Rețele Vitual Private. IPsec

Internet Protocol Security (IPsec) - o stiva de protocoale pentru securizarea comunicatiilor IP prin autentificarea si/sau criptarea fiecarui pachet IP al fluxului de date.

Facilitati:

- IPsec include protocoale pentru stabilirea autentificarii mutuale intre agenti la inceputul sesiunii si negocierea cheilor criptografice ce vor fi utilizate in sesiune
- IPsec poate fi utilizat pentru protejarea fluxului de date intre doua masini (masini client sau servere), intre o pereche de gateway-uri securizate (rutere) sau intre un gateway securizat si o masina gazda.
- Opereaza la nivelul 3 al modelului OSI. De notat ca alte sisteme de securitate ca SSL, TLS si SSH opereaza la niveluri superioare ale modelului OSI!

De ce IPsec?

- IPsec este flexibil deoarece opereaza la un nivel OSI inferior
- Complet transparent pentru aplicatii. Poate fi utilizat la protejarea traficului deoarece aplicatiile nu trebuie sa fie proiectate pentru a utiliza IPsec. Alte protocoale de nivel superior trebuie incorporate in aplicatie.

Precursori:

- IPsec - successor al standardului ISO NLSP (Network Layer Security Protocol). Protocolul NLSP s-a bazat pe protocolul de layer 3 SP3 care a fost publicat de NIST si realizat prin proiectul Secure Data Network System (SDNS) de catre NSA.
- swIPe (Ioanidis si Blaze) – o implementare UNIX network-layer security protocol pentru IP ce realizeaza autentificarea, integritatea si confidentialitatea datagramelor IP, implementare ce utilizeaza un protocol de incapsulare pentru a pastra compatibilitatea cu infrastructura existenta in momentul aparitiei. Partea de implementare care proceseaza pachetele sosite si cele plecate este realizata integral in kernel; setarea parametrilor si manipularea exceptiilor este gestionata de procesele din userspace.

Structura IPsec

IPsec utilizeza o serie de protocoale pentru a realiza diverse functii:

- Internet Key Exchange (IKE si IKEv2) pentru stabilirea Security Association (SA), negocierea procoalelor si algoritmilor si generarea cheilor de criptare si autentificare care sunt utilizate de IPsec.

- Authentification Header (AH) pentru a realiza integritatea conexiunii si autentificarea pentru datagramele IP cat si protectia impotriva atacurilor prin replicare (replay attacks)

- Encapsulating Security Payload (ESP) pentru realizarea confidentialitatii, autentificarea originii datelor, integritatea conexiunii.

- Pachetele includ headerele: IP, ESP, AH si poate altele, cum ar fi TCP sau UDP

- Lucreaza cu IPv4 si cu IPv6

Moduri de operare

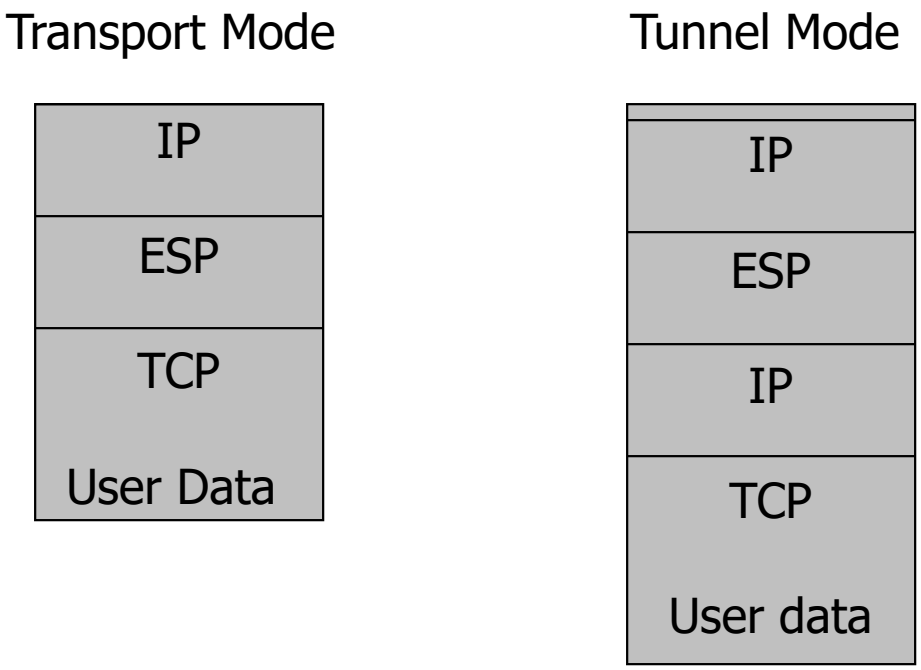
Moduri de operare:

