Palomuurit I

Palomuurin tehtävät:

Palvelunhallinta: Palomuuri määrää, minkätyyppisiä internetin palveluja voidaan käyttää tai luovuttaa käytettäväksi. Palomuuri voi suodattaa tietoliikennettä perustuen IP-osoitteeseen, protokollaan tai porttiin. Se voi ottaa vastaan ja tulkita sovellustason palvelupyyntöjä ja tutkia ne, ennen kuin se päästää ne läpi. Palomuurissa voi myös sijaita palveluja, kuten Web ja sähköposti.

Suunnanhallinta: Määrittelee, mihin suuntaan palveluja voidaan pyytää tai tarjota.

Palomuurit II

Käyttäjänhallinta: Palomuuri voi toteuttaa pääsynvalvontaa palveluihin. Tällaista pääsynvalvontaa sovelletaan tyypillisesti palomuurin sisäpuolella oleviin käyttäjiin. Pääsynvalvontaa voidaan soveltaa myös sisäverkon ulkopuolella oleviin, mutta tällöin tarvitaan lisäksi muuta ohjelmistoa suojaamaan verkon yli tapahtuvaa liikennettä (esim. IPsec).

Käyttäytymisenhallinta: Säätelee, miten palveluja käytetään. Esimerkiksi palomuuri voi suodattaa roskapostin tai se voi rajoittaa Web-palveluihin tai -sivuille pääsyä.

Palomuurien piirteitä

1. Palomuuri määrittelee yhden kohdan, josta oikeutetut käyttäjät tai palvelut pääsevät sisäverkkoon tai sisäverkosta ulos. Täten se voi estää asiaankuulumattomia käyttäjiä tai vahingollisia palveluja pääsemästä sisäverkkoon tai palveluihin. Se suojelee erilaisilta huijaus- ja reitityshyökkäyksiltä. Yhden pääsykohdan käyttö yksinkertaistaa turvajärjestelyjä.
2. Palomuuri voi monitoroida turvallisuuteen liittyviä tekijöitä. Palomuureissä voi olla hälytysmekanismeja.
3. Palomuurissa voidaan tehdä monia operaatioita, jotka eivät suoraan liity turvallisuuteen. Esimerkiksi NAT-operaatiot.
4. Palomuuri voi toimia IPsec:in alustana virtuaalisia yksityisiä verkkoja toteutettaessa.

Palomuurien rajoituksia

1. Palomuuri ei voi suojella hyökkäyksiltä, jotka tapahtuvat palomuurin ohi. Verkolla voi olla yhteyksiä ulkomaailmaan muutakin kautta.
2. Palomuuri ei suojele sisältäpäin tulevilta hyökkäyksiltä.
3. Jos langattomat verkot on huonosti konfiguroitu, niihin saattaa päästä ulkopuolelta palomuurien ohi.
4. Kannettavaa tietokonetta voidaan käyttää palomuurin ulkopuolella, jolloin se voi saastua. Tämä voi lopulta saastuttaa koko sisäverkon.

Paketteja suodattava palomuuri I

Paketteja suodattava reititin soveltaa sääntöjä jokaiseen tulevaan ja lähtevään IP-pakettiin. Jos paketti noudattaa määriteltyä turvapolitiikkaa, se reititetään eteenpäin, muuten se tuhotaan. Suodatussäännöt käyttävät hyväkseen paketin tietoja:

- kohdeosoite,
- lähdeosoite,
- TCP- tai UDP-porttinumero,
- IP-protokollakenttä, joka määrittelee kuljetusprotokollan,
- jos reitittimellä on kolme tai useampia portteja, niin suodatusperusteena voi olla myös, mihin porttiin paketti tulee tai mistä se lähtee.

Esimerkki. Sääntö

Paketteja suodattava palomuuri II

action	*our host*	*port*	*their host*	*port*
allow	*	*	*	25

sanoo, että mikä tahansa sisäverkon kone voi lähettäää postia ulkopuolelle. TCP-paketti, jonka kohdeportti on 25, ohjataan kohdekoneen SMTP-palvelimelle. Ongelmana tässä säännössä on, että ulkopuolella olevassa koneessa portti 25 voi liittyä myös muuhun sovellukseen. Tähän liittyy seuraava sääntö:

action	*src*	*port*	*dest*	*port*	*flags*
allow	our hosts	*	*	25	
allow	*	25	*	*	ACK

Paketteja suodattava palomuuri III

Kun yhteys on luotu, TCP-segmentin ACK-lippu nostetaan, jotta toiselta koneelta lähetetyt segmentit kuitataan. Siten tämä sääntö sanoo, että sallitaan IP-paketit, joiden lähdeosoite on jokin luetelluista koneista ja kohdeportti 25. Se myös sallii sisään tulevat paketit porttiin 25, joissa on ACK-lippu päällä. □

Pakettisuodatuksen heikkouksia

- Sovellustason haavoittuvuuksia hyväksikäyttäviä hyökkäyksiä ei välttämättä havaita.
- Kirjanpito on rajoittunutta.
- Useimmat tämänkaltaiset palomuurit eivät tue käyttäjän todennusta.
- Ne ovat haavoittuvia hyökkäyksille, joissa käytetään hyväksi TCP/IP-protokollaperheen heikkouksia, esimerkiksi osoiteväärennöksiä.
- On myös helppo tehdä virheitä palomuurin konfiguroinnissa, minkä johdosta epätoivottuja paketteja pääsee läpi.

Seuraavassa on puolestaan joitakin hyökkäysyrityksiä ja niiden torjuntakeinoja:

- Hyökkääjä väärentää IP-osoitteeksi sisäverkon osoitteen. Hyökkäys torjutaan, jos hylätään paketit, jotka tulevat ulkopuolelta ja joissa on sisäverkon osoite.
- Lähettävä kone määrittelee reitin, jota paketti noudattaa kulkiessaan internetin läpi. Tavoitteena on hämätä vastustajan palomuuria. Torjunnassa hylätään kaikki paketit, jotka käyttävät lähdereititystä.
- Hyökkääjä käyttää IP:n paloitteluoptiota ja luo hyvin pieniä paketteja ja pakottaa TCP:n otsaketiedon vähintään kahteen palaan. Tavoitteena on kiertää suodatussääntöjä, jotka käyttävät TCP:n otsaketietoja. Hyökkääjä toivoo, että vain ensimmäinen pala tutkitaan ja muut pääsevät läpi. Torjunnassa vaaditaan, että ensimmäisen palan on sisällettävä tietty minimimäärä otsaketta. Jos ensimmäinen pala hylätään, palomuuri muistaa paketin ja hylkää myös seuraavat palat.

Tilat muistava palomuuri I

- Jotta ymmärrettäisiin pakettisuodatuksen heikkoudet ja tilat muistavan palomuurin tarve, tarkastellaan SMTP:n toimintaa (Simple Mail Transfer Protocol).
- Se perustuu asiakas/palvelin-malliin. Asiakas luo uusia sähköposteja ja palvelin hyväksyy tulevat sähköpostit ja vie ne vastaaviin käyttäjien postilaatikoihin. SMTP perustaa TCP-yhteyden asiakkaan ja palvelimen välille. Palvelimen porttinumero on 25 ja asiakkaan välillä 1024-65535. Asiakkaan numeron luo asiakas itse.
- Tyypillisesti kun TCP:tä käyttävä sovellus luo istunnon kaukaisen koneen kanssa, se perustaa TCP-yhteyden, jossa kaukaisen koneen poprttinumero on pienempi kuin 1024 ja paikallisen asiakassovelluksen porttinumero on välillä 1024-65535. Lukua 1024 pienemmät numerot edustavat hyvin tunnettuja protokollia. Luvut väliltä 1024-65535 luodaan dynaamisesti ja ne ovat voimassa vain TCP-istunnon ajan.

Tilat muistava palomuuri II

- Yksinkertaisen paketteja suodattavan palomuurin täytyy päästää sisään kaikki paketit, joiden porttinumero on välillä 1024-65535. Tätä voivat hyökkääjät käyttää hyväkseen. Tilat muistava palomuuri pitää kirjaa TCP-yhteyksistä. Jokaista luotua yhteyttä kohti on yksi tietue. Palomuuri päästää läpi vain ne paketit, jotka sopivat yhteen tietokannan tietojen kanssa.

