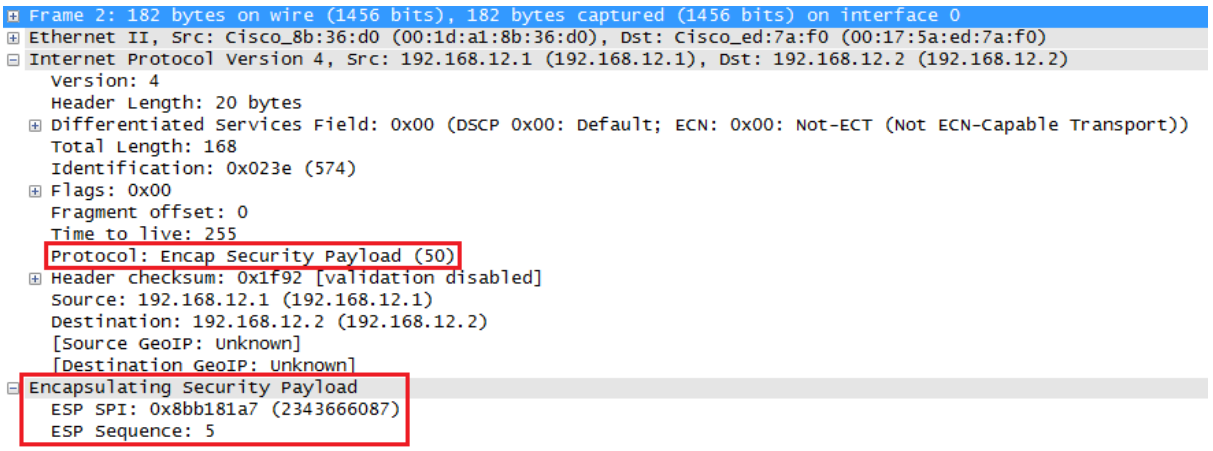
Вище ви бачите оригінальний IP-пакет і те, що ми використовуємо ESP. IP-заголовок є відкритим текстом, але все інше зашифровано.

Тунелювання за допомогою ESP

Тунелювання бере оригінальний заголовок IP-пакета і інкапсулює його в ESP. Потім до пакета додається новий IP-заголовок, що містить адресу пристрою-шлюзу. Тунелювання дозволяє користувачеві надсилати нелегальні IP-адреси через публічну мережу (наприклад, Інтернет), яка в іншому випадку не прийняла б їх. Тунелювання за допомогою ESP пропонує перевагу приховування оригінальних адрес джерела та призначення від користувачів у загальнодоступній мережі. Приховування цих адрес зменшує потужність атак на основі аналізу трафіку. Атака на основі аналізу трафіку використовує методи моніторингу мережі, щоб визначити, скільки даних і якого типу передається між двома користувачами.



Це схоже на транспортний режим, але ми додаємо новий заголовок. Оригінальний заголовок IP тепер також зашифрований.



Результат перехоплення, наведений вище, схожий на те, що ви бачили в транспортному режимі. Єдина відмінність полягає в тому, що це новий IP-заголовок, ви не побачите оригінальний IP-заголовок.

Поле автентифікації ESP

Поле автентифікації ESP містить значення перевірки цілісності (ICV), яке функціонує як цифровий підпис, що обчислюється над рештою частини ESP. Довжина поля автентифікації ESP варіюється залежно від використовуваного алгоритму автентифікації. Це поле можна повністю пропустити, якщо автентифікація не потрібна для ESP. Автентифікація обчислюється в пакеті ESP після завершення шифрування. Поточний стандарт IPsec вимагає використання HMAC (схема симетричного підпису) з хешами SHA1 і MD5 як алгоритмів для IPsec-сумісного апаратного і програмного забезпечення в полі автентифікації ESP-пакета.