- Transport mode. Numai datele transportate de pachetul IP sunt criptate si/sau autentificate. Rutarea este identica deoarece headerul IP nu este modificat sau criptat. Cu toate acestea atunci cand este utilizat header-ul de autentificare adresele IP nu pot fi translatate, deoarece acesta va invalida valoarea hash. Nivelurile de transport si aplicatie sunt intotdeauna securizate prin hash asa ca acestea nu pot fi modificate in nici un fel (de ex. translatarea numerelor de port). Un mod de incapsulare a mesajelor IPsec pentru traversarea NAT a fost definit in documentele ce descriu mecanismul NAT-T.

- Tunnel mode. In acest mod intregul pachet IP (datele si headerul IP) este criptat si/sau autentificat. El este incapsulat intr-un nou pachet IP cu un nou header IP. Acest mod este utilizat la crearea retelelor private virtuale (Virtual Private Network) pentru comunicatia intre retele (ex: intre rutere care leaga retele), comunicatia gazda-retea (ex: remote user acces) si comunicatia gazda la gazda (ex: chat privat).

Formatul pachetelor

Formatul pachetelor depinde de modul de operare:



Header de autentificare

Authentication Header (AH) este membru al protocolului IPsec, garanteaza integritatea conexiunii si autentificarea originii datelor din pachete IP. Este gandit ca in viitor sa poata proteja impotriva replay attacks utilizand tehnica de fereastra alunecatoare (sliding window) si pierderea pachetelor vechi.

- AH protejaza datele din datagrama IP si toate campurile din header exceptand campurile ce se modifica in timpul tranzitului. Campurile din header neautentificate la IPv4 sunt: Type of Service (ToS), Flags, Fragment Offset, TTL, Header Checksum
- AH opereaza direct in fata protocolului IP si are numarul 51 (in asignarea IANA)
- AH se bazeaza pe o cheie cripografica realizata cu o functie hash
- Utilizeaza Security Parameter Index (SPI) pentru a identifica asociatia de securitate, tip de cheie si algoritm, etc

ESP - Encapsulating Security Payload

ESP este partea IPsec care realizeaza autentificarea originii, protectia integritatii si confidentialitatii pachetelor.

- ESP transporta pachetul criptat.

- ESP suporta configuratiile numai criptare sau numai autentificare insa utilizarea criptarii fara autentificare este puternic descurajata datorita nesigurantei.

- Spre deosebire de AH, ESP nu protejaza headerul pachetului IP. Cu toate acestea in modul tunnel cand intreg pachetul IP original este incapsulat cu un nou headet de pachet adaugat, protectia ESP se produce la intreg pachetul IP (inclusiv headerul interior).

- ESP opereaza in fata IP si utilizeaza numarul de protocol IP 50 (IANA);

- Utilizarea standard ESP este pentru DES in mod Cipher Block Chaining (CBC).

AH - Header de autentificare (format)

Structura pachetului AH

Next protocol	Lungime	rezervat
SPI		
Numar secventa		
Data autentificata (lungime variabila)		

In care:

- Next protocol - numar ce identifica urmatorul protocol in payload conform IANA;
- Lungime - lungimea portiunii data autentificata;
- SPI – identifica parametrul de securitate care in combinatie cu adresa IP identifica SA implementata cu acest pachet;
- Numar secventa – un numar generat crescator utilizat pentru prevenirea atacurilor replica
- Data autentificata – contine valoarea de verificarea integritatii (ICV) necesara pentru autentificarea pachetului.