Sovellustason yhdyskäytävä

- *Sovellustason yhdyskäytävä* (application-level gateway, proxy) välittää sovellustason liikennettä.
- Käyttäjä ottaa yhteyden yhdyskäytävään TCP/IP-sovelluksen avulla ja yhdyskäytävä kysyy sen kaukaisen koneen nimen, jonka kanssa käyttäjä haluaa kommunikoida. Kun käyttäjä vastaa ja todentaa samalla itsensä, yhdyskäytävä ottaa yhteyden kaukaiseen koneeseen ja ryhtyy välittämään paketteja käyttäjän ja kaukaisen koneen välillä. Jos yhdyskäytävä ei tue jotain palvelua, käyttäjä ei voi sitä käyttää. On myös mahdollista, että palvelusta voidaan käyttää vain tiettyjä osia.
- Sovellustason yhdyskäytävät ovat turvallisempia kuin paketti suodattimet, koska yhdyskäytäville voidaan määritellä vain muutamia sovelluksia, joista ne huolehtivat. On lisäksi helpompaa seurata liikennettä sovellustasolla. Haittana on ylimääräiseen prosessointiin kuluva aika.

Piiritason yhdyskäytävä I

- *Piiritason yhdyskäytävä* (circuit-level gateway) ei salli päästä-päähän TCP-yhteyksiä. Sen sijaan se perustaa kaksi TCP-yhteyttä, yhden itsensä ja paikallisen käyttäjän välille ja toisen itsensä ja kaukaisen koneen välille.
- Kun nämä yhteydet on perustettu, yhdyskäytävä välittää toisen yhteyden paketit suoraan toiselle yhteydelle tutkimatta sisältöä tarkemmin. Turvallisuus syntyy siitä, että yhdyskäytävä päättää, mitä TCP-yhteyksiä sallitaan.
- Piiritason yhdyskäytäviä sovelletaan tyypillisesti tilanteissa, joissa ylläpito luottaa sisäverkon käyttäjiin.

Piiritason yhdyskäytävä II

- Yhdyskäytävä voidaan konfiguroida sovellustason yhdyskäytäväksi sisään tulevan liikenteen suhteen ja piiritason yhdyskäytäväksi ulospäin menevän liikenteen suhteen. Tässä konfiguraatiossa yhdyskäytävä joutuu tutkimaan sisääntulevan liikenteen kiellettyjen toimintojen osalta, mutta sen ei tarvitse tehdä samaa ulosmenevän liikenteen suhteen.

Vallikone I

Vallikone (bastion host) on systeemi, joka suunnitellaan erityisen turvalliseksi. Tyypillisesti se toimii sovellustason tai piiritason yhdyskäytävän alustana. Sen ominaispiirteitä ovat:

- Vallikoneen käyttöjärjestelmä on erityisen turvallinen.
- Vain tarpeelliset palvelut ovat käytössä.
- Vallikone saattaa vaatia ylimääräistä autentikointia ennenkuin käyttäjä pääsee proxy-palveluihin.
- Jokainen proxy on konfiguroitu toteuttamaan vain osaa sovelluksen käskyjoukosta.
- Kukin proxy pitää yksityiskohtaista lokikirjaa liikenteestä, liitynnöistä ja kunkin liitynnän kestosta.
- Jokainen proxy-sovellus on oma pieni, suhteellisen yksinkertainen ja erityisesti verkon turvaamiseen suunniteltu ohjelmisto.

Vallikone II

- Kukin vallikoneella oleva proxy on itsenäinen, toisista proxyistä riippumaton.
- Proxy ei normaalisti tee muita levyoperaatioita kuin lukee oman konfiguraationsa.
- Kukin proxy on oikeudeton käyttäjä vallikoneen yksityisessä ja varmistetussa hakemistossa.

Palvelinkoneiden palomuurit

Tällainen on ohjelmisto, joka suojelee yksittäistä konetta. Monet käyttöjärjestelmät sisältävät tällaisen palomuurin, mutta se voidaan hankkia erillisenä. Edut:

- Suodatussäännöt voidaan suunnitella tarkemmin vastaamaan palvelua. Organisaation turvapolitiikka voidaan toteuttaa siten, että eri palvelimissa on erilaiset säännöt.
- Palomuuri on riippumaton topologiasta. Sekä ulkoiset että sisäiset palvelupyynnöt kulkevat palomuurin läpi.
- Jos palvelimen palomuureja käytetään yhdessä yleisten palomuurien kanssa, saadaan aikaan ylimääräinen turvataso. Uusi palvelu yhdessä siihen liittyvän palomuurin kanssa voidaan ottaa käyttöön muuttamatta yleisen palomuurin asetuksia.

Henkilökohtainen palomuuri

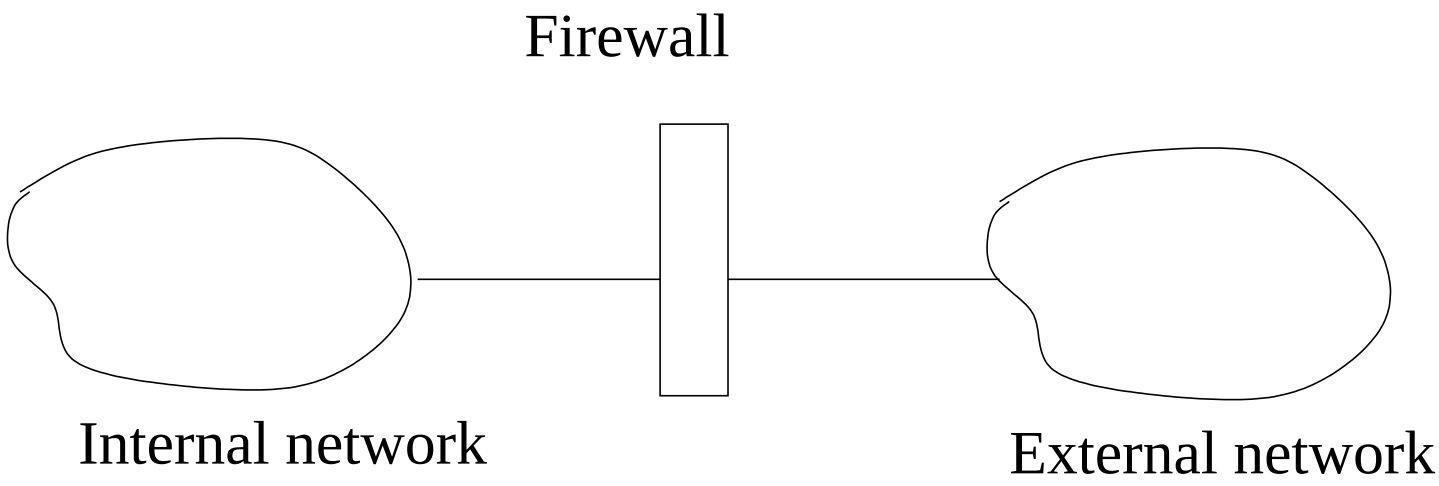
- Palomuuri kontrolloi liikennettä henkilökohtaisen tietokoneen tai internetin välillä. Se on yleensä ohjelmistopohjainen. Palomuuri voi sijaita myös reitittimessä, joka palvelee useampia kotikoneita.
- Henkilökohtaiset palomuurit ovat yleensä paljon yksinkertaisempia kuin palvelinkoneiden tai erilliset palomuurit. Henkilökohtaisen palomuurin tärkein tehtävä on estää ulkopuolisten luvaton käyttö. Se voi myös seurata ulosmenevää liikennettä havaitakseen matoja tai viruksia.

Tyypillisiä palomuuriratkaisuja I

Seuraavassa luetellaan ja kuvataan piirroksin tyypillisiä palomuuriratkaisuja.

