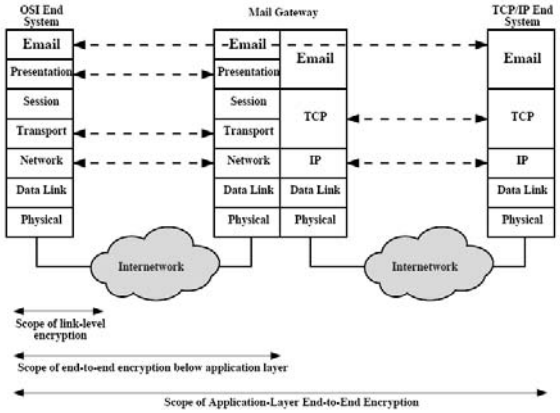
Bereik van encryptie – beveiliging

beveiliginstoepassingen: PGP, S/MIME, Kerberos, SSL, SET, …

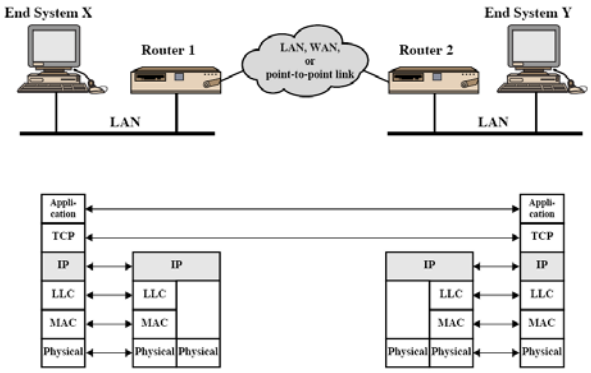


IPSec: IP security protocol

- IP heeft zelf geen beveiliging
- IP-pakketten
  - adres kan worden vervalst
  - payload kan bekeken worden
  - payload kan aangepast worden
  - kan opnieuw worden verstuurd
- beveiliging moet zorgen voor
  - echtheid van adres van de afzender
  - echtheid van de inhoud van IP-Pakket
  - geheimhouding van inhoud (en adres?)

IPSec: IP security protocol (2)

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



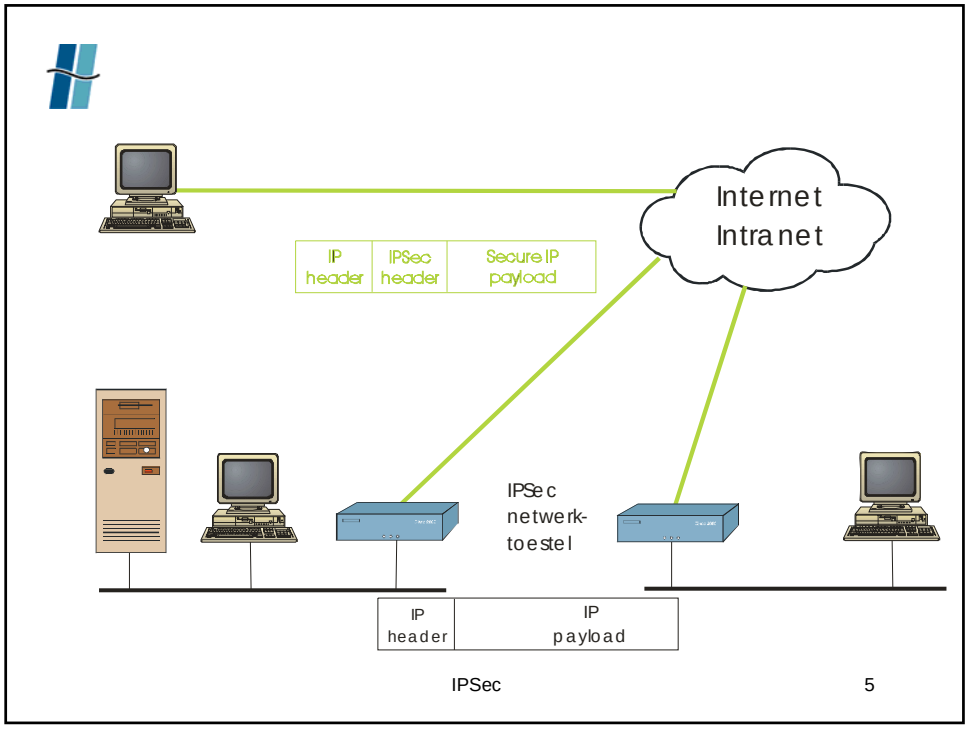
Data Link:
LLC = logical link control
MAC = Media Access Control

