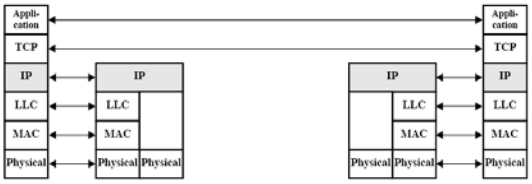
IPSec: IP security protocol

- boven op IP
- zowel voor IPv4 (optioneel) als voor IPv6 (verplicht)
- onder transportlaag (TCP/UDP), dus transparant voor toepassingen en gebruikers



LLC = logical link control

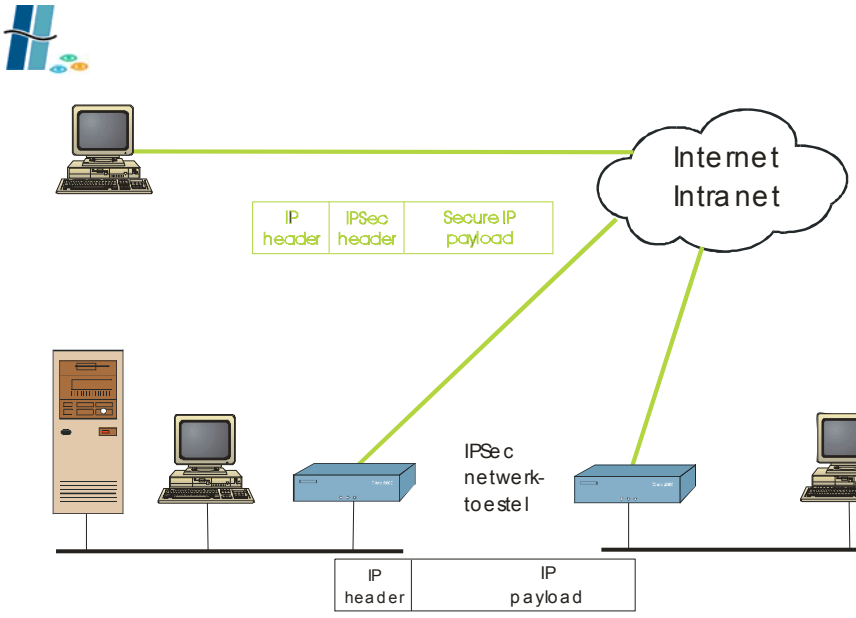
MAC = Media Access Control

1

IPSec: IP security protocol (2)

- end-to-end beveiliging op basis van cryptografie
  - toegangscontrole
  - authenticatie van data-oorsprong
  - integriteit van de boodschap (wijzigen)
  - beveiliging tegen herhaling (*replay*)
  - geheimhouding
  - beperkte beveiliging tegen analyse van netwerkverkeer
- geen overhead op lokaal netwerk indien geïmplementeerd in router of firewall

IPSec 2



IPSec 3

IPSec: toepassingen

- veilig netwerkverkeer tussen bedrijfsafdelingen over het Internet
- veilig netwerkverkeer van gebruiker naar bedrijfsnetwerk via ISP en Internet
- opzetten van intranet-extranet verbindingen met partners (authenticering, confidentialiteit, sleuteluitwisseling)
- verbetert beveiliging van E-commerce

- samengevat:
  - voor elke applicatie kan alle trafiek geëncrypteerd en geauthentiseerd worden op IP-niveau

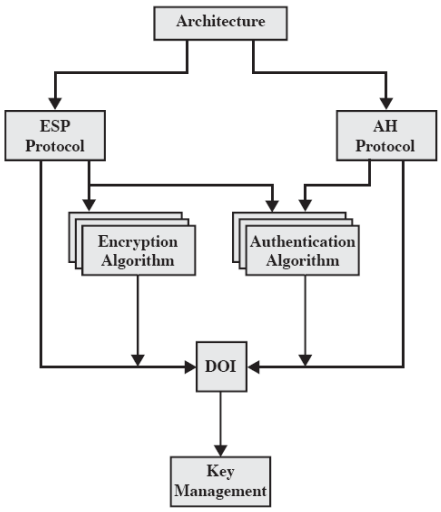
IPSec 4

IPSec: specificatie

- vrij complex
- gedefinieerd in verschillende RFC's
  - incl. RFC 2401/2402/2406/2408
- en verschillende andere, gegroepeerd per categorie
  - architectuur
    - algemene concepten, definities, vereisten, ...
  - ESP
    - algemeen gebruik en pakketinfo
  - AH
    - algemeen gebruik en pakketinfo
  - encryptiealgoritmen
    - welke en hoe te gebruiken bij ESP
  - authenticatiealgoritmen
    - welke en hoe te gebruiken bij ESP en AH
  - sleutelbeheer
  - Domain of Interpretation (referenties naar andere documenten)