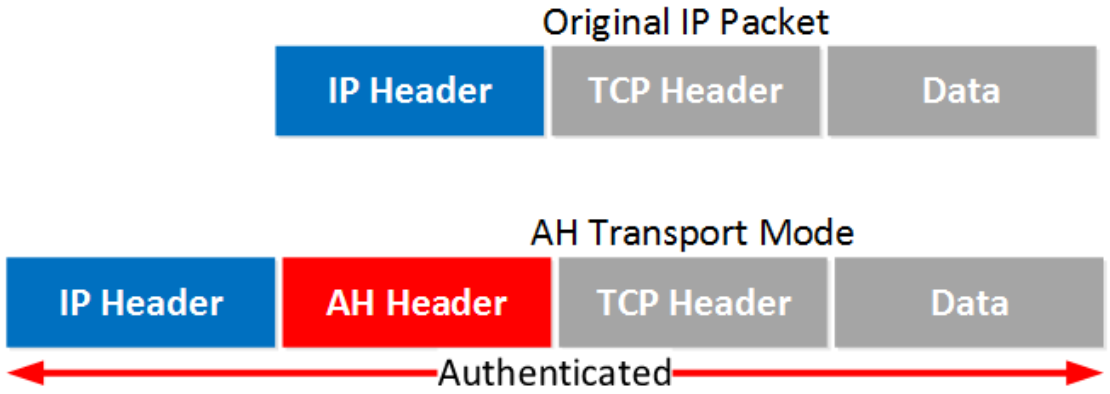
Значення перевірки цілісності підтримує автентифікацію симетричного типу. Пристрій-відправник шифрує хеш корисного навантаження даних і додає його як поле автентифікації. Пристрій-одержувач підтверджує, що нічого не було змінено і що корисне навантаження надійшло від правильного пристрою-джерела.

AH (Authentication Header)

Заголовок автентифікації (Authentication Header, AH), надає послуги автентифікації. AH може застосовуватися окремо, разом з ESP або вкладеним чином, коли використовується тунельний режим. Автентифікація, що забезпечується AH, відрізняється від автентифікації, що забезпечується ESP, тим, що можливості автентифікації ESP не

захищають IP-заголовок, який знаходиться перед ESP, хоча інкапсульований IP-заголовок у тунельному режимі захищений. Служби AH захищають цей зовнішній IP-заголовок разом з усім вмістом пакету ESP. AH захищає не всі поля в зовнішньому IP-заголовку, оскільки деякі з них змінюються під час транзиту, і відправник не може передбачити, як саме вони можуть змінитися. AH захищає все, що не змінюється під час передачі. У пакеті AH розташовується після IP-заголовка, але перед ESP (якщо він присутній) або іншим протоколом вищого рівня, наприклад, TCP. Як і ESP, AH може реалізовувати режим тунелювання. Також, як і ESP, IPsec вимагає наявності спеціальних алгоритмів для реалізації AH.

У транспортному режимі, додається заголовок AH після заголовка IP. Ось приклад IP-пакета, який містить деякий TCP-трафік:

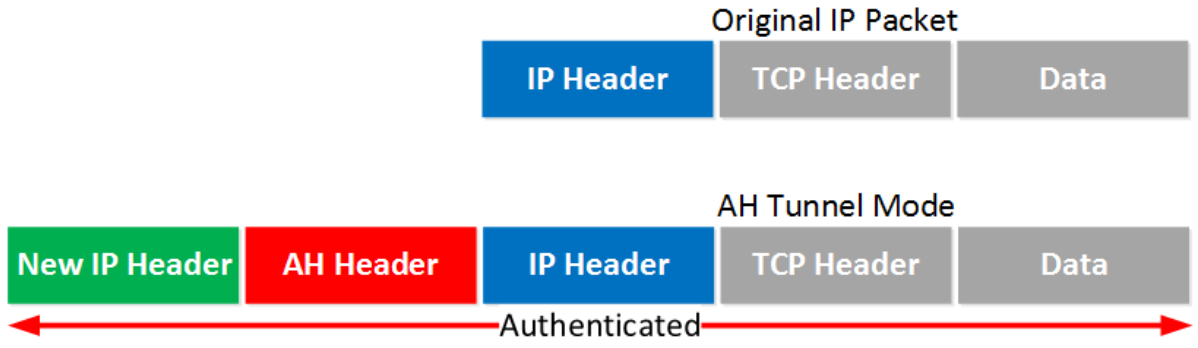



```
Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 124
    Identification: 0x0028 (40)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: Authentication Header (51)
  Header checksum: 0x21d3 [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Authentication Header
    Next Header: ICMP (0x01)
    Length: 24
    AH SPI: 0xcf54ccdf
    AH Sequence: 30
    AH ICV: aa9cafe5ed06d6c74cb3c671
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x7994 [correct]
    Identifier (BE): 8 (0x0008)
    Identifier (LE): 2048 (0x0800)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 2]
  Data (72 bytes)
```