Format ESP

Structura header

<table>
<tr><td colspan="3">SPI</td></tr>
<tr><td colspan="3">Numar secventa</td></tr>
<tr><td colspan="3">Payload data</td></tr>
<tr><td>Payload data</td><td colspan="2">Padding</td></tr>
<tr><td colspan="2">Padding</td><td>padlen</td><td>next header</td></tr>
<tr><td colspan="4">Data autentificata (lungime variabila)</td></tr>
</table>

In care:

- Payload data – datele ce vor fi transferate;
- Padding – utilizat pentru a completa dimensiunea unui bloc
- Padlen – marimea padding in octeti (max 255)
- Celelalte campuri au aceeasi semnificatie cu cele de la AH

Security Association

- Arhitectura IP security utilizeaza conceptul de Security Association (SA) ca baza pentru a construi functiile de securitate in IP. SA este o colectie de algoritmi si parametrii (ca o cheie) utilizati pentru criptarea si autentificarea unui flux de date intr-o directie. La trafic bidirectional fluxul de date este securizat cu o pereche SA
- Pentru a decide ce protectie va fi aplicata pentru un pachet care pleaca, IPsec utilizeza SPI, index la Security Association DataBase (SADB) impreuna cu adresa destinatie din header-ul pachetului. Ambele identifica asociatia de securitate pentru acel pachet.
- O procedura similara este utilizata la pachetele care sosesc unde IPsec culege cheile de verificare de la SADB
- Pentru multicast o SA este furnizata pentru un grup si este duplicata pentru fiecare dintre receptorii autorizati ai grupului.
- Pot exista mai multe SA pentru un grup care utilizeaza SPI diferite, permitand in acest mod multiple niveluri si setari ale securitatii in grup
- Fiecare transmitator poate avea SA multiple, fapt ce permite autentificarea, pe cand receptorul poate stii numai ca cineva cunoaste cheile cu care au fost trimise datele
- Standardele nu descriu cum este aleasa asocierea si asignarea la un grup, ci presupune ca o parte responsabila face aceasta alegere.

IPsec si Firewall

Utilizari IPsec:

- Virtual Private Network
- Securitate Internet in general

IPsec si Firewall:

- IPsec rezolva doua mari probleme: autentificatrea end to end (o masina comunica cu masina cu care crede ca comunica) si criptarea (preintimpinarea atacurilor care asculta traficul).
- Nici unul dintre aceste lucruri nu este rezolvat de firewall. Firewall ajuta la protejarea impotriva unor riscuri prezente in Internet fara autentificare si criptare.

Concluzie: IPsec nu inlocuieste firewall si nici invers. Interesanta posibilitatea de combinare a IPsec si firewall

- Controlul accesului poate fi aplicat la traficul criptat, in functie de sursa.
- Adresa IP sursa poate fi autentificata numai daca este legata de un certificat.
- Traficul criptat poate utiliza diferite firewall-uri, insa este necesara coordonarea politicilor.
- Cele mai bune filtre de pachete sunt eficiente indiferent daca au IPsec AH. Firewall-urile aplicatie au o mai buna capacitate de verificare a sursei utilizand IPsec AH, in comparatie cu increderea acordata (sau nu) implicit pachetelor IP normale.

Probleme privind implementarea

La orice implementare este necesara analiza urmatoarelor aspecte:

- Cum cer aplicatiile protectie criptografica?
- Cum se poate verifica existenta lor?
- Cum mandateaza administratorul criptarea intre o masina si alte parti ale retelei?
- Cum se face autorizarea?

Managementul cheilor

Intrebari:

- De unde vin cheile folosite de IPsec? Comunicatia IPsec SA.
- Se pot utiliza chei statice?
- Care sunt cerintele privind gestionarea cheilor?

Teoretic pot fi utilizate chei statice, au o multime de dezavantaje:

- Nu sunt complet aleatoare.
- Atacatorii pot lansa password guessing attack.
- Teoria si analiza istorica arata ca este o idee gresita sa se cripteze prea multe informatii cu aceeasi cheie.
- Nu se poate utiliza protectia la replici cand se utilizeaza chei statice.
- Chiar daca este mai usor de administrat nu reprezinta o practica recomandata.