3

IPSec: IP security protocol (3)

- 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 4



IPSec 5

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

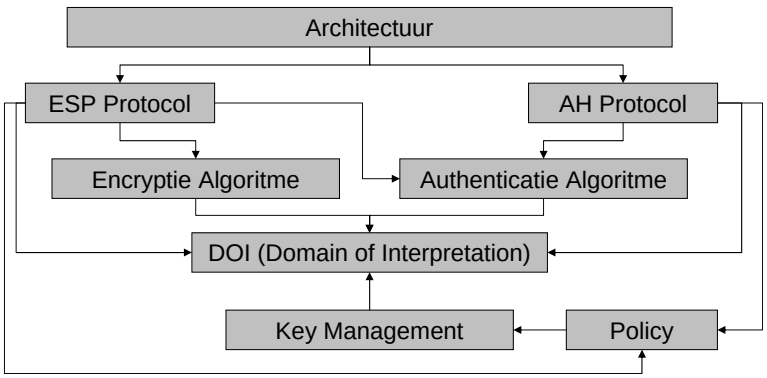
- samengevat:
  - voor elke applicatie kan alle trafiek geëncrypteerd en geauthenticeerd worden op IP-niveau

IPSec 6

IPSec: specificatie (1)

- vrij complex
- gedefinieerd in verschillende RFC's
  - incl. RFC 2401 (→ 4301) / 2402 / 2406 / 2408 + andere
- categorieën:
  - architectuur
    - algemene concepten, definities, vereisten i.v.m. veiligheid, mechanismen, ...
  - ESP en AH
    - algemeen gebruik en pakketinfo
    - welke diensten en formaat van hoofdingen
    - geen transformaties
  - encryptiealgoritmen
    - welke en hoe te gebruiken bij ESP
  - authenticatiealgoritmen
    - welke en hoe te gebruiken bij ESP en AH

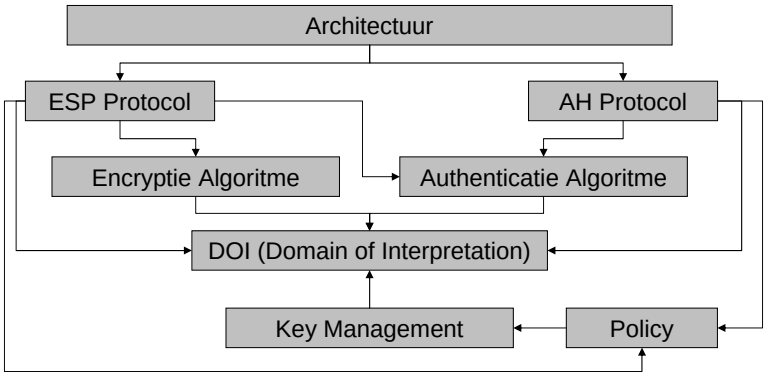
IPSec: samenhang documenten



IPSec: specificatie (2)

- categorieën (vervolg):
  - sleutelbeheer
    - IKE maakt sleutels voor alle IPSec-protocollen ook voor OSPF (routing protocol)
    - generische payload
    - geen onderhandeling van parameters (vb. initialisatievectoren)
  - Domain of Interpretation (referenties naar andere documenten)
    - onderhandeling over parameters in ≠ protocollen
  - Policy
    - kunnen entiteiten via IPSec communicieren?
    - als ja → welke transformaties (AH, ESP, algo's) nodig?
    - beschrijft voorstelling: hoe beleid opslaan en bevragen
    - beschrijft implementatie: hoe beleid uitvoeren via transformaties

IPSec: samenhang documenten



Bestanddelen van IPSec (1)

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
- …

IPSec 11

Bestanddelen van IPSec (2)

IPSec derde protocol:

- IKE (Internet Key Exchange):
  - raamwerk voor onderhandeling van
    - SA's (security associations)
    - cryptografische sleutels (+ uitwisseling)
  - gebruikt onderdelen van
    - Internet Security Association and Key Management Protocol (ISAKMP)
    - Oakley
    - SKEME
- IKE alleen gebruikt om ESP en AH te kunnen definiëren en gebruiken

IPSec 12

Overzicht IPSec-diensten

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

Toegangscontrole IPSec

- AH en ESP pas bruikbaar na toegangscontrole
- gebeurt tijdens distributie van sleutels in IKE
- publieke-sleutelcrytografie alleen tijdens IKE
- te traag voor encryptie en authenticatie per pakket
- AH gebruikt HMAC
- ESP gebruikt symmetrische encryptie