- Henkilökohtainen ja palvelinkohtainen palomuuri. Näitä palomuureja voidaan käyttää yksinään tai osana muita palomuuriratkaisuja.
- Reititinpalomuuri. Sisä- ja ulkoverkon rajalla oleva reititin, jossa on pakettisuodatus. Tyypillinen ratkaisu kotona ja pienissä toimistoissa.
- Yksinkertainen palomuuri on seuraavassa kuvassa:

Tyypillisiä palomuuriratkaisuja II

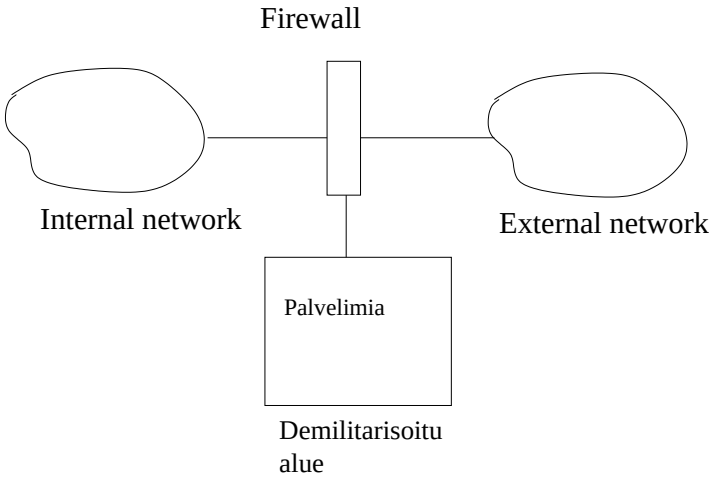


Kuva: Yksinkertainen palomuuri

Palomuuri voi olla tilat muistava tai sovellusyhdyskäytävä. Tyypillinen ratkaisu pienissä tai keskisuurissa organisaatioissa.

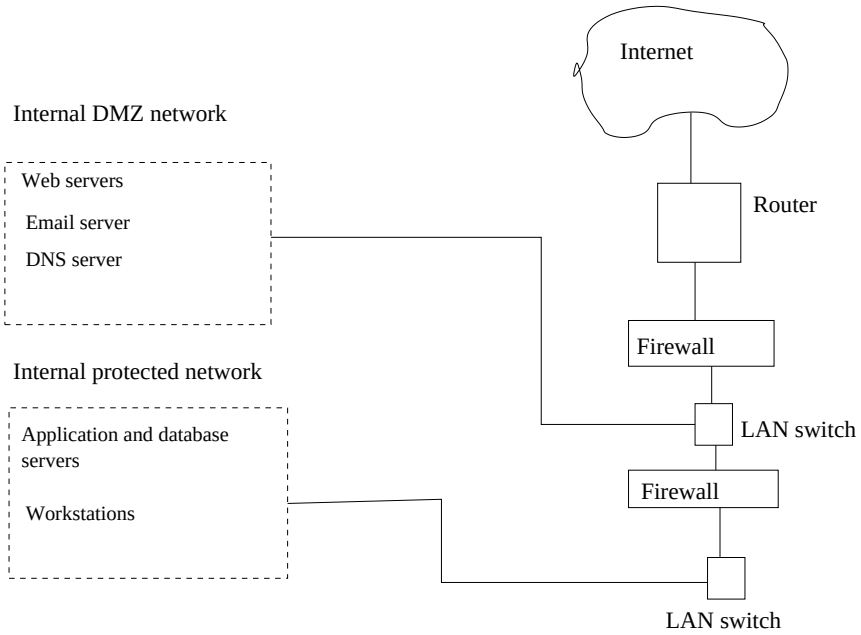
- Yksinkertainen T-palomuuri muistuttaa edellistä, mutta palomuurissa yhteydet kolmeen verkkoon. Kuva valaisee tilannetta.

Tyypillisiä palomuuriratkaisuja III



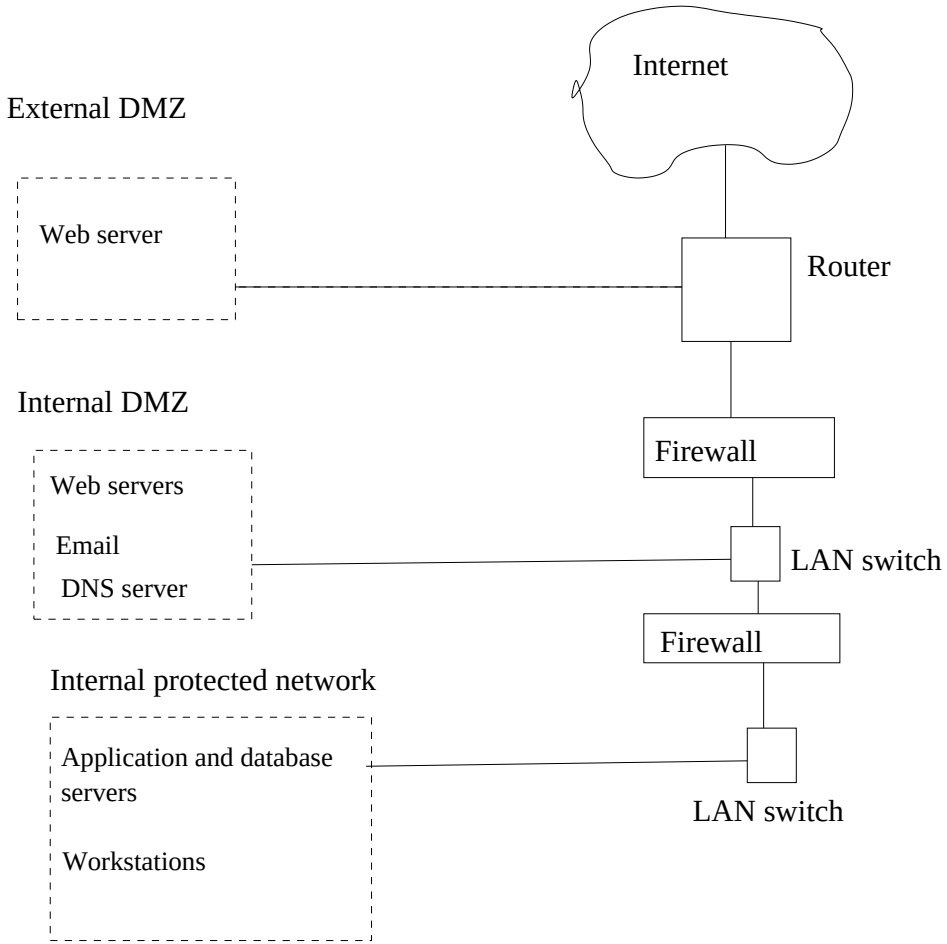
Kuva: Yksinkertainen T-palomuuri

- Kaksinkertainen palomuuri. Seuraava kuva valaisee tilannetta, joka on tyypillinen suurissa organisaatioissa.



Kuva: Kaksinkertainen palomuuri

- Kaksinkertainen T-palomuuri. Tämä eroaa edellisestä siten, että demilitarisoitu alue on yhdistetty palomuuriin erillisellä yhteydellä. Ratkaisu on tyypillinen suurille kaupallisille ja hallinnollisille organisaatioille.
- Hajautettu palomuuri. Myös suurten organisaatioiden ratkaisu. Kuva valaisee tilannetta. Kaikissa palvelimissa ja työasemissa voi olla lisäksi konekohtainen palomuuri.



Kuva: Hajautettu palomuuri

SSL I

SSL (Secure Socket Layer) on standardi, joka on suunniteltu web-selainten ja -palvelimien turvamekanismiksi. SSL käyttää termejä istunto ja yhteys. Istunto on perustettu osapuolten (asiakas-palvelin) välille ja yhteys on kokoelma mekanismeja, joille tietoa siirretään istunnossa. Yhdellä istunnolla voi olla monta yhteyttä. Kahdella osapuolella voi olla myös monia istuntoja yhtäaikaa keskenään, mutta se ei ole tavallista. Jokaiseen istuntoon liittyy tietoa, jonka avulla istunto identifioidaan ja hallitaan:

- istunnon tunnus,
- osapuolen X.509-varmenne,
- tiivistysmenetelm,
- salausmenetelmä,
- pääsalaisuus (48 bittiä, symmetrinen).