Protectia la raspuns

- La stabilirea unei noi asocieri de securitate SA, sursa initializează numaratorul de pachete cu valoarea zero ce va fi incrementata la fiecare pachet emis. Valoarea va fi scrisa in campul *numar secventa* din AH.
- In orice moment o masina poate fi repornita, se pierde numarul de secventa curent si se restarteaza numararea de la 1.
- La atingerea valorii 2^{32} -1 sursa trebuie să termine SA curentă si să negocieze o nouă SA, cu o nouă cheie.
- Deoarece IP asigură un serviciu fără conexiune, IPSec recomandă ca destinatarul să implementeze o fereastra de receptie *W* cu valoarea implicită *W*=64. Limita superioară a ferestrei este reprezentată de *N* numărul de secventă cel mai mare receptionat pentru un pachet valid, iar limita inferioară este $N - W + 1$.
- La cheile statice replicile pot fi utilizate pentru atacarea confidentialitatii prin ignorarea numarului de secventa.

Comentarii IPsec

- IPsec nu utilizeaza PKI, iar schimbul de chei inainte de stabilirea conexiunii IPsec creaza probleme.
- IKE rezolva generarea unei chei simetrice pentru o sesiune IPsec, dar fara PKI atacurile man-in-the-middle sunt posibile.
- IKE creaza Security Associations (SA).
- SA are o structura ce contine chei si alte informatii relevante despre conexiune.
- IKE este in general un protocol de schimb chei.
- IPsec SA nu este echivalent IKE SA, insa IKE SA poate fi convertit la IPsec SA.
- IKE ca toate protocoalele de criptare este complicat.

Internet Key Exchange (IKE)

- **Internet Key Exchange** (**IKE** sau **IKEv2**) este protocolul utilizat pentru stabilirea asociatiei de securitate (SA) in IPsec. IKE utilizeaza in schimbul de chei Deffie-Hellman pentru stabilirea unui secret partajat sesiunii de la care cheia criptografica este derivata. O tehnica cu cheie publica/privata (PKI) sau o cheie prepartajata se utilizeaza pentru autentificarea mutuala a partilor in comunicare.

- Multe implementari constau intr-un demon IKE care ruleaza in user space si stiva IPsec din kernel. Demonul din user space are acces facil la informatiile de configurare cerute, ca adresele endpoint IPsec, chei si certificate. Modulele Kernel pot procesa eficient pachetele cu overhead minim.

IKE - filozofia de baza

- IKE este un protocol care asigura trei obiective pentru IPsec:
  - Stabilirea politicii pentru o sesiune IKE
  - Stabilirea unei chei pentru IKE SA
  - Stabilirea de SA

- In proces sunt implicate doua parti *Initiator* si *Responder*

- Stabilirea unei chei pentru IKE SA se realizeaza in doua faze:
  - Stabilirea unui *control SA* (cunoscuta ca faza 1 SA);
  - Utilizare control SA pentru a crea un *copil SA (child SA)* (cunoscuta si ca faza 2 SA).

- In acest moment datele IPsec sunt protejate prin child SA.