Security Association (SA)

- 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
  - A beschikt over $SA1_{in}$ en $SA2_{uit}$
  - B beschikt over $SA1_{uit}$ en $SA2_{in}$
- SA is protocolspecifiek: één SA geldt voor
  - ofwel AH
  - ofwel ESP
  - niet beide samen

SA gegevensbanken

- steeds aanwezig bij elke implementering van IPSec
- SAD (association) en SPD (policy)
- verborgen door de gebruikersinterface
- beide geraadpleegd om beveiliging pakket te kennen
- beleid (policy) bepaalt
  - protocol (AH, ESP) en mode (transport, tunnel)
  - transformaties
  - hoe pakket moet worden behandeld, i.f.v.
    - **bron- en bestemmingsadres (IP)**
    - **en protocol en poort op transportniveau (TCP)**
- bij ontvangst
  - transportgegevens beschikbaar na verwerking van IPSec
  - dus …

Identificatie SA

- ➔ SA + policy identificeren zonder transportgegevens
- SA geïdentificeerd door 3 parameters, uniek bij ontvanger
  - Security Parameter Index (**SPI**)
    - 32 bits
    - identificeert SA in lokale inkomende SAD
    - uniek voor ontvanger, door hem bepaald bij "onderhandeling"
  - **IP-adres** van bestemming bij ontvanger (unicast)
  - Security Protocol Identificatie (AH of ESP)
- IP-pakket bevat IPSec-hoofding (AH of ESP)
- SPI maakt deel uit van IPSec-header
- SPI + bestemmingsadres bepalen SA
  ➔ ontvanger weet hoe pakket moet worden behandeld

SA gegevensbanken (2)

- consultatie bij inkomend verkeer
  - pakket bevat SPI, bestemmingsadres en protocol (AH/ESP)
  - SPD en SAD worden geconsulteerd om te weten hoe het pakket moet worden behandeld
  - zie verder
- consultatie bij uitgaand verkeer
  - SPD bepaalt welke SA moet worden gebruikt voor pakketbehandeling
  - SA info wordt uit SAD gehaald

Security Association Database (1)

- bevat entry voor elke SA
- ingang bevat o.a.
  - informatie over het protocol (AH of ESP)
    - algoritmen, sleutels + levensduur
  - sequentienummer
    - waarde in te vullen in header van het pakket
    - nr++ bij verzending van elk volgend pakket
    - gebruikt bij ontvangst voor controle op heruitzenden
  - overflow sequentienummer
    - boolean: true == nummer is te groot geworden
    - gebruikt bij verzenden van pakketten
    - policy zegt: verder pakketten sturen of overdracht stoppen
  - …

IPSec 19

Security Association Database (2)

- ingang bevat o.a. (vervolg …)
  - mode waarin protocol is gebruikt:
    - transport of tunnel
  - levensduur van de SA
    - # overgedragen bytes of tijdsduur
    - indien overschreden → SA niet meer gebruiken
    - kernel kan zorgen dat tijd voordien nieuwe SA wordt opgezet
  - PMTU (path max transmission unit)
    - max grootte van pakket voor pad zonder fragmentatie
  - anti-replay window
    - gebruikt samen met sequentienummer
    - bepaalt of pakket eventueel reeds vroeger werd ontvangen

IPSec 20

Beleid en SPD

- IPSec-beleid kan vb. bepalen
  - verkeer tussen lokaal onbeveiligd subnet en net van een andere router: encryptie (AES) + authenticatie (HMAC-MD5)
  - telnet-verkeer naar mailserver op ander subnet: encryptie (3DES) + authenticatie (HMAC-SHA)
  - web-verkeer naar andere server: encryptie (IDEA) + authenticatie (HMAC-RIPEMD)
  - ander verkeer onbeveiligd
- beleid vastgelegd in Security Policy Database (SPD)
- elke entry definieert trafiek en legt vast
  - bescherming of niet
  - hoe
  - met welke netwerkentiteit bescherming gemeenschappelijk is

Security Policy Database SPD (1)

- bevat vergelijkbare regels als die van firewall of packet-filter
- bepaalt manier waarop bepaalde 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
  - protocol transportlaag
    - NextHeader field IPv6, Protocol IPv4
    - 1 nummer, lijst, bereik
  - TCP of UDP poorten van bron en bestemming
    - aparte poortnummers, lijst, wildcard
  - userID
    - gebruikt bij IKE
  - actie
    - verwijzing naar al dan niet beveiliging via SA('s)
    - ...