Myös jokaiseen yhteyteen liittyy tietoa, jonka avulla yhteyttä hallitaan:

SSL II

- satunnaista dataa palvelimelle ja asiakkaalle (tarvitaan esimerkiksi lohkon täytteissä),
- salausavaimet,
- MAC-avain,
- alustusvektorit,
- järjestysnumerot.

Alempi kerros I

Alempi kerros eli SSL Record Protocol huolehtii yhteydestä. Sovellus on tämän kerroksen päällä. Esimerkiksi SSL:n alempi kerros ottaa vastaan sanomia HTTP:ltä ja käsitelee ne ennen kuin luovuttaa ne kuljetuskerrokselle. Erityisesti kerros huolehtii salauksesta ja eheydestä. Se tekee seuraavat toimenpiteet:

- Jokainen ylemmältä tuleva sanoma pilkotaan lohkoiksi. Sen jälkeen jokaiseen lohkoon sovelletaan seuraavaa.
- Lohko tiivistetään.
- Lohkon MAC lasketaan.
- Tiivistetty lohko MAC-arvon kanssa salataan.
- Lopuksi viimeistellään SSL-tietueen otsake, joka sisältää mm. viestin tyypin, versionumerot ja lohkon pituuden.

Tiivistearvo

Tiivistearvo lasketaan kaavalla

$$\begin{aligned} hash(MAC_{write-secret} \quad &|| \quad pad_2 || hash(MAC_{write-secret} || pad_1 \\ &|| \quad seq - num || SSLCompressed.type \\ &|| \quad SSLCompressed.length \\ &|| \quad SSLCompressed.fragment)) \end{aligned}$$

missä

- MAC-write-secret on jaettu salainen avain,
- pad_1 on täyte 00110110 toistettuna 48 kertaa (MD5) tai 40 kertaa (SHA-1),
- pad_2 on samanlainen täyte bittijonon 01011100 avulla;
- muut symbolit tarkoittavat järjestysnumeroa, käytettävää tiivistealgoritmia, tiivisteen pituutta ja palan tunnusta.

Sekä tiivistetty sanoma että MAC-arvo salataan symmetrisellä salauksella.

Ylempi kerros I

Ylempi kerros koostuu kolmesta protokollasta: SSL Handshake Protocol, SSL Change Cipher Spec Protocol ja SSL Alert Protocol.

Näistä Change Cipher -protokolla on yksinkertaisin. Se lähettää vain yhden tavun, jonka arvo on 1. Protokollan tarkoituksena on informoida vastapuolta ottamaan käyttöön uudet salausmenetelmät, jotka on jo neuvoteltu valmiiksi.

Alert-protokollaa käytetään välittämään virheilmoituksia yms sellaisia asioita SSL:ää käyttävälle sovellukselle. Esimerkkejä ilmoituksista:

- unexpected message,
- bad record mac,
- decompression failure,
- handshake failure,
- ym.

Kättelyprotokolla I

Kättelyprotokolla on SSL:n ylemmän kerroksen pääprotokolla, jonka avulla istunto perustetaan. Se käsittää 4 kierrosta ja sen jälkeen on todennettu käyttäjät, sovittu avaimista, salausmenetelmästä ja MAC-algoritmista. Kättely muodostuu seuraavista askelista (C client, S server):

1. $C \longrightarrow S$: *version, rand-1, session-id, cipher-list, compression-list*
   Eli asiakas lähettää istuntopyynnön palvelimelle ja ilmoittaa samalla istunnon numeron ja listat niistä salaus- ja tiivistysalgoritmeista, joita asiakas tukee. Lisäksi välittyy versionumero ja satunnaisluku (itse asiassa pari (timestamp (32 bit, random number (28 byte)), jota käytetään uusintahyökkäysten (vanha paketti lähetetään uudestaan) havaitsemiseen.
   Tämä sanoma voidaan lähettää olemassaolevan istunnon aikana. Jos tällöin session-id on 0, lähettäjä haluaa uuden yhteyden uudessa istunnossa. Jos taas session-id on erisuuri kuin nolla, lähettäjä haluaa uudet salausparametrit tai uuden yhteyden tässä istunnossa.

Kättelyprotokolla II

2. $S \longrightarrow C$: *version, ran-2, session-id, cipher, compression*
   Palvelin valitsee salaus- ja tiivistysalgoritmin listoista ja palauttaa tiedon näistä uuden satunnaisluvun kera asiakkaalle.
3. $S \longrightarrow C$: *server-cert*
   Palvelin lähettää myös oman varmenteensa.
4. $S \longrightarrow C$: $\{mod, exp, hash(rand\text{-}1, rand\text{-}2, mod, exp)\}_{K_S}$
   Palvelin lähettää varmenteeseensa liittyvät tunnusluvut eli modulonarvon ja julkisen avaimen sekä allekirjoittaa nuo tiedot salaisella avaimellaan. Allekirjoitus sisältää myös satunnaisluvut.
5. $S \longrightarrow C$: *cert-type, good-cert-authorities*
   Nyt palvelin pyytää asiakkaan varmennetta. Sen tulisi olla ehdotettua tyyppiä ehdotettujen luotettavien viranomaisten varmentama.
6. $S \longrightarrow C$: *end-round-2*
7. $C \longrightarrow S$: *client-cert*
   Asiakas lähettää pyydetyn varmenteen.

Kättelyprotokolla III

8. $C \longrightarrow S$: *premasterkey*
   Ja yhteisen salaisuuden, josta avaimia voidaan johtaa. Tämä sanoma on salattu palvelimen julkisella avaimella.
9. $C \longrightarrow S$: *hash(mastr, opad, hash, hash(messages, mastr, ipad))*
   Molemmat voivat laskea nyt pääavaimen yhteisestä salaisuudesta. Lisäksi lasketaan MAC:ia varten tarvittavat parametrit ipad ja opad. Nämä asiakas välittää myös palvelimelle ja niiden lisäksi myös kaikki aikaisemmat viestit. Tiedot lähetetään kryptografisen tiivistysfunktion kautta.
10. $C \longrightarrow S$: Viimeiset kaksi viestiä ovat eräänlaisia kuittauksia. Ensin asiakas ilmoittaa palvelimelle, että kaikki mikä seuraa seuraa on todennettua ja salattua (jos salauksesta on sovittu). Sen jälkeen lähtee vielä sanoma "finished".
11. $S \longrightarrow C$: Palvelin lähettää samanlaisen viestin asiakkaalle, sen jälkeen myös finished-sanoman ja kaiken tämän jälkeen varsinainen tietoliikenne voi alkaa.

Pääavain I

Pääavain lasketaan kaavalla

$$
\begin{aligned}
\text{master} - \text{secret} \quad = \quad & MD5(pre - master - secret \\
& || \quad SHA('A'||premastersecret \\
& || \quad ClientHello.random||ServerHello.random)) \\
& || \quad MD5(premastersecret \\
& || \quad SHA('BB'||premastersecret||ClientHello.random \\
& || \quad ServerHello.random)) \\
& || \quad MD5(premastersecret \\
& || \quad SHA('CCC'||premastersecret||ClientHello.random \\
& || \quad ServerHello.random))
\end{aligned}
$$

Pääavaimesta generoidaan

Pääavain II

- client write MAC secret,
- server write MAC secret,
- client write key,
- server write key,
- client write IV (initialization vector),
- server write IV.

Generointi tapahtuu tiivistefunktioiden avulla (hash).

Edellä on kuvattu vain tilanne, jossa kumpikin todentaa toisensa. SSL sallii myös muunlaisia tilanteita. Lisäksi SSL:ssä on mahdollisuus uudelleen neuvotella istunto. Näihin tilanteisiin löäydettiin kuitenkin hyökkäysmahdollisuuksia 2009. (Marsh Ray: Renegotiating TLS, November 4, 2009.)