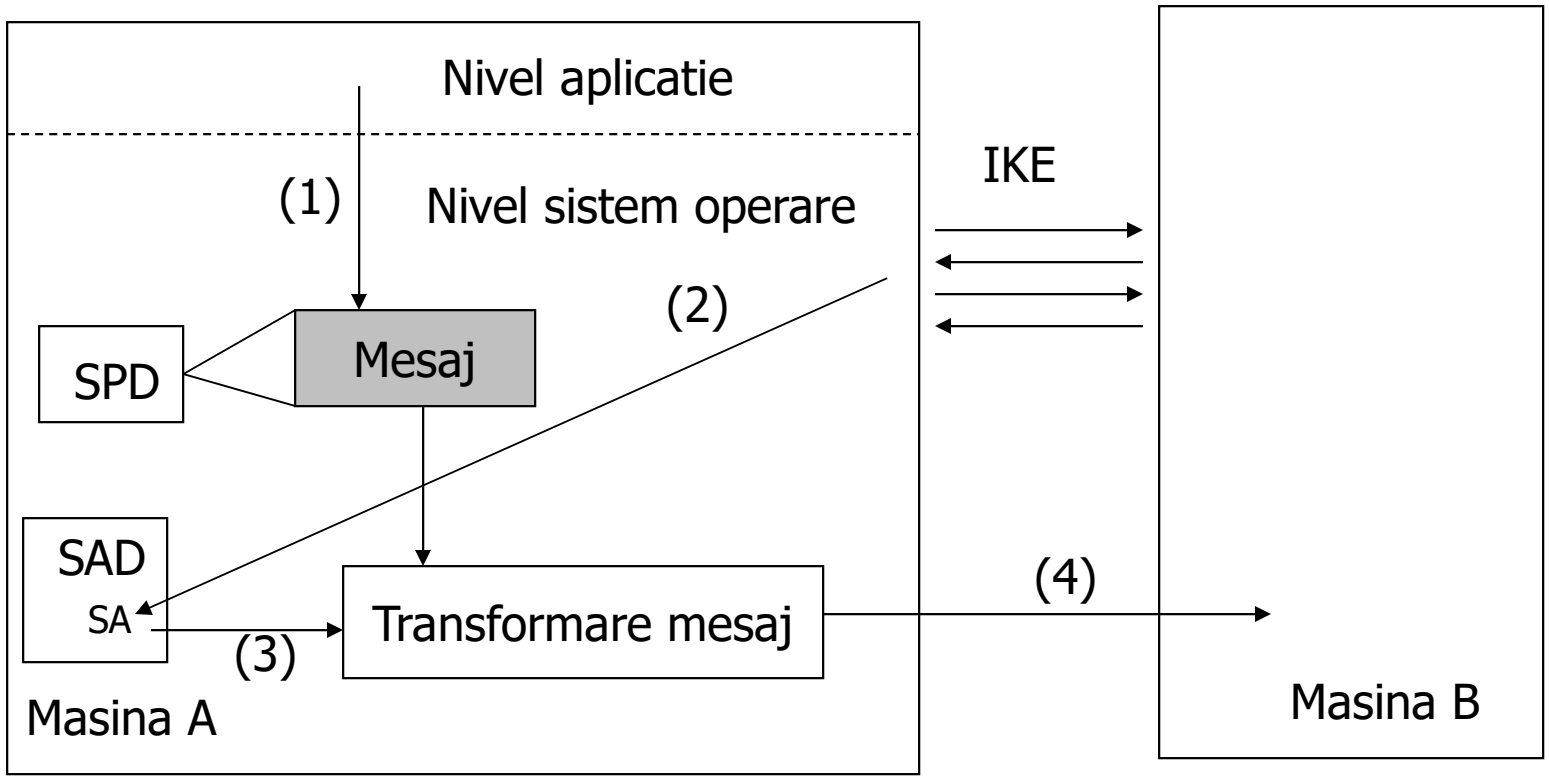
- Alt controlor de trafic poate utiliza control SA.