Вище ви бачите заголовок AH між заголовком IP і заголовком ICMP. Це знімок пінгу між двома маршрутизаторами. Ви можете бачити, що AH використовує 5 полів:

- *Наступний заголовок: визначає наступний протокол, у нашому прикладі - ICMP.*
- *Довжина: це довжина заголовка AH.*
- *SPI (Індекс параметрів безпеки): це 32-бітний ідентифікатор, щоб одержувач знав, до якого потоку належить цей пакет.*
- *Sequence (послідовність): це порядковий номер, який захищає від атак повторного відтворення.*
- *ICV (Integrity Check Value - значення перевірки цілісності): це обчислений хеш для всього пакета. Одержувач також обчислює хеш, і якщо він не збігається, ви знаєте, що щось не так.*

У тунельному режимі ми додаємо новий IP-заголовок поверх оригінального IP-пакета. Це може бути корисно, якщо ви використовуєте приватні IP-адреси і вам потрібно тунелювати свій трафік через Інтернет. Це можливо за допомогою AH, але він не пропонує шифрування:



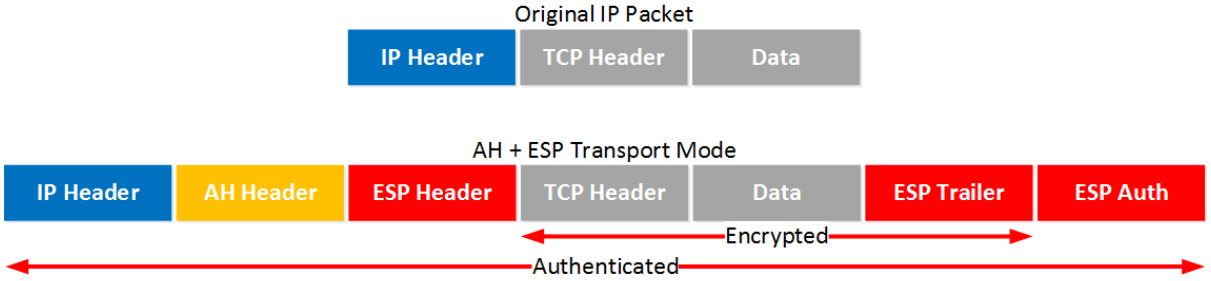
Весь IP-пакет буде автентифіковано.

```
Frame 1: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 144
    Identification: 0x0215 (533)
  + Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: Authentication Header (51)