IPSec I

- IPSec on IP-verkkoprotokollien laajennus, millä estetään IP-pakettien urkkiminen ja muuntaminen. IPSec on syntynyt uuden IPv6-protokollan yhteydessä ja IPv6 onkin IPSec:in luonteva alusta. IPSec voidaan kuitenkin sovittaa myös IPv4-protokolliin.
- Verkkotason suojaus ei vaikuta sovellusohjelmiin tai sovellusprotokolliin ja IPSec-paketteja voivat käsitellä jo käytössä olevat reitittimet ja reitittävät isäntäkoneet. IPSec:iä käytetään nykyisin erityisesti virtuaalisten yksityisten verkkojen toteutukseen.
- Yritys voi rakentaa turvallisen virtuaalisen yksityisen verkon Internetin tai julkisen WAN-verkon yli. Tämä mahdollistaa sen, että yritykset voivat luottaa Internetiin ja säästää yksityisen verkon perustamis- ja käyttökustannukset.
- Loppukäyttäjä, jolla on IPSec implementoituna, voi ottaa paikallisen yhteyden Internetin palveluntarjoajaan, jota kautta hän voi edelleen saada turvallisen yhteyden yrityksensä suljettuun verkkoon.

IPSec II

- IPSec:iä voidaan käyttää varmistamaan kommunikointi toisten organisaatioiden kanssa niin, että todennus ja luottamuksellisuus taataan.

IPSec-arkkitehtuurin yleiskuva I

- IPSec on varsin monimutkainen ja terminologiakin on erikoista. Protokolla on suunniteltu toteuttamaan luottamuksellisuus (salauksen avulla) ja todennus.
- Kummallekin suojaustavalle on määritelty oma otsikkonsa, koteloitu salattu data ja todennusotsikko. Yksi ja sama IP-paketti voi sisältää yhden tai molemmat otsikot riippuen tarvittavasta turvapalvelusta.
- Todennusotsikko (AH, Authentication Header) sisältää eheyden tarkistustietoa, millä voidaan tarkistaa, onko paketti väärennös tai onko sitä muutettu matkalla epäluotettavan verkon läpi.
- Otsikko sisältää tätä varten tarkistussumman. Tarkistussumma sisältää salaista tietoa, josta syystä ulkopuolinen ei pysty laskemaan toista tarkistussummaa, mikä osoittaisi sisällön aitouden.
- Koteloitu salattu data -otsikkoa (ESP, Encapsulating Security Payload) käyttämällä salataan paketin loppuosan datasisältö.

IPSec-arkkitehtuurin yleiskuva II

- ESP-otsikon muoto vaihtelee sen mukaan, mitä salausalgoritmia käytetään. Kaikissa tapauksissa käytettävä salausavain valitaan parametrin SPI (security parameter index) avulla.
- IPSec-protokolla koostuu siten kahdesta versiosta, joista ensimmäinen kattaa pelkästään todennuksen todennusotsikon avulla. Toinen versio on yhdistetty todennus- ja salausprotokolla, jonka yhteydessä käytetään otsikkoa koteloitu salattu data yksinään tai todennusotsikon kanssa, jos halutaan salauksen lisäksi todennus.
- IPSec tarjoaa kuitenkin enemmän kuin pelkästään yksinkertaisen todennuksen ja salauksen. Seuraavassa on lueteltu IPSec:in tarjoamat palvelut:
  - Pääsynvalvonta.
  - Yhteydetön eheys.
  - Datan alkuperään liittyvä todennus.
  - Toistohyökkäysten torjunta.
  - Luottamuksellisuus.

IPSec-arkkitehtuurin yleiskuva III

- Rajoitettu liikennevirran luottamuksellisuus.

Turvayhteydet I

- Turvayhteydet (security associations) on avainsana toteutettaessa todennusta ja luottamuksellisuutta. Kummankin IPSec-suojaukseen pyrkivän koneen tulee muodostaa aluksi turvayhteys toinen toiseensa.
- Turvayhteys määrittelee, mitä ja miten IPSec-suojausta käytetään, eli mitä turvapalvelua milloinkin käytetään, miten salaus ja/tai todennus suoritetaan ja mitä avaimia pitää käyttää. Eli turvayhteys sisältää kaiken sen informaation, mitä tarvitaan luotettavan yhteyden määrittelemisessä ja toteutuksessa.
- IETF:n dokumentit käsittelevät turvayhteyttä ja sen sälytyspaikkaa, *SAD*:ia (security association database), hypoteettisinä käsitteinä, koska ne ovat osapuolten sisäisiä asioita.

Turvayhteydet II

- Ne sisältävät kommunikoinnin kannalta oleellisia tietoja, mutta itse SA kokonaisuudessaan ei ole osa kommunikointia. Sen tähden dokumentit eivät ota kantaa sen muotoon tai sijaintiin. Käytännössä SAD on taulukko, jota säilytetään suojatussa muistissa, ja SA on tietue taulukossa.
- Jokainen turvayhteys sisältää tietoa, jonka avulla IPSec-prosessi voi päättää, sovelletaanko SA:n määrittelemää suojaa tiettyyn lähtevään tai tulevaan pakettiin. Ratkaisu tehdään SA:n *valitsimien* (selectors) perusteella. Valitsimet sisältävät seuraavaa:
  - Lähde- ja kohdeosoite. Toistaiseksi sallitaan vain yksittäiset osoitteet, ei yleislähetyksiä. Kohdeosoite voi olla joko loppukäyttäjä tai palomuuri tai reititin.
  - Nimi on joko käyttäjätunnus tai systeemin nimi.
    - Käyttäjätunnus rajaa SA:n vain erityisen käyttäjän aloittamaan tai vastaanottamaan kommunikointiin.

Turvayhteydet III

- Jos ainoat valitsimet ovat kommunikoivien osapuolten käyttäjätunnuksia, SA:ta kutsutaan käyttäjäsuuntautuneeksi (user-oriented).
- Jos taas käytetään systeeminimiä, se rajaa liikenteen tiettyjen systeemien välille. Systeemi voi olla isäntäkone, turvayhdyskäytävä tms.

- Kuljetuskerroksen protokolla (TCP tai UDP).
- Lähde- ja kohdeportti. Yleensä käytetään yhtä ainoaa porttinumeroa, jolla rajataan SA:n käyttö tiettyyn sovellukseen (esim. FTP).

- Jokainen SA sisältää myös seuraavia tietoja:
  - *Järjestysnumerolaskuri* on 32 bitin arvo, jota käytetään AH- ja ESP-otsakkeissa järjestysnumeroiden generoimiseen.
  - *Järjestysnumeron ylivuoto* on lippu, joka osoittaa, kirjataanko järjestysnumeron ylivuodosta lokitapahtuma vai ei. Jos kirjataan, niin seuraavien pakettien lähetys tässä turvayhteydessä on estetty.
  - *Uudelleenlähetysikkunaa* (anti-replay window) käytetään ratkaisemaan, onko saapunut AH- tai ESP-paketti uudelleenlähetys vai ei.

Turvayhteydet IV

- *AH-informaatio* sisältää todennusalgoritmin, avaimet, avainten eliajan ja parametrit, joita tarvitaan AH-paketin ja todennuksen yhteydessä.
- *ESP-informaatio* sisältää salaus- ja todennusalgoritmit, avaimet, alustusarvot, avainten elinajat ja muut parametrit, joita tarvitaan ESP:n kanssa.
- *Turvayhteyden elinaika* on aikaväli tai tavumäärä, jonka jälkeen turvayhteys täytyy korvata uudella tai päättää. Elinaikaan liittyy vielä tieto, kumpi noista kahdesta on käytössä.
- *IPSecin protokollamoodi* tarkoittaa *tunneli-, kuljetusmoodia* tai *villiä korttia*, joiden merkitystä selvitetään myöhemmin.
- *Polun MTU* (maximum transmission unit) tarkoittaa maksimaalista pakettikokoa, joka voidaan välittää pilkkomatta. Lisäksi paketteihin liittyvät aikamääreet kuuluvat MTU-parametriin.