Procesarea pachetelor IPsec

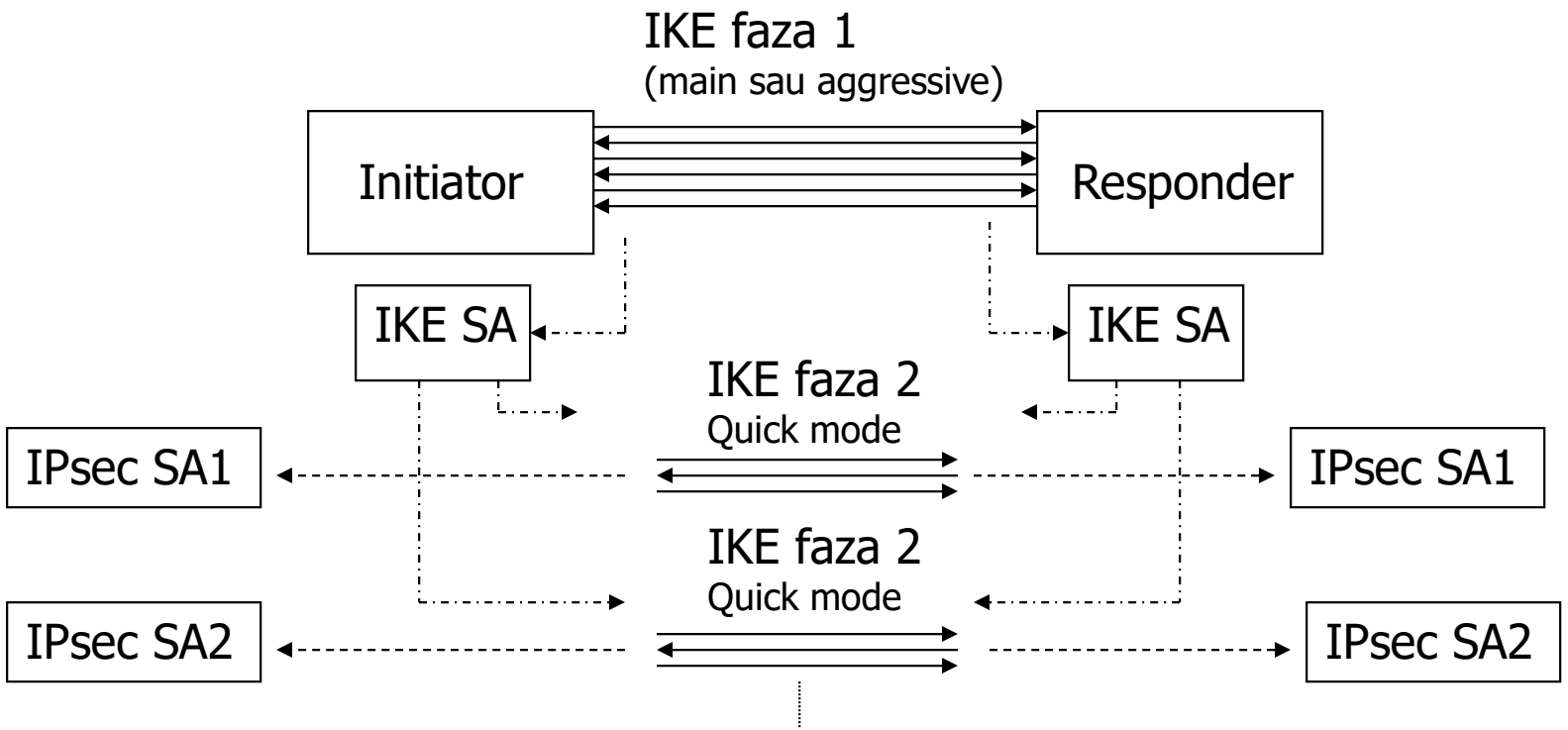
Procesarea traficului IP pe arhitectura IPsec:

- Presupunem ca initial masina A nu a comunicat cu B
- O aplicatie oarecare de la A doreste sa trimita date la o masina B prin UDP (1);
- Dupa receptie, implementarea IPsec de la A ca: tipul de protocol (UDP), adresa destinarie (B) si alte informatii sunt mapate in *Security Policy Database (*SPD) la o politica IPsec. In exemplu politica mandateaza Encapsulating Security Payload (ESP) mod confidential si management cheie automat.
- IKE protocol este lansat intre cele doua masini si cheile de sesiune sunt stabilite (2);
- Terminarea cu succes a protocolului IKE este crearea unui SA care defineste cheile, politica ESP si timp de viata SA.
- Pachetul este transformat (3) si transmis la B (4).

Procesare IPsec



Flux protocol IKE



Explicatii IKE protocol

Faza 1:

- Permite celor doua entitati sa creeze IKE SA
- IKE SA defineste cheile si politicile utilizate pentru stabilirea procesarii datelor numita si IPspec SA
- Poate opera in 2 moduri:
  - Main mode – sase mesaje care asigura protectia identitatii, adica initiatorul nu este expus unui atacator care ataca activ sistemul
  - Aggressive mode – trei mesaje, mai simplu dar mai putin sigur
- In ambele moduri acelasi rezultat – IKE SA

Faza 2 numita si quick mode;

- Utilizeaza IKE SA stabilit anterior pentru a crea un IPsec SA
- Opereaza cu trei mesaje: cerere, raspuns la cerere si confirmarea raspunsului
- Pentru simplitate cheile si configuratia utilizata pentru definire IPsec SA sunt generate din valorile schimbate intre parti
- Daca se doreste partile pot angaja alt schimb Diffie-Hellman
- Un singur IKE SA poate fi utilizat pentru a defini mai multe IPsec SA simultan.