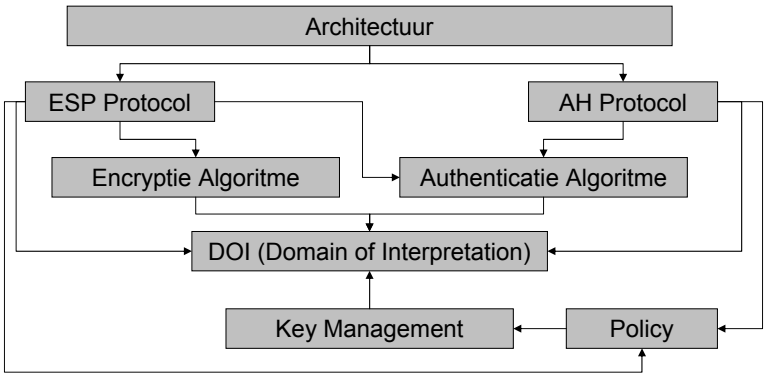
IPSec 5

IPSec: samenhang documenten



IPSec 6

IPSec: samenhang documenten



Bestanddelen van IPSec

IPSec bestaat uit volgende drie protocollen:

- Authentication Header (AH)
  - authenticatie van gegevensoorsprong
  - connectieloze data-integriteit
  - ontvanger van een IP-pakket kan verifiëren dat
    - de oorsprong ervan authentiek is
    - het pakket tijdens de overdracht niet is gewijzigd
- Encapsulating Security Payload (ESP)
  - beveiliging van gegevens (encryptie)
  - voorziet optioneel ook in authenticatie
- IKE (Internet Key Exchange): gebruikt delen van
  - Internet Security Association and Key Management Protocol (ISAKMP)
  - Oakley
  - SKEME

Overzicht IPSec-diensten

	AH	ESP (encr)	ESP (encr+auth)
Toegangscontrole	•	•	•
Gegevensintegriteit	•		•
Authenticatie van de gegevensoorsprong	•		•
Verwerpen van heruitgezonden pakketten	•	•	•
Confidentialiteit		•	•
Beperkte bescherming van analyse trafficflow		•	•

Security Association (SA) (1)

- belangrijk concept voor zowel AH als ESP
- is een **uni**directionele *verbinding* (relatie) tussen twee IPSec-systemen (zender en ontvanger, 2 eindpunten)
  - overeenkomst tussen 2 partijen
  - bepaalt welke veiligheidsdiensten ze zullen gebruiken en hoe
- twee SA's indien beveiligde uitwisseling noodzakelijk in de 2 richtingen tussen die 2 eindpunten

Security Association (SA) (2)

- één SA geldt voor
  - ofwel AH
  - ofwel ESP

  niet voor beide samen
- SA geïdentificeerd door 3 parameters:
  - Security Parameter Index (**SPI**)
    - identificeert SA (lokale betekenis, uniek voor ontvanger, door hem bepaald)
    - zit in header van AH en ESP protocol, zodat ontvanger weet hoe pakket moet worden behandeld
  - **IP-adres** van bestemming (unicast)
  - Security Protocol Identificatie (AH of ESP)
- in IP-pakket: SPI en IP-adres identificeren SA

SA gegevensbanken

- steeds aanwezig bij elke implementering van IPSec
- SAD (association) en SPD (policy)
- verborgen door de gebruikersinterface
- consultatie bij inkomend verkeer
  - pakket bevat SPI
  - SPD en SAD worden geconsulteerd om te weten hoe het pakket moet worden behandeld
- consultatie bij uitgaand verkeer
  - SPD bepaalt welke SA moet worden gebruikt voor pakketbehandeling
    - policy informatie bevat vaak transportinformatie (poortnrs)
    - is onbereikbaar bij ontvangst vooraleer IPSec behandeld is
  - SA info wordt uit SAD gehaald

Security Association Database

- bevat entry voor elke SA
- ingang bevat o.a.
  - informatie over protocol (AH of ESP)
    - algoritmen
    - sleutels + levensduur
  - sequentienummer
    - waarde in te vullen in header van het pakket
    - wat te doen bij overflow? (verder doen of overdracht stoppen)
  - mode waarin protocol is gebruikt: transport of tunnel
  - levensduur van de SA
  - MTU (max transmission unit = max grootte van pakket voor pad)
  - Anti-replay window

Security Policy Database SPD (1)

- bevat vergelijkbare regels als die van firewall of packet-filter
- bepaalt hoe welke IP-trafiek wordt beveiligd
  - afhankelijk van
    - bron en bestemming
    - inkomend of uitgaand verkeer
- 1 entry bevat subset van IP-verkeer incl. transportinfo
- SPD legt relatie tussen IP-verkeer en SA's
  - 1 entry (of meer) → geen SA
  - 1 entry → 1 SA
  - meerdere ingangen → 1 SA
  - 1 ingang → meerdere SA's

Security Policy Database SPD (2)

- policy-entry bevat o.a.
  - IP-adressen van bron en bestemming
    - 1 adres
    - lijst
    - bereik
    - wildcard
  - TCP of UDP poorten van bron en bestemming
    - aparte poorten
    - lijst
    - wildcard
  - protocol transportlaag (NextHeader field IPv6, Protocol IPv4)
  - userID
  - verwijzing naar al dan niet beveiliging via SA('s) aanduiding