Security Policy Database SPD (3)

- mogelijke acties
- DISCARD
  - pakket wordt gedropt, mag niet binnen of buiten
- BYPASS
  - uitgaand pakket ➔ geen beveiliging
  - inkomend pakket ➔ er zou geen IPSec mogen toegepast zijn
- PROTECT
  - entry verwijst naar SA of SA-bundel in SAD
  - uitgaand pakket ➔ gepaste IPSec-beveiliging wordt toegepast
  - inkomend ➔ controle nadien of pakket gepaste beveiliging had

Security Policy Database SPD (4)

- aparte ingangen op elke interface voor
  - inkomend verkeer
  - uitgaand verkeer
  - ofwel twee aparte SPD's (afh. van implementatie)
- 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

SPD (5): een voorbeeld (Stallings)

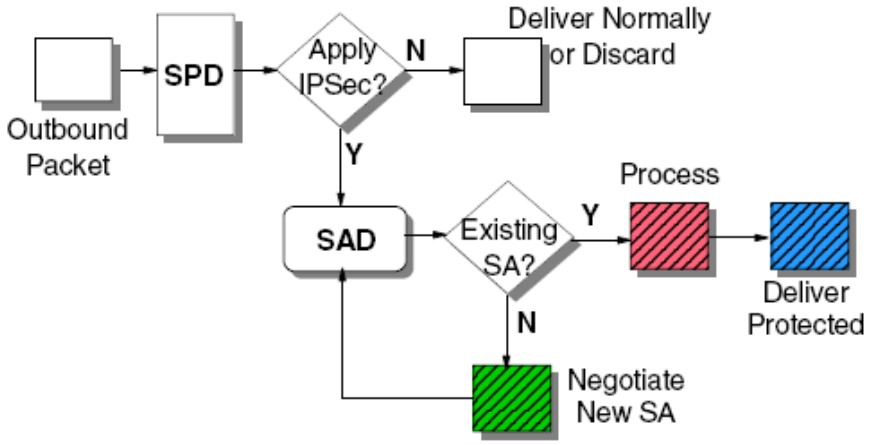
Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

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, actie==DISCARD)
  - geen IPSec vereist (actie == BYPASS)
    - **IP-header toegevoegd**
    - **pakket doorgegeven naar netwerklaag**
  - wel IPSec vereist (actie == PROTECT) ➔ 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
- bij routering nog extra stappen (zie verder)

IPSec 27

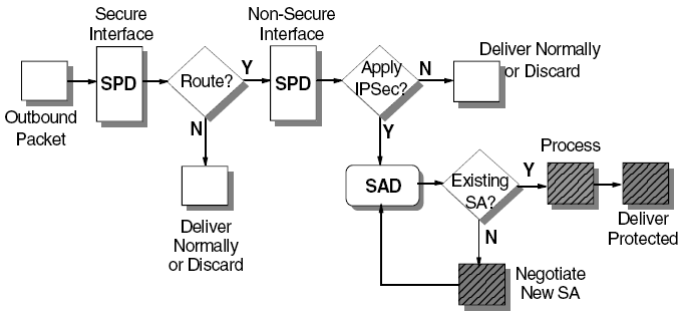
IPSec verwerking: uitgaand verkeer (host)



IPSec 28

IPSec verwerking uitgaand router

- consultatie SPD van interface waar pakket is ontvangen
- routeren? → routetabel → SPD andere interface

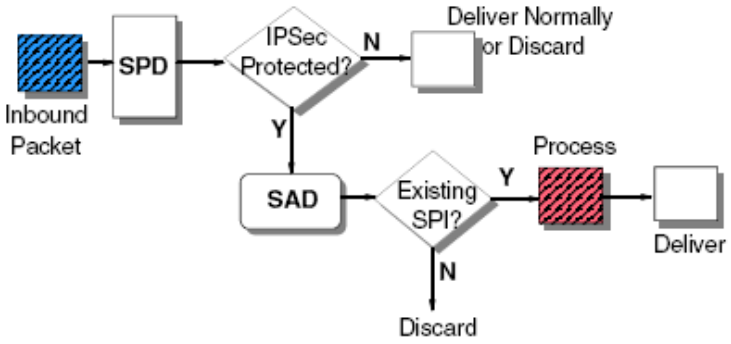


IPSec verwerking: inkomend verkeer

- indien geen IPSec header aanwezig
  - check policy in SPD
    - == discard → drop pakket
    - == protect doch geen ISec dus geen SA's → drop pakket
    - anders: pakket wordt 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, gebruikte beveiliging==die van SPD)? (fig. existing spi?)
  - zo ja → payload doorgegeven naar hogere laag
  - zo neen → drop pakket