SPI I

- On varsin todennäköistä, että kommunikoivat osapuolet sopivat useammasta kuin yhdestä SA:sta. Esimerkiksi sähköposti ja Web-sovellus vaativat vähemmän kuin maksuja siirtävä protokolla.
- Kun suojattua pakettia ollaan lähettämässä, lähettäjän täytyy tiedottaa vastaanottajalle, mitä SA:ta on käytetty paketin kohdalla, jotta vastaanottaja tietäisi valita saman SA:n. Tätä palvelee turvaparametri-indeksi (SPI).
- Koska jokainen SA on *yksisuuntainen*, turvallinen kaksisuuntainen yhteys vaatii kahden SA:n määrittelemistä: sisään tulevan ja ulos menevän.
- SPI yhdessä kohdeosoitteen ja turvaprotokollan (AH, ESP) kanssa on riittävä, jotta sisään tulevan paketin SA osataan hakea SAD:sta. Jotta taataan SPI:n yksikäsitteisyys, kumpikin osapuoli valitsee oman sisääntulevan SPI:n.

Turvapolitiikan tietokanta I

- Kaikki liikenne IPSec-verkoissa jaetaan turvayhteyksiin ja muuhun liikenteeseen. Turvayhteyksiä voidaan yhdistellä monella tavalla halutun tuloksen aikaansaamiseksi. Turvayhteyksiin liittyvää liikennettä säädellään turvapolitiikan tietokannan (SPD) avulla.
- Yksinkertaisimmillaan SPD sisältää tietueita, joista kukin liittyy tiettyyn osaan IP-liikennettä ja tiettyyn turvayhteyteen.
- Monimutkaisemmissa tilanteissa moni tietue voi liittyä samaan turvayhteyteen tai moni turvayhteys voi liittyä yhteen SPD-tietueeseen. Tällä kurssilla ei kaikkia mahdollisuuksia käsitellä yksityiskohtaisesti.
- Jokainen SPD-tietue määritellään IP- ja ylemmän kerroksen kenttäarvojen avulla, joita kutsutaan valitsimiksi (selectors). Näitä valitsimia käytetään suodattamaan ulosmenevä liikenne siten, että se kyetään yhdistämään tiettyyn turvayhteyteen.

Turvapolitiikan tietokanta II

- Ulosmenevän liikenteen käsittely noudattaa seuraavia periaatteita:
  1. Etsi paketin sopivien kenttien perusteella liikennettä vastaava SPD-tietue, joka puolestaan viittaa nollaan tai useampaan turvayhteyteen.
  2. Poimi SPD-tietueen ja paketin SPI:n perusteella pakettiin liittyvä turvayhteys.
  3. Prosessoi paketti turvayhteyden mukaisesti.
- SPD-tietueen määrittelemiseksi käytetään seuraavia valitsimia:
  - *Kohteen IP-osoite* voi olla joko yksittäinen osoite, osoitelista, osoiteväli tai villi kortti -osoite. Jos osoite käsittää useita yksittäisiä osoitteita, niiden haltijat sijaitsevat saman palomuurin takana ja niihin liittyy sama turvayhteys.
  - *Lähteen IP-osoite* voi myös olla yksittäinen, lista, väli tai villi kortti.
  - *Käyttäjätunnus* on käyttöjärjestelmään liittyvä käyttäjätunnus. Tätä ei käytetä IP- tai ylemmissä otsakkeissa, mutta se on saatavilla, jos IPSec toimii saman käyttöjärjestelmän alaisuudessa kuin käyttäjäkin.

Turvapolitiikan tietokanta III

- *Tiedon luottamuksellisuusaste* on esimerkiksi salainen tai luokittelematon.
- *Kuljetuskerroksen protokolla* saadaan IPv4:n tai IPv6:n kentästä Next Header. Se voi olla yksittäisen protokollan numero, lista protokollanumeroita tai protokollanumeroiden väli.
- *Lähde- ja kohdeportit* voivat jälleen olla yksittäisiä tai usean portin joukkoja.

Todennusotsake I

- Todennusotsakkeeseen (AH) perustuva protokolla huolehtii siis tiedon eheydestä ja IP-pakettien todennuksesta. Pakettien todennus varmistaa käyttäjän tai palvelun identiteetin, joiden pohjalta suodatus tapahtuu. AH suojaa myös uudelleenlähetyksiä vastaan.
- Todennus perustuu MAC-koodiin, joka edellyttää samaa salaista avainta lähettäjällä ja vastaanottajalla. Todennusotsake koostuu seuraavista kentistä:
  - Seuraavan paketin otsakkeen tyyppi (8 b).
  - Hyötykuorman pituus (8 b).
  - Varattu osa (16 b).
  - SPI (32 b).
  - Järjestysnumero (32 b).
  - Todennustieto (muuttuva). Tämä kenttä sisältää eheyden tarkistusarvon (ICV, integrity check value) tai MAC-arvon.

Todennusotsake II

- Uudelleenlähetysten torjuntaan käytetään AH:n järjestysnumerokenttää. Kun uutta turvayhteyttä perustetaan, lähettäjä alustaa järjestysnumerolaskurin nollaksi.
- Joka kerran kun paketti lähetetään käyttäen perustettua turvayhteyttä, lähettäjä kasvattaa laskuria ja asettaa sen arvon järjestysnumerokenttään.
- Siten ensimmäinen arvo on 1. Laskurin suurin arvo on $2^{32} - 1$. Laskuria ei saa päästää tämän jälkeen takaisin nollaan, vaan jos lisäpaketteja on tulossa, on perustettava uusi turvayhteys uudella avaimella.
- Koska IP on yhteydetön, epäluotettava palvelu, protokolla ei takaa, että paketit luovutetaan perille järjestyksessä tai että edes kaikki paketit menevät perille. Siksi IPSec vaatii, että vastaanottajan on toteutettava ikkuna, jonka oletusarvoinen koko on $W = 64$. Ikkunan oikea reuna sisältää suurimman tähän asti vastaanotetun järjestysnumeron, N.

Todennusotsake III

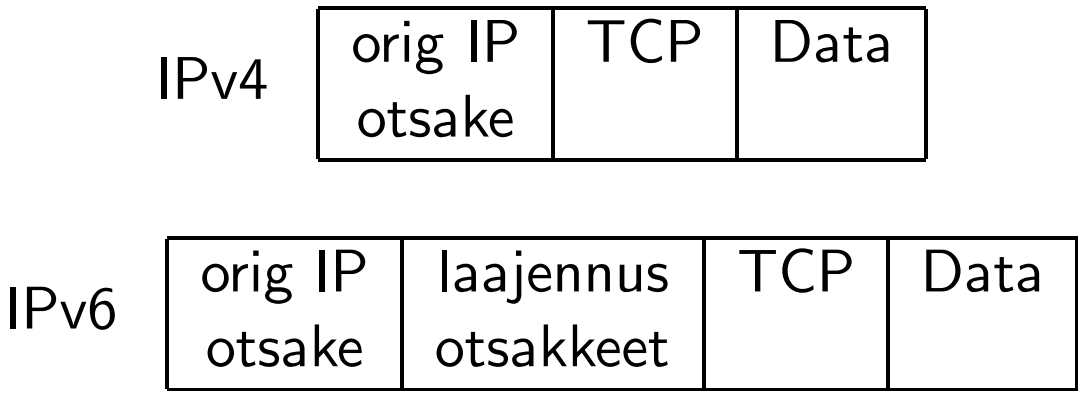
- Jos saapuvan paketin järjestysnumero on välillä $[N - W + 1, N]$, vastaava paikka ikkunassa merkitään. Tarkemmin kuvattuna vastaanottopäässä tehdään seuraavaa:
  1. Jos saapuneen paketin järjestysnumero sisältyy ikkunan lukuihin ja on uusi, MAC tarkistetaan. Jos todennus onnistuu, järjestysnumeroa vastaava paikka ikkunassa merkitään.
  2. Jos saapuneen paketin järjestysnumero menee oikealta ikkunan ulkopuolelle ja on uusi, MAC tarkistetaan. Jos todennus onnistuu, ikkunaa siirretään oikealle niin, että vastaanotetusta järjestysnumerosta tulee ikkunan uusi oikea reuna.
  3. Jos saapuneen paketin järjestysnumero menee vasemmalta ikkunan ulkopuolelle tai jos todennus epäonnistuu, paketti hylätään. Hylkäys kirjataan lokiin.