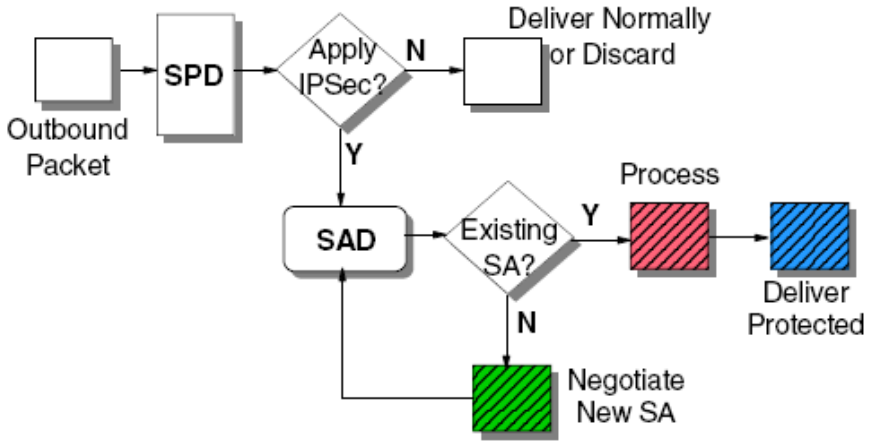
Security Policy Database SPD (3)

- aparte ingangen voor
  - inkomend verkeer
  - uitgaand verkeer
- verwerking uitgaand verkeer:
  - vergelijk velden in pakket om SPD-ingang te vinden
  - bepaal SA (of geen) en SPI
  - voer IP-Sec bewerking uit (AH of ESP)
- ingang bepaalt of trafiek al dan niet
  - moet verwerkt worden door IPSec
  - of moet worden tegengehouden

IPSec verwerking: uitgaand verkeer

- pakket van transportlaag wordt door IP-laag verwerkt
- IP consulteert SPD (is IPSec vereist? zo ja hoe?)
- mogelijke resultaten
  - laat pakket vallen (drop)
  - geen IPSec vereist
    - IP-header toegevoegd
    - pakket doorgegeven naar netwerklaag
  - wel IPSec vereist ➔ zie verder hieronder
- zoek SA in SAD
  - indien niet bestaand ➔ stel nieuwe SA op (via IKE)
- voeg AH en/of ESP toe zoals SA voorschrijft
- deels geïllustreerd in volgende figuur
- bij routering nog extra stappen

IPSec verwerking: uitgaand verkeer (2)



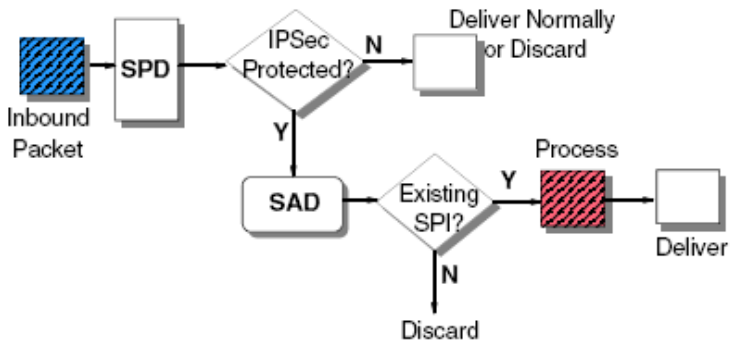
IPSec verwerking: inkomend verkeer

- indien geen IPSec header aanwezig
  - check policy in SPD
    - = discard ➔ drop pakket
    - = apply doch geen SA's ➔ drop pakket
    - anders: pakket doorgegeven naar hogere laag
- indien wel IPSec headers ➔ pakket verwerkt door IPSec-laag
- <SPI + destination addr + protocol> bepalen SA in SAD
- AH of ESP laag behandelen payload
- SPD wordt geconsulteerd om policy te bepalen
- is SA correct gebruikt (vb. komen adressen overeen met die van policy)?
- zo ja ➔ payload doorgegeven naar hogere laag

IPSec 19

IPSec verwerking: inkomend verkeer (2)

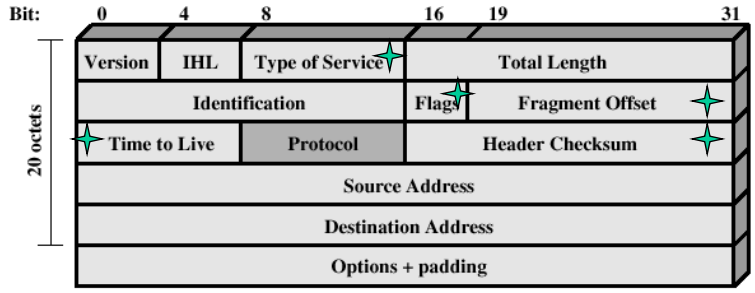
figuur (IBM Redbook VPN voll (p58) beschrijft andere volgorde van acties, maar komt op zelfde neer



IPSec 20

IP-pakket

- IP-header + IP-payload
- figuur = IPv4 header (Protocol == NextHeader in IPv6)



= veranderbaar veld

IPSec 21

IPSec werkingsmodi

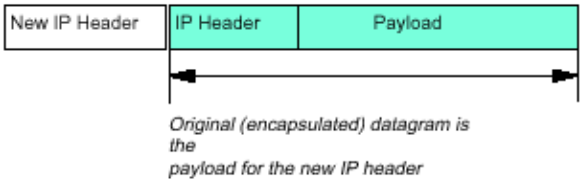
- AH en ESP protocols werken beide op twee manieren
- transport-mode
- tunnel-mode