  + Header checksum: 0x1fd2 [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Authentication Header
    Next Header: IPIP (0x04)
    Length: 24
    AH SPI: 0x646adc80
    AH Sequence: 5
    AH ICV: 606d214066853c0390cfe577
Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  + Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 100
    Identification: 0x003c (60)
  - Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  + Header checksum: 0x2209 [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```

Вище ви бачите новий IP-заголовок, потім заголовок AH і, нарешті, оригінальний IP-пакет, який містить деякий ICMP-трафік.

Однією з проблем AH є те, що він погано працює з NAT / PAT. Поля в IP-заголовку, такі як TTL і контрольна сума, виключаються AH, оскільки він знає, що вони можуть змінитися. Однак IP-адреси та номери портів залишаються. Якщо ви зміните їх за допомогою NAT, ICV AH не спрацює.

AH та ESP разом



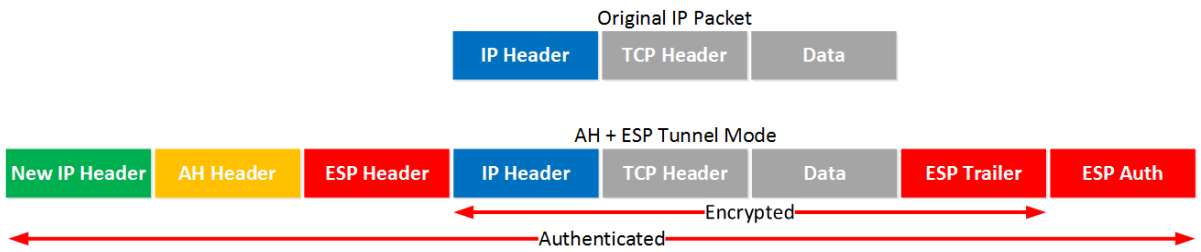
Для транспортного способу ми будемо використовувати оригінальний IP-заголовок, за яким слідують заголовок AH і заголовок ESP.

Транспортний рівень, корисне навантаження і трейлер ESP будуть зашифровані.

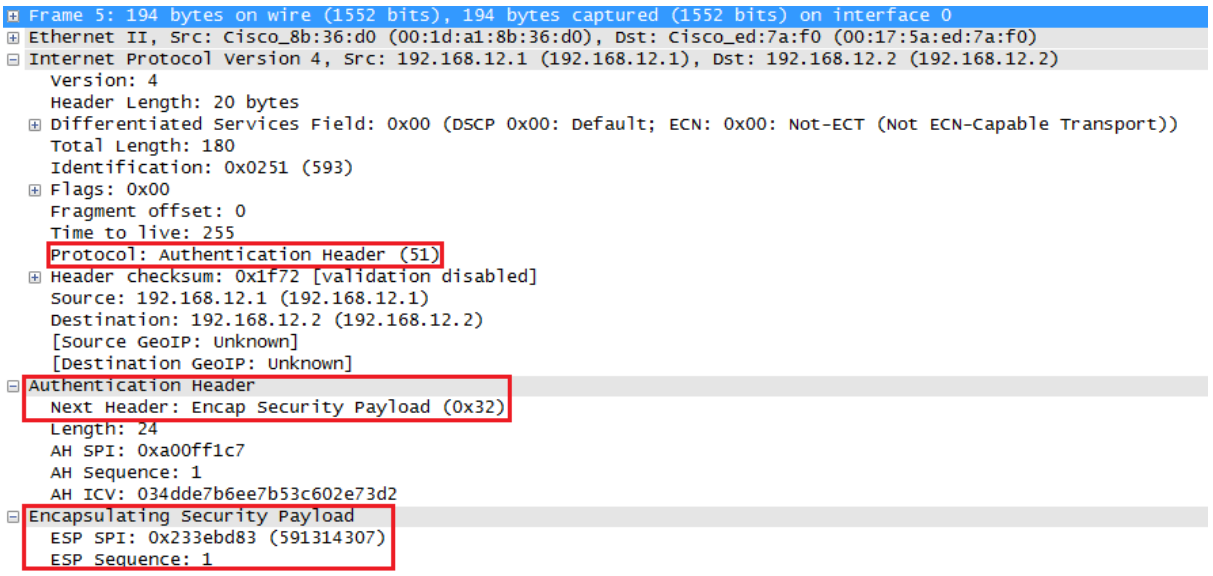
Оскільки ми також використовуємо AH, весь IP-пакет проходить автентифікацію.