IPSec verwerking: inkomend bij host

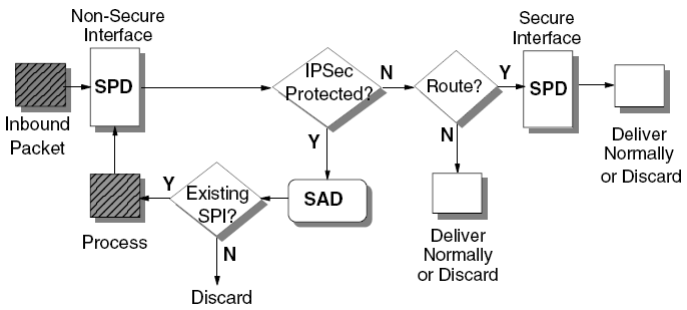
figuur (IBM Redbook VPN voll (p58) beschrijft andere volgorde van acties: SPD raadplegen na vraag *IPSec protected?*



IPSec verwerking: inkomend bij router

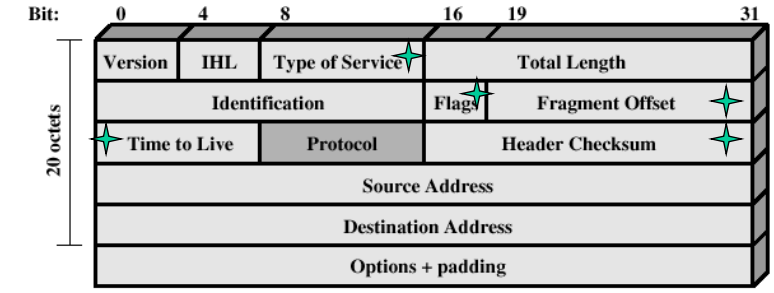
figuur (IBM Redbook VPN voll)

volgorde van acties: SPD raadplegen na vraag *IPSec protected?*



IP-pakket

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



= veranderbaar veld

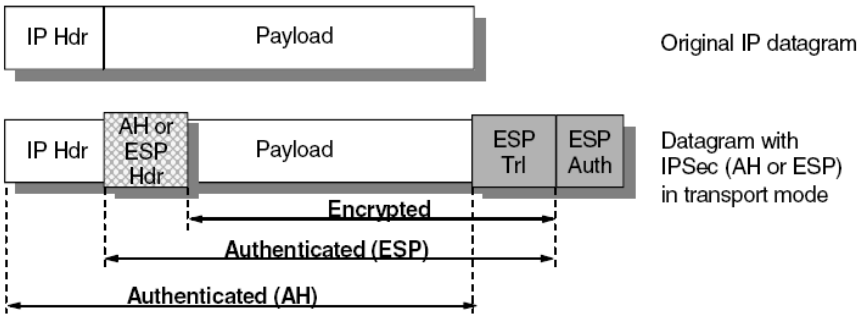
IPSec 33

IPSec werkingsmodi

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

IPSec 34

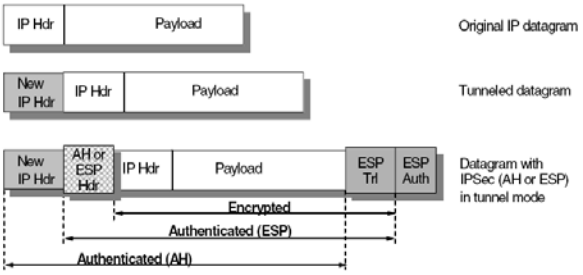
IPSec: transport-mode (1)



IPSec: transport-mode (2)

- 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 (+authenticeert) IP-payload, niet IP-header
- AH authenticeert IP-payload, gedeeltelijk IP-header
- pakketten moeten worden geïnterpreteerd door de ontvanger

IPSec: tunnel-mode (1)