IPSec 22

IPSec: transport-mode

- biedt bescherming voor
  - payload
  - = protocols in bovenlagen (TCP, UDP, ICMP)
- beschermt typisch end-to-end communicatie
- AH of ESP komen ná IP-hoofding en pakken slechts de rest van pakket in
- ESP encrypteert (+authentiseert) IP-payload, niet IP-header
- AH authenticeert IP-payload, gedeeltelijk IP-header
- pakketten moeten worden geïnterpreteerd door de ontvanger

IPSec: tunnel-mode (1)



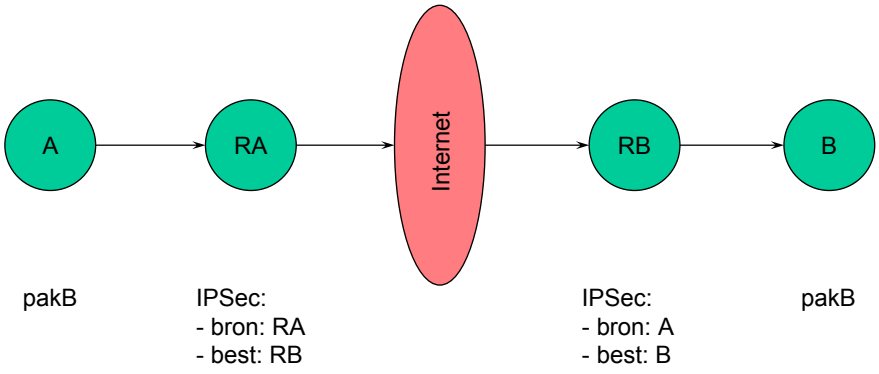
Original (encapsulated) datagram is the payload for the new IP header

- biedt bescherming aan het gehele IP-pakket
- origineel pakket + AH of ESP velden worden volledig in nieuw pakket ingebed
- indien origineel pakket is geëncrypteerd, kan de oorspronkelijke bestemming of oorsprong niet worden achterhaald

IPSec: tunnel-mode (2)

- laat uitwisseling van pakketten toe met private adressen over publiek netwerk
- Voorbeeld:
  - host A maakt pakket met adresB voor host B op ander netwerk
  - wordt verzonden naar veilige router op de grens van netwerk A
  - router filtert uitgaande pakketten en bepaalt de nood aan behandeling door IPSec
  - router pakt oorspronkelijk IP-pakket in een nieuw pakket in:
    - **bron IP-adres = router**
    - **bestemming IP-adres = router netwerkB**
  - pakket wordt geleid naar router netwerkB
  - router netwerkB stript IP-header en past IPSec toe
  - oorspronkelijk pakket wordt aan B geleverd

IPSec: voorbeeld tunnel-mode



Zijsprong: IP-spoofing

- aanvaller zendt pakketten met incorrect bronadres
- antwoorden worden naar verkeerd adres gestuurd, niet noodzakelijk naar de aanvaller
- drie mogelijkheden:
  - de aanvaller kan de antwoorden onderscheppen en zo een onbeperkte *gekaapte* verbinding in stand houden
  - de aanvaller hoeft de antwoorden niet te zien, bijvoorbeeld bij een *denial of service* aanval
  - de aanvaller wil de antwoorden niet zien
    - er worden antwoorden gestuurd naar een ander slachtoffer door een nietsvermoedende afzender
    - adres van afzender en bron is zelfde, computer hangt

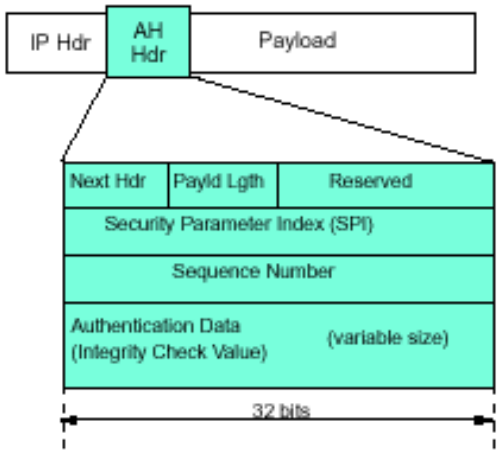
AH: Authentication Header (1)

- voorziet in … van IP-datagrams
  - integriteit
  - authenticatie
  - optioneel: bescherming tegen *replay*
  - vermijdt IP-spoofing
- geen authenticatie van veranderbare velden in IP header
  - type of service
  - flags
  - fragment offset
  - time to live
  - header checksum
- anders tunnel-mode gebruiken