Todennusotsake IV

- Eheyden tarkistusarvo on tiivistefunktion tai MACin arvo. IPSec:in tulee tarjota ainakin kaksi tiivistefunktiota, HMAC-MD5-95 ja HMAC-SHA-1-96. Molemmat käyttävät HMAC-algoritmia, edellinen MD5-tiivistefunktion, jälkimmäinen SHA-1 -tiivistefunktion kanssa. Kummassakin lasketaan ensin kryptografinen tiivistekoodi, mutta siitä otetaan mukaan vain ensimmäiset 96 bittiä.
- Tiivistearvo lasketaan seuraavista kentistä:
  - IP:n tunnusosan kentät, jotka eivät muutu liikenteessä tai joiden arvo vastaanotettaessa on ennustettavissa. Kentät, jotka muuttuvat matkalla eivätkä ole ennustettavissa, asetetaan nollaksi tiivistettä laskettaessa.
  - AH-otsake paitsi todennustietokenttää, joka asetetaan nollaksi.
  - Kaikki ylemmän tason tieto, joka oletetaan muuttumattomaksi liikenteessä.

AH:n kuljetus- ja tunnelimoodi I

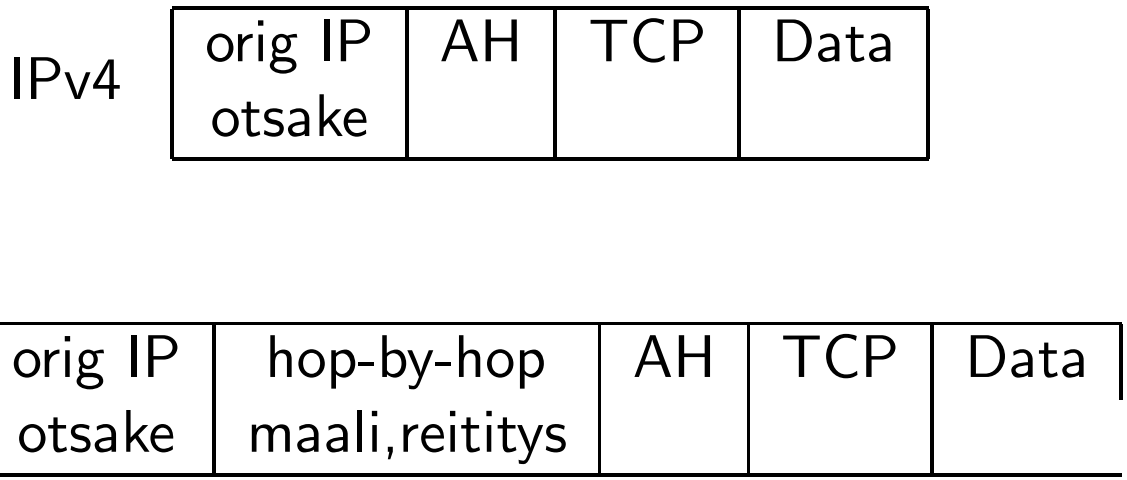
IPSec:in todennuspalvelua voidaan käyttää kahdella tavalla. Näitä tapoja kutsutaan kuljetusmoodiksi ja tunnelimoodiksi. Kuvassa 5 nähdään pakettien tilanne ennen AH:n soveltamista.



Kuva: Ennen AH:n soveltamista

AH:n kuljetus- ja tunnelimoodi II

Kuvassa 6 puolestaan on pakettien tilanne kuljetusmoodissa AH:n soveltamisen jälkeen.

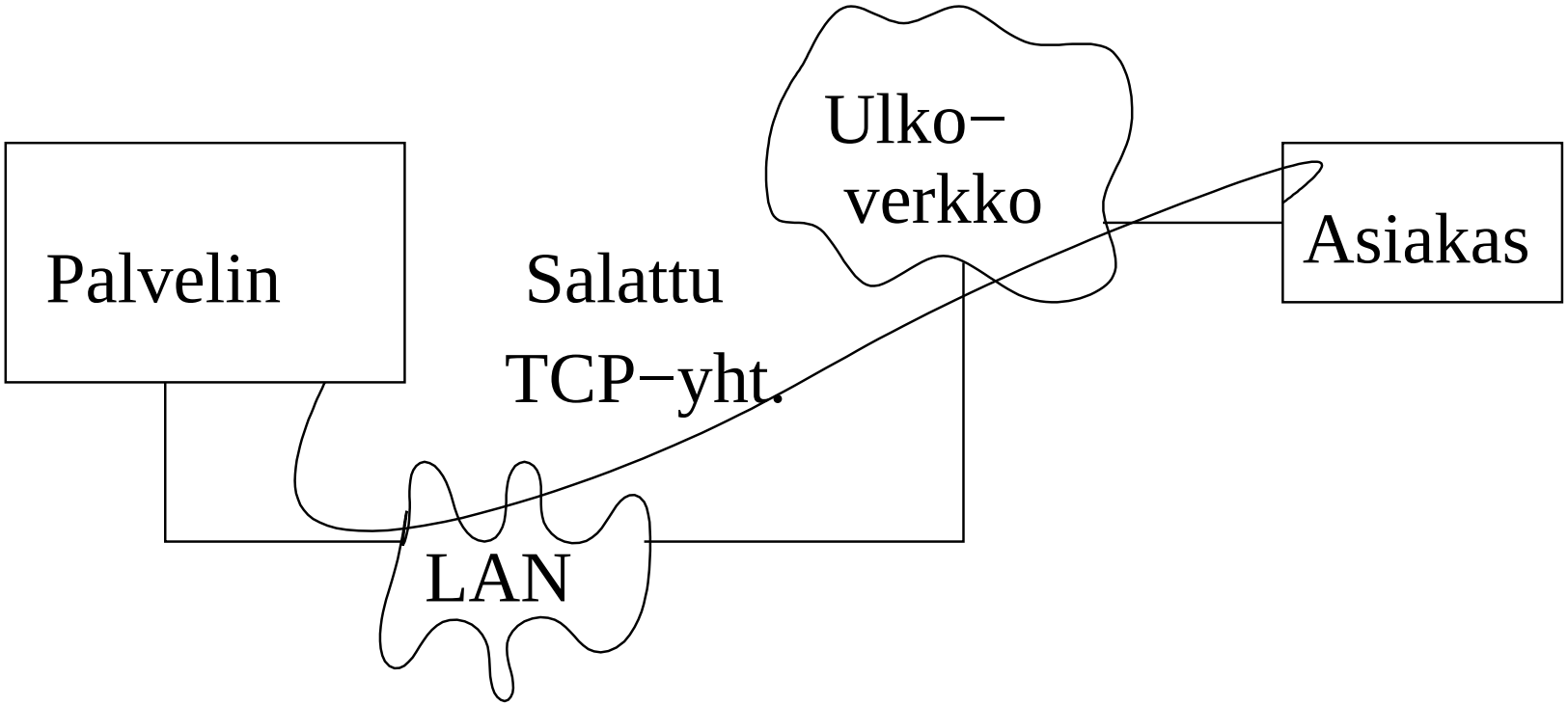


Kuva: AH:n kuljetusmoodi

AH todentaa koko kentän mahdollisia muuttuvia kenttiä lukuunottamatta. Huomattakoon, että tilanne on erilainen IPv4:n ja IPv6:n välillä.

AH:n kuljetus- ja tunnelimoodi III

Kuljetusmoodia käytetään esimerkiksi kuvan 7 tilanteessa, jossa asiakas ja palvelin kommunikoivat suoraan ja niillä on yhteinen salainen avain. Asiakas voi olla joko samassa verkossa palvelimen kanssa tai eri verkossa.