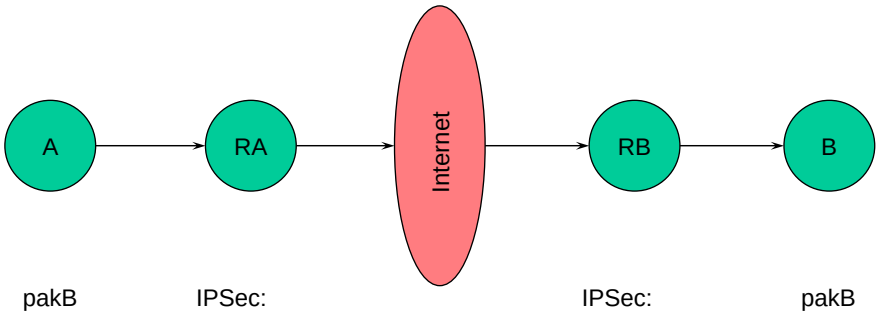


- biedt bescherming aan het gehele IP-pakket
- origineel pakket wordt volledig in nieuw pakket ingebed
- nieuw pakket wordt beveiligd door IPSec in **transportmode**
- indien origineel pakket wordt geëncrypteerd (ESP), kan oorspronkelijke bestemming of oorsprong niet worden achterhaald

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 A**
    - **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



pakB

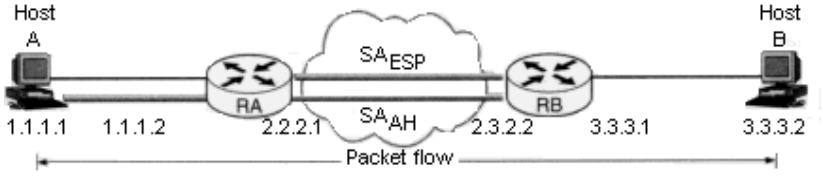
IPSec:
- bron: RA
- best: RB

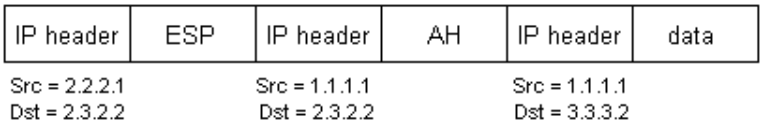
IPSec:
- bron: A
- best: B

pakB

IPSec 39

IPSec: voorbeeld geneste tunnel





Src = 2.2.2.1
Dst = 2.3.2.2

Src = 1.1.1.1
Dst = 2.3.2.2

Src = 1.1.1.1
Dst = 3.3.3.2

- policy zegt: A authenticeert zich tov RB met AH (tunnel)
- VPN tussen RA en RB
- pakket = pakket zoals RB het ziet

40

Anti-Replay voorziening (1)

- replay
  - aanvaller krijgt kopie van geauthenticeerd pakket
  - verstuurt het later opnieuw naar zelfde bestemming
  - ontvangst kan dienst onderbreken of …
- IPSec bevat teller (Sequence Number) in hoofding
- opzetten van nieuwe SA impliceert teller=0
- bij elk verzonden pakket:
  - teller++ in veld van protocol-hoofding en in SAD-entry
- als teller==(2^{32}-1)
  - nieuwe SA opzetten (indien anti-replay)
- IP is connectieloos ➔
  pakketten komen niet allemaal toe (in volgorde)
- IPSec voorziet glijdend venster

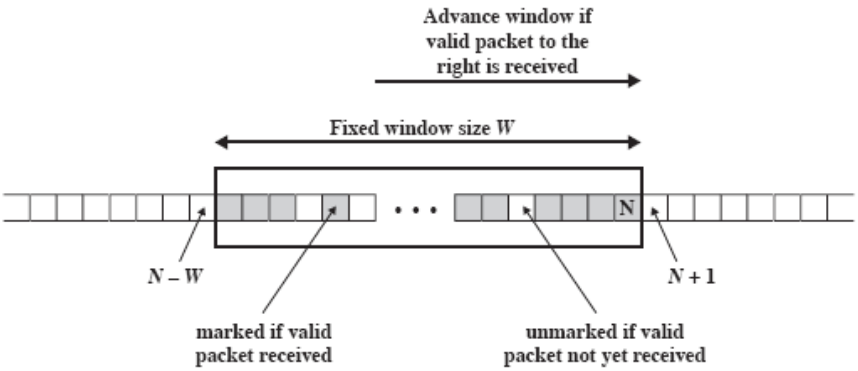
IPSec 41

Anti-Replay voorziening (2)