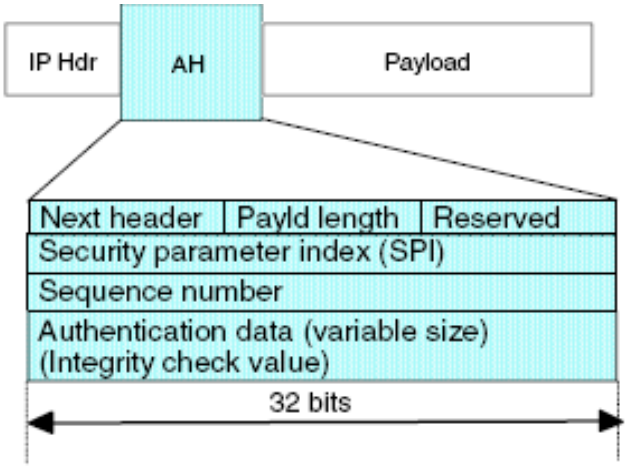
AH: Authentication Header (2)

- protocolnummer = 51 (of NextHeader in IPv6)
- werkt alleen in op niet gefragmenteerde pakketten
- IPSec-pakket kan nadien
  - wel worden gefragmenteerd verzonden
  - opnieuw geassembleerd worden
  - vooraleer IPSec opnieuw wordt toegepast
- pakketten met niet geslaagde authenticatie worden niet naar hogere lagen doorgegeven

AH hoofding



AH hoofding



AH hoofding

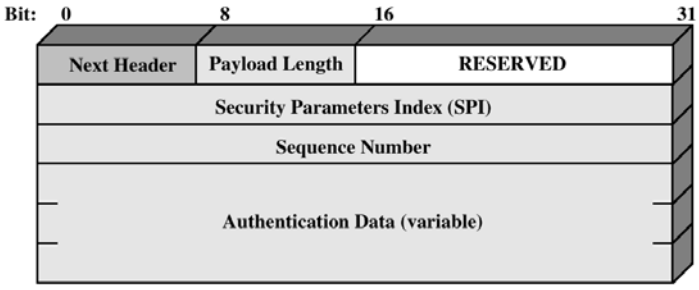


Figure 6.3 IPSec Authentication Header

AH hoofding (2)

- Next Header
  - 8 bits identificeren het type header dat vlak na de AH komt
  - overgenomen van protocolnummer van IP-header
- Payload Length (lengte van de AH in 32bit woorden)
- reserved
  - voor gebruik in de toekomst (?)
  - 16 bits = 0
- SPI (security parameter index, identificeert SA)
- …

AH hoofding (3)

- Sequence number
  - 32-bitwaarde van teller die monotoon stijgt
  - bescherming tegen anti-replay (optioneel)
  - niet gebruikt met manuele sleuteluitwisseling of oude RFC
- Authentication Data
  - bevat *Integrity Check Value* (ICV)
  - berekende MAC volgens afspraken in SA
    HMAC-MD5-96 of HMAC-SHA1-96 berekend over:
    - immutable IP header fields (mutable=0 voor de berekening)
    - AH header zonder authentication data (auth data =0 voor de berekening)
    - gegevens van bovenliggende protocols (vb. TCPsegment)
  - beperkt tot eerste 96 bits

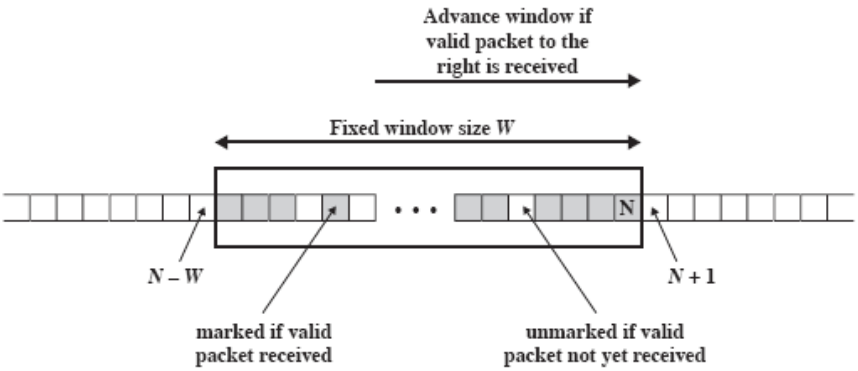
Anti-Replay voorziening (1)

- replay
  - aanvaller krijgt kopie van geauthentiseerd pakket
  - verstuurt het later opnieuw naar bestemmeling
  - ontvangst kan dienst onderbreken of …
- AH bevat teller (Sequence Number)
- opzetten van nieuwe SA impliceert teller=0
- bij elk verzonden pakket:
  - teller++ in veld van AH
- als teller==(2^{32}-1)
  - nieuwe SA opzetten

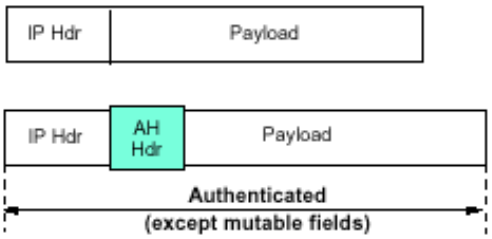
Anti-Replay voorziening (2)

- controle:
  - glijdend venster van W=64 (of …) pakketten
  - N is hoogste ontvangen pakketnummer
  - is bij ontvangst van een pakket
    - N-W < nummer <= N ➔ MAC wordt gecontroleerd
    - N < nummer
      - ➔ MAC wordt gecontroleerd
      - ➔ indien OK : venster wordt aangepast
  - pakket verworpen en melding als
    - MAC verkeerd
    - nummer <= N-W