```
Frame 5: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface 0
Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
    Version: 4
    Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 164
    Identification: 0x0056 (86)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: Authentication Header (51)
  Header checksum: 0x217d [validation disabled]
    Source: 192.168.12.1 (192.168.12.1)
    Destination: 192.168.12.2 (192.168.12.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Authentication Header
    Next Header: Encap Security Payload (0x32)
    Length: 24
    AH SPI: 0xa90dc9aa
    AH Sequence: 1
    AH ICV: 157ba6cc340b1a30049ea551
Encapsulating Security Payload
    ESP SPI: 0xd2264f7a (3525726074)
    ESP Sequence: 1
```

Вище ви бачите оригінальний IP-пакет, заголовок AH і заголовок ESP.



Спочатку ми отримаємо новий IP-заголовок, а потім заголовок AH та ESP. Оригінальний IP-пакет буде повністю зашифрований, і все буде автентифіковано завдяки AH.



Вище ви бачите новий заголовок IP, за яким слідують заголовки AH та ESP.

IKE (Internet Key Exchange)

Internet Key Exchange (IKE) - це протокол для узгодження протоколів та обміну ключами через Інтернет. IKE дозволяє домовитися про те, які протоколи, алгоритми та ключі слід використовувати. Він забезпечує безпечні послуги автентифікації з самого початку обміну. Він безпечно керує ключами після того, як вони були узгоджені, і безпечно обмінюється цими ключами.

IKE надає чотири можливості:

- Надає сторонам можливість домовитися про те, які протоколи, алгоритми та ключі використовувати.
- З самого початку обміну гарантує, що ви говорите з правильною людиною.
- Керує цими ключами після того, як вони були узгоджені.
- Забезпечує безпечний обмін ключами.

Обмін ключами тісно пов'язаний з управлінням асоціацією безпеки. Після створення асоціації безпеки необхідно обмінятися ключами. IKE об'єднує їх разом і постачає як інтегрований пакет. IPsec визначає, що сумісні системи також підтримують ручне введення ключів. Як наслідок, у певних ситуаціях можливий ручний обмін ключами.

Однак, для більшості великих підприємств, ручний обмін ключами є непрактичним. Таким чразом, очікується, що IKE продовжуватиме узгоджувати SA та автоматично обмінюватися ключами через публічні мережі. IKE функціонує у дві фази:

- Фаза 1: встановлюються безпечний канал для виконання операцій ISAKMP.
- Фаза 2: узгодження загальної асоціації безпеки.

IKE забезпечує три режими обміну ключовою інформацією та налаштування асоціацій безпеки IKE: основний режим, агресивний режим та швидкий режим.

Існує дві версії IKE: IKEv1 та IKEv2. Між цими двома версіями є деякі відмінності:

- IKEv2 вимагає меншої пропускної здатності, ніж IKEv1.
- IKEv2 підтримує автентифікацію EAP (поряд з попередньо наданими ключами та цифровими сертифікатами).
- IKEv2 має вбудовану підтримку обходу NAT (необхідна, коли ваш IPsec одноранговий сервер знаходиться за NAT-маршрутизатором).
- IKEv2 має вбудований механізм підтримки тунелів в актуальному стані.

Security Associations (SA)

Протоколи автентифікаційного заголовка та інкапсуляції корисного навантаження безпеки є складовими IPsec. Послуги шифрування, що надаються AH і ESP, є потужними інструментами для збереження секретності даних, перевірки їх походження і захисту від непоміченого втручання. Але ці інструменти не працюватимуть, якщо немає ретельно розробленої інфраструктури для роботи з ними. Безпека VPN досягає успіху або зазнає невдачі в залежності від надійності та масштабованості цієї інфраструктури.