Kuva: AH:n kuljetusmoodin soveltaminen

AH:n kuljetus- ja tunnelimoodi IV

Tunnelimoodissa AH lisätään puolestaan pakettiin kuvan 29 mukaisesti. Edelleeen todennus koskee koko pakettia muuttuvia kenttiä lukuunottamatta.

IPv4

uusi IP otsake	AH	orig IP otsake	TCP	Data

IPv6

uusi IP otsake	laajennus otsakkeet	AH	orig IP otsake	laajennus otsakkeet	TCP	Data

Kuva: AH:n tunnelimoodi

AH:n kuljetus- ja tunnelimoodi V

Siis tunnelimoodissa koko alkuperäinen paketti todennetaan ja AH lisätään alkuperäisen IP-otsakkeen ja uuden, ulomman IP-otsakkeen väliin. Sisempi IP-otsake sisältää varsinaisen lähde- ja kohdeosoitteen, kun taas ulompi IP-otsake voi sisältää muita, esimerkiksi reitittimien, osoitteita.

Tunnelimoodia käytetään tyypillisesti tilanteessa, jossa ulkoinen työasema todentaa itsensä palomuurille päästäkseen sen jälkeen palomuurin suojaamaan verkkoon. Tunnelimoodia käytetään erityisesti rakennettaessa ns. virtuaalisia yksityisiä verkkoja(VPN).

Koteloitu salattu data I

Koteloitu salattu data eli ESP tarjoaa siis salauksen ja haluttaessa myös todennuksen. ESP-otsake koostuu seuraavista kentistä:

- SPI (sama kuin AH:ssa).
- Järjestysnumero (AH:ssa).
- Hyötykuorma on kuljetuskerroksen segmentti (kuljetusmoodi) tai IP-paketti (tunnelimoodi), joka suojataan salauksella.
- Täyte (0-255 B) selitetään myöhemmin.
- Täytteen pituus (8 b) on täytteen pituus tavuissa.
- Seuraava otsake (8 b) määrittelee sen datan tyypin, joka sijaitsee hyötykuormakentässä. Tyyppi määräytyy ensimmäisen tunnusosan mukaan.
- Todennustieto (AH).

ESP-palvelu salaa kentät

Koteloitu salattu data II

- hyötykuorma,
- täyte,
- täytteen pituus ja
- seuraava otsake.

Jos salausalgoritmi vaatii esimerkiksi alustusvektorin, se välitetään yleensä kentän hyötykuorma alussa salaamattomana.

Täyte palvelee montaa tarkoitusta. Jos salausalgoritmi vaatii, että selväteksti on tavujen monikerta, selvätekstiin voidaan lisätä täyte. Täyte voidaan lisätä myös salatekstin ja kenttien täytteen pituus ja seuraava otsake väliin. Täytettä voidaan käyttää myös salaamaan hyötykuormakentän todellinen pituus.

ESP:n kuljetus- ja tunnelimoodi I

Samoin kuin AH:n kohdalla myös ESP-protokollaa voidaan käyttää kuljetus- ja tunnelimoodissa. Kuvassa 9 nähdään, mitkä kentät salataan ja todennetaan ESP-paketeissa kuljetusmoodissa.

IPv4:

orig IP otsake	ESP otsake	TCP	Data	ESP pääte	ESP tod

IPv6:

orig IP otsake	hop-by-hop, kohde reititys, palat	ESP otsake	kohde	TCP	Data

ESP pääte	ESP tod

Kuva: ESP:n kuljetusmoodi

ESP:n kuljetus- ja tunnelimoodi II

Kuljetusmoodin toiminta etenee seuraavasti:

1. Lähettäjän puolella ensin salataan kentät 3-5 (IPv4) tai 4-7 (IPv6). Selväkieliset vastaavat kentät korvataan salatekstillä. Todennus lisätään, jos sitä halutaan. Todennus kattaa kentät 2-5.
2. Paketti reititetään kohteeseen. Jokainen välillä oleva reitittäjä tutkii IP-otsakkeen ja selväkielisen laajennusotsakkeen, mutta ei salattua osaa.
3. Vastaanottaja tutkii selväkieliset kentät. ESP-osan SPI-tietojen perusteella vastaanottaja purkaa salauksen.

ESP:n kuljetus- ja tunnelimoodi III

Tunnelimoodissa koko IP-paketti plus ESP-perä salataan. Reititystä varten alkuperäisestä IP-paketista kerätään tarvittavat tiedot, joita käytetään ulomman IP-paketin tunnusosassa. Kuvassa 10 näkyy salaukseen ja todennukseen käytetyt kentät.

IPv4:

Uusi IP otsake	ESP otsake	orig otsake	TCP	Data	ESP pääte	ESP tod

IPv6:

Uusi IP otsake	laaj. otsakkeet	ESP otsake	orig IP otsake	laaj. otsakkeet	TCP	Data

ESP pääte	ESP tod

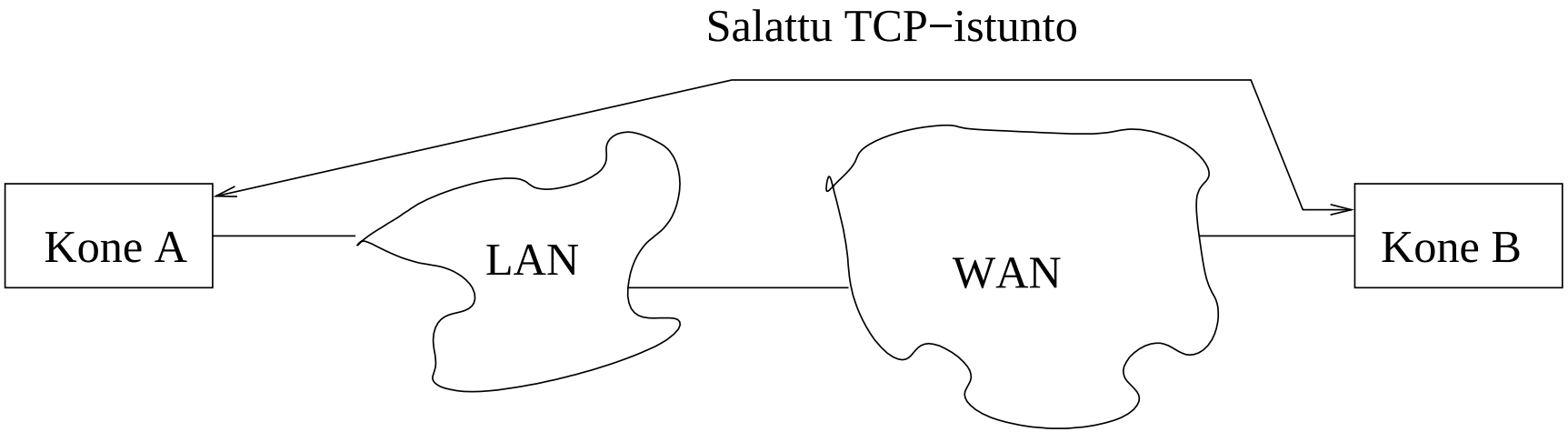
Kuva: ESP:n tunnelimoodi

ESP:n kuljetus- ja tunnelimoodi IV

- Kuljetusmoodi sopii suojaamaan yhteyksiä kahden koneen välillä, joissa kummassakin on ESP.
- Tunnelimoodi on hyödyllinen, kun toisena osapuolena on palomuuri tai muu turvallinen yhdyskäytävä, joka suojaa verkkoa ulkopuolisilta.
- Salaus on käytössä tässä tapauksessa yleensä vain ulkoisen koneen ja yhdyskäytävän välillä. Suojatun verkon sisällä salausta ei tarvita.

AH ja ESP kuvioina I

Seuraavassa esitetään AH:n ja ESP:n toimintaa kuvioiden avulla. Näitä voidaan sitten käyttää hyväksi kuvattaessa havainnollisesti turvayhteyksien yhdistämistä. Kuvassa 11 on tyypillinen tilanne, jossa kahden koneen yhteys on suojattu kuljetusmoodin avulla. Tällä saavutetaan TCP-istunnon salaus.