Anti-Replay voorziening (2)

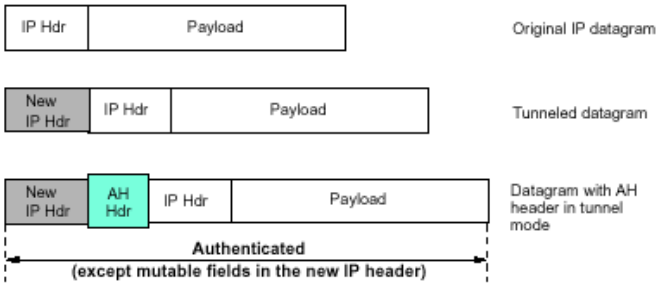


AH in transport-mode



- alleen gebruikt door hosts en niet door gateways
- gateways moeten niet noodzakelijk transportmode ondersteunen
- voordeel: weinig overhead
- nadeel: niet alle velden zijn geauthentiseerd

AH in tunnel-mode

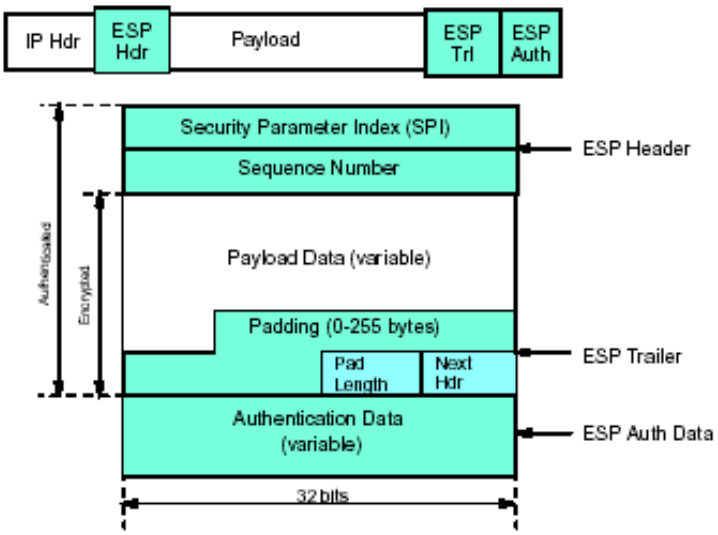


- altijd indien een van de SA uiteinden een gateway is
- binnenste en buitenste adressen kunnen verschillend zijn
- voordeel: volledige bescherming en private adressen mogelijk
- nadeel: meer overhead
- niet steeds geïmplementeerd

Encapsulating Security Payload

- voorziet in … van IP-datagrams
  - confidentialiteit (eigenlijk ook optioneel)
  - optioneel: integriteit en authentisering (gaan altijd samen)
  - optioneel: bescherming tegen *replay*
- aanbeveling: encryptie nooit alleen gebruiken (cryptanalyse mogelijk door het vervalsen van pakketten)
- werkt alleen op niet gefragmenteerde pakketten (cf. AH)
- pakketten met verkeerde authenticatie worden niet gedecrypteerd (vermindert werklading)
- protocolnummer = 50 (of NextHeader in IPv6)

ESP pakket



ESP pakket

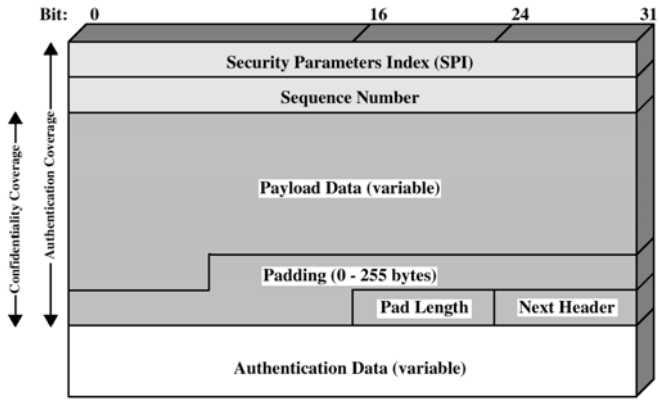


Figure 6.7 IPSec ESP Format

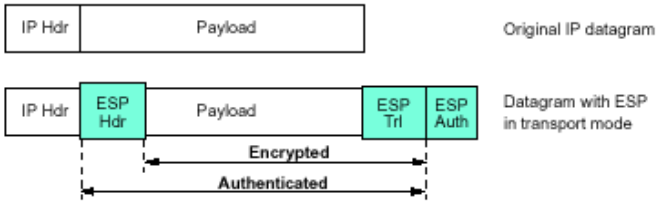
ESP pakket (2)

- SPI: security parameter index identificeert SA
- Sequence Number (zie AH)
- Payload Data
  - segment op transportniveau indien transportmode
    of
    IP-pakket in tunnelmode
  - bevat ook indien nodig initialisatievectoren voor encryptie-algoritme
  - geëncrypteerd volgens afspraken in SA
    3DES in CBC-mode met drie sleutels, RC5, IDEA, CAST, Blowfish, AES, …

ESP pakket (3)