Безпечна комунікація з автентифікацією та шифруванням вимагає узгодження, обміну ключами та можливості відстежувати ключі. IPsec відстежує деталі, а також те, які ключі та алгоритми використовувати, об'єднуючи все разом в Security Association (SA). Асоціація - це односторонній зв'язок між відправником і одержувачем, який забезпечує

безпеку трафіку, що ним передається. SA об'єднує всі елементи, необхідні для безпечної комунікації між двома сторонами.

SA є захищеним каналом через загальнодоступну мережу. SA також дозволяє системі створювати класи каналів безпеки. Якщо потрібні більш надійні гарантії безпеки, можна вжити більше заходів, а правила SA можуть бути змінені, щоб вказати сильніші механізми.

База даних асоціацій безпеки (SAD) - це, по суті, динамічний реєстр, який містить інформацію про активні асоціації безпеки (SA) для вхідного та вихідного трафіку. Цей реєстр наповнюється динамічно під час процесу створення системи безпеки, особливо після створення SA. Кожен SA в цьому контексті унікально визначається трьома параметрами:

Індекс параметрів безпеки (SPI)
Адреса призначення
Ідентифікатор протоколу безпеки (ESP або AH)

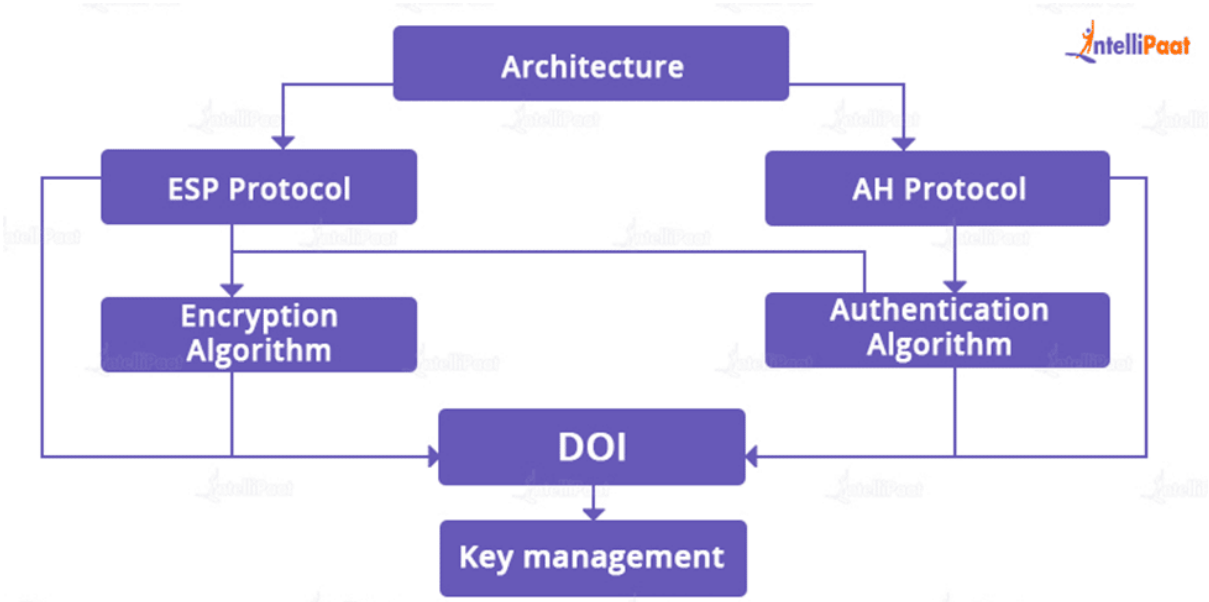
У SAD ретельно реєструються такі атрибути:

- Індекс параметрів безпеки (SPI)
- Адреса призначення
- Порядковий номер
- Вікно захисту від повторного відтворення
- Протокол безпеки IP
- Алгоритм шифрування та аутентифікації
- Криптографічний ключ
- Термін дії SA
- Асоційований IPSec

До SAD примикає база даних політики безпеки (Security Policy Database, SPD) - структурована колекція правил і політик безпеки. SPD діє як фільтр трафіку, визначаючи обробку IP-пакетів. Він керує застосуванням рівнів захисту для вихідних пакетів у поєднанні з SAD і допомагає у перевірці рівнів захисту для вхідних пакетів. По суті, SPD є критично важливим для керування обробкою трафіку на основі вимог безпеки.

Архітектура засобів захисту IPsec

- На найвищому рівні маємо протоколи для захисту віртуальних каналів та процеси узгодження захисних параметрів. Тут ключове - забезпечення безпеки даних під час їхнього транспортування.
- Середній рівень присвячений криптографічним алгоритмам, які використовуються у протоколах AH та ESP. Ці алгоритми забезпечують шифрування та аутентифікацію даних. Також тут розглядаємо алгоритми для узгодження та управління криптографічними ключами, використовуючи, зокрема, протокол IKE.
- На нижньому рівні маємо справу з доменом інтерпретації (DOI), який представляє собою базу даних. Вона містить інформацію про всі протоколи та алгоритми, що застосовуються в IPSec, включаючи їх параметри, ідентифікатори та інші важливі деталі.



Криптографічні алгоритми в IPsec

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

Особливості основних схем застосування протоколів IPSec для встановлення VPN тунелю

- ***Хост-хост***

  Особливість цього типу з'єднання полягає в тому, що кожен хост є кінцевим пунктом VPN тунелю, та обидва хости повинні бути налаштовані для підтримки IPSec. Цей метод забезпечує безпеку комунікації між конкретними комп'ютерами, дозволяючи безпечно передавати дані через незахищені мережі, як-от Інтернет.

- ***Шлюз-шлюз***

  В цьому випадку, VPN-тунель створюється між двома мережами через їхні шлюзи. Кожен шлюз повинен підтримувати IPSec, що забезпечує безпечне з'єднання між двома віддаленими мережами через Інтернет. Цей метод широко використовується для з'єднання філій компанії через публічний простір.

- ***Хост-шлюз***

  Особливості цього методу полягають в тому, що один чи кілька хостів підключаються до центрального шлюзу. Кожен хост та шлюз повинні підтримувати IPSec. Це дозволяє забезпечити безпеку комунікації між індивідуальним комп'ютером та центральним шлюзом, який часто використовується в корпоративних мережах для надання доступу до корпоративних ресурсів віддаленим працівникам