- controle bij ontvangst van pakketten:
  - glijdend venster van W=64 (of …) pakketten
  - N is hoogste ontvangen pakketnummer
  - is bij ontvangst van een pakket
    - N < nummer
      ➔ nieuw pakket, controle van authenticiteit
      ➔ indien OK : venster wordt aangepast (N=nummer)
      ➔ pakket aangeduid als ontvangen
    - N-W < nummer <= N
      ➔ drop indien reeds ontvangen
      ➔ anders controle authenticiteit
      ➔ indien OK : pakket aangeduid als ontvangen
  - pakket verworpen en melding als
    - authenticiteit niet OK
    - nummer <= N-W

42

Anti-Replay voorziening (3)



IPSec 43

Zijsprong: IP-spoofing

- Source address 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

IPSec 44

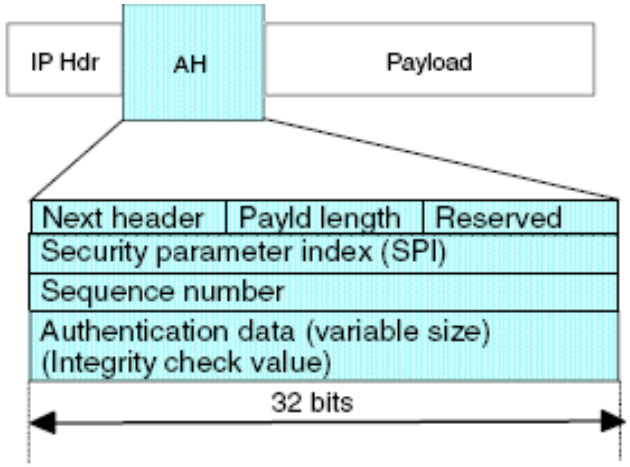
AH: Authentication Header (1)

- 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)
  - vervangt protocol in originele IP-header
- 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

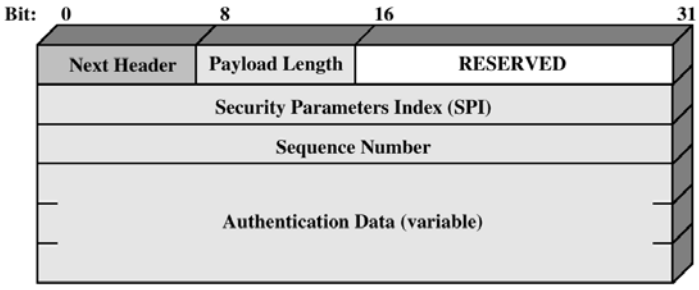


Figure 6.3 IPSec Authentication Header

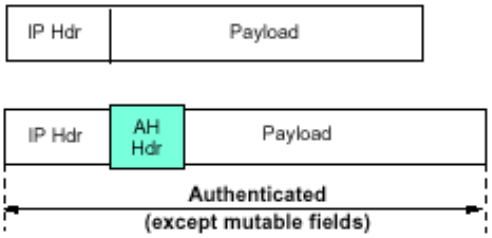
AH hoofding (2)

- Next Header
  - 8 bits identificeren het type header dat vlak na de AH komt
  - overgenomen van protocolnummer van IP-header
    - dit laatste wordt nadien 51
- 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)

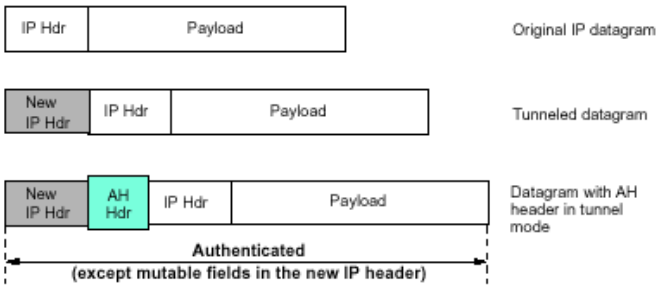
- Sequence number
  - 32-bitwaarde van teller die monotoon stijgt
  - bescherming tegen anti-replay (optioneel)
  - niet gebruikt met manuele sleuteluitwisseling of oude RFC
- Authentication Data
  - bevat *Integrity Check Value* (ICV)
  - berekende MAC volgens afspraken in SA
    HMAC-SHA1-96 (moet) of HMAC-MD5-96 (mag) of AES-XCBC-MAC-96 (zou moeten) 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)
  - meestal beperkt tot eerste 96 bits