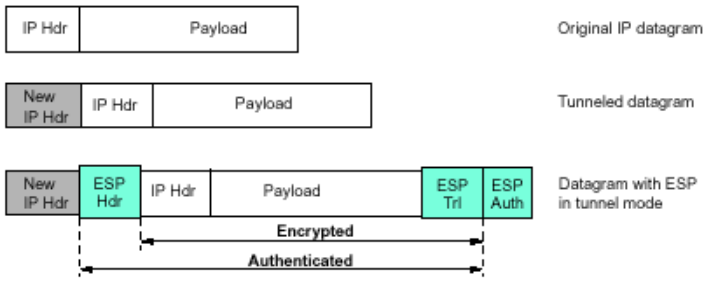
- Padding
  uitlijning nodig voor
  - encryptie-algoritme (geheel aantal blokken)
  - plaats van *PadLength* en *Next Hdr* in pakket (rechts uitgelijnd)
  - extra vertrouwelijkheid: door opvullen werkelijke lengte van payload verbergen.
- Next Header
  - identificeert data in payload (vb TCP-info)
- Authentication Data
  - cfr AH
  - IP-header niet in rekening genomen

ESP in transport-mode



- geen authenticatie van IP-header
- geen encryptie van IP-header
- nadeel: valse pakketten kunnen aangeboden worden vóór verwerking door ESP + analyse van trafief mogelijk
- voordeel: weinig overhead
- alleen gebruikt bij hosts, niet bij gateways

ESP in tunnel-mode



opmerkingen zoals bij AH:

- altijd indien een van de SA uiteinden een gateway is
- binnenste en buitenste adressen kunnen verschillend zijn
- voordeel: volledige bescherming en private adressen mogelijk
- nadeel: meer overhead
- niet steeds geïmplementeerd

Authentisering op 2 manieren?

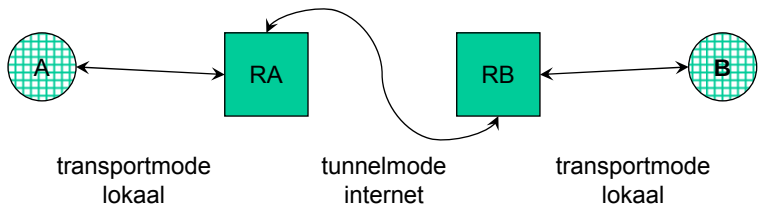
- Waarom bestaat AH ?
- Waarom bij ESP geen authentisering van IP-header?

Geen officieel antwoord, maar:

- ESP vereist sterke cryptografe algoritmen, niet in alle landen toegelaten; er zijn geen restricties voor authentisering
- soms alleen authentisering gewenst, dan is AH performanter dan ESP (complexere opbouw)
- ESP en AH kunnen ook worden gecombineerd met voordelen van beide

Combineren van SA's (1)

- één SA = één protocol in één richting
- AH en ESP alleen of gecombineerd in twee modi
- eventueel verschillende eindpunten
- van de vele mogelijke combinaties zijn er slechts enkele zinvol



Combineren van SA's (2)

- combinaties worden samengevoegd in SA-bundels
- SA-bundel
  - sequentie van SA's die moeten gebruikt worden na elkaar om gewenst IP-sec effect te verkrijgen
  - SA's mogen eindigen in de zelfde of verschillende eindpunten
- twee benaderingen:
  - *transport adjacency* (nabijheid)
  - *iterated tunneling* (genest)

zie verder …

Combineren van SA's (3)

- *transport adjacency*
  - verschillende protocols toegepast op zelfde IP-pakket
  - authenticatie van geëncrypteerde gegevens (zie figuur bord)
  - AH na ESP (zonder authenticatie) toegepast
  - in transportmode (geen tunneling)
  - toepassing van meer dan 2 protocols heeft geen zin (slechts 1 pakket)
  - voordeel:
    authenticering van AH beslaat meer velden dan die van ESP
  - nadeel:
    meer werk

Waarom niet ESP ná AH? (transport adjacency)

- IP-header bevat protocol van IP-payload
  - http://www.iana.org/assignments/protocol-numbers
- AH authenticeert ook IP-header, incl protocol
- indien nadien nog ESP toegepast:
  - AH + payload wordt omgeven door ESP-headers
  - IP-protocol moet veranderd worden
  - gegevens voor authenticatie kloppen niet meer

Toch ESP ná AH?

- vaak authenticatie vóór encryptie gewenst
  - gegevens van authenticatie kunnen niet gewijzigd worden
  - gegevens van authenticatie kunnen bij boodschap worden opgeslagen
- niet mogelijk bij transport adjacency
- wel bij iterated tunneling

Combineren van SA's (4)

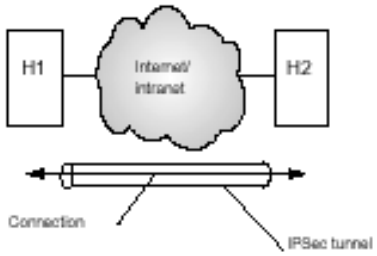
- *iterated tunneling*
  - beide protocols worden na elkaar toegepast
    vaak eerst transportmode, dan tunnelmode
  - na elke toepassing, creatie van nieuw pakket en aangeboden aan volgend protocol
  - aantal vernestelde protocols onbeperkt
    (in praktijk meestal 2, maximaal 3)
  - telkens verschillende eindpunten

Combineren van SA's (5)

Opmerkingen:

- combinatie van beide benaderingen is mogelijk
- toegepast voor VPN's
- indien SA's met verschillende eindpunten, minstens 1 niveau van tunneling (niet mogelijk met transport)
- bij ontvangst eerst authentisering dan encryptie behandelen (reden: liever geen foutieve pakketten decrypteren)
- bij verzenden dus eerst ESP dan AH
- Gebruiken we ESP met authentisering?
  alleen zinvol als ESP-SA verder reikt dan AH-SA
  vb.: ESP end-to-end en AH slechts tot gateway
- 4 praktijkvoorbeelden

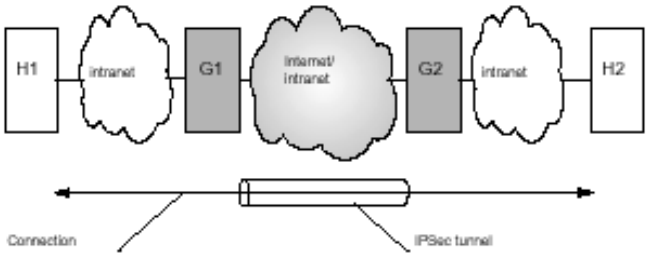
1. End-to-End beveiliging



- geen gateways
- ESP, AH of beide
- mogelijke combinaties:
  - Transportmode:
    - **AH alleen, ESP alleen, AH ná ESP (transport adjacency)**
  - Tunnelmode
    - **AH alleen, ESP alleen**
    - **AH of ESP na transportmode (laat encryptie van de authentisering toe)**

IPSec 55

2. Basis VPN opbouw



- hosts H1 en H2 voorzien geen IPSec
- gateways G1 en G2 voorzien IPSec in tunnel-mode, AH en/of ESP
- vermits zelfde eindpunten, heeft iterated tunneling geen zin
- wel bv ESP in tunnel-mode en nadien AH in transport-mode

IPSec 56

ESP tunnel + AH transport

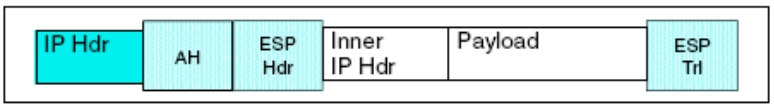
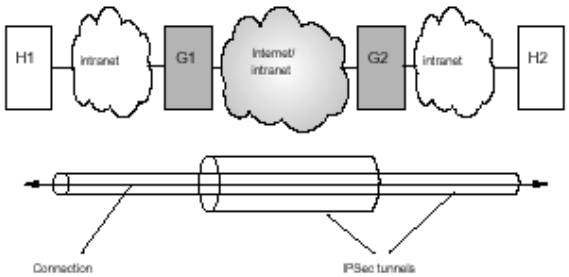


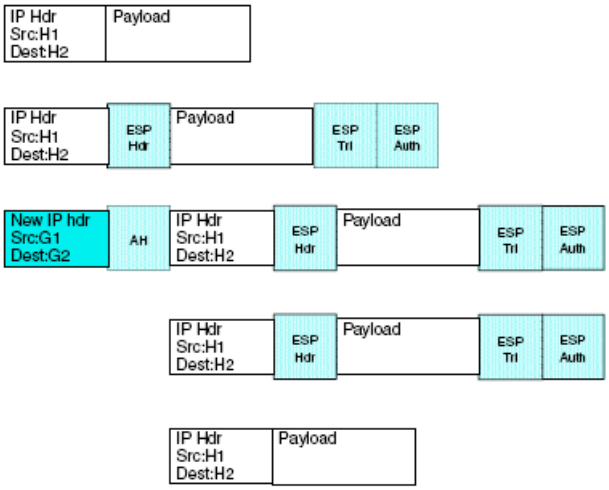
Figure 293. Combined AH-ESP tunnel

3. End-to-End beveiliging + VPN

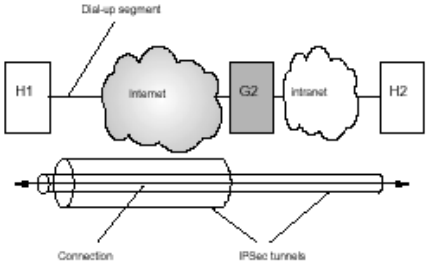


- hosts H1 en H2 voorzien wél IPSec
- typische opbouw: (zie figuur volgende dia)
  - G's: AH in tunnelmode
  - H's: ESP in transportmode
- beter: tussen G's AH-ESP tunnel zodat eindadressen niet kunnen worden achterhaald (bundel van 3 SA's → kostelijk)

AH tunnel + ESP transport



4. Remote Access



- host H1 belt in naar ISP
- tunnelmode tussen H1 en G2 (keuzes zie geval 2)
- tussen H1 en H2: tunnel of transport (zie geval 1)
- typische opbouw (2 gevallen):
  - H1-G2: AH in tunnel-mode H1-H2: ESP in transport-mode
  - H1-G2: AH-ESP tunnel H1-H2: ESP in transport-mode