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

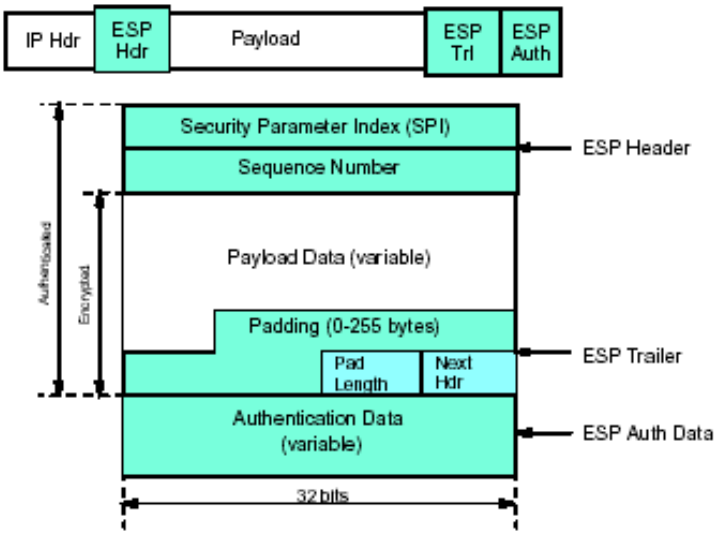


- altijd tunnel indien een van de SA-uiteinden een gateway is
- binnenste en buitenste adressen kunnen verschillend zijn
- voordeel: volledige bescherming (auth) en private adressen mogelijk
- nadeel: meer overhead
- niet steeds geïmplementeerd

Encapsulating Security Payload

- voorziet in … van IP-datagrams
  - confidentialiteit (eigenlijk ook optioneel)
  - optioneel: integriteit en authenticatie (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

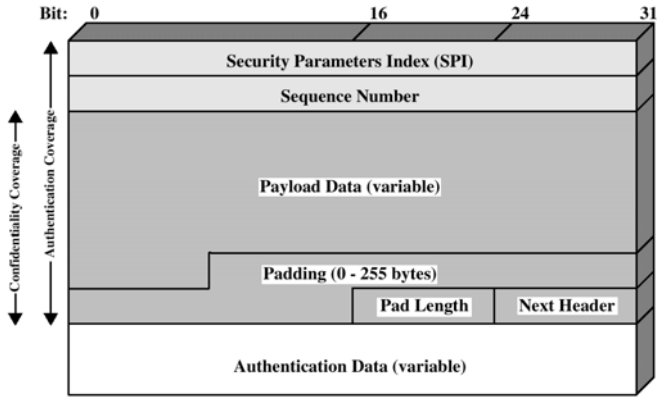


Figure 6.7 IPSec ESP Format

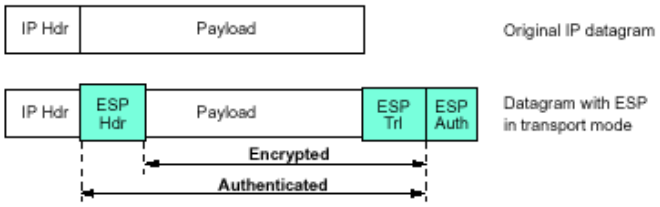
ESP pakket (2)

- 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 (RFC 4835 / 2007)
    MUST NULL (1)
    MUST- TripleDES-CBC [RFC2451]
    MUST AES-CBC with 128-bit keys [RFC3602]
    SHOULD AES-CTR [RFC3686]
    SHOULD NOT DES-CBC [RFC2405] (3)

ESP pakket (3)

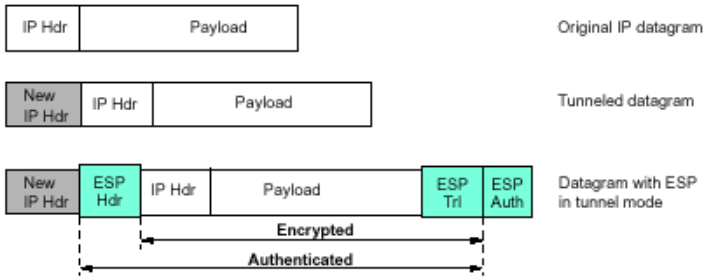
- Padding
  uitlijning nodig voor
  - encryptie-algoritme (geheel aantal blokken)
  - plaats van *PadLength* en *Next Hdr* in pakket (rechts uitgelijnd)
  - extra vertrouwelijkheid: door opvullen werkelijke lengte van payload verbergen.
- Next Header
  - identificeert data in payload (vb TCP-info); cf.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

Authenticatie 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 authenticatie
- soms alleen authenticering gewenst, dan is AH performanter dan ESP (complexere opbouw)
- ESP en AH kunnen ook worden gecombineerd met voordelen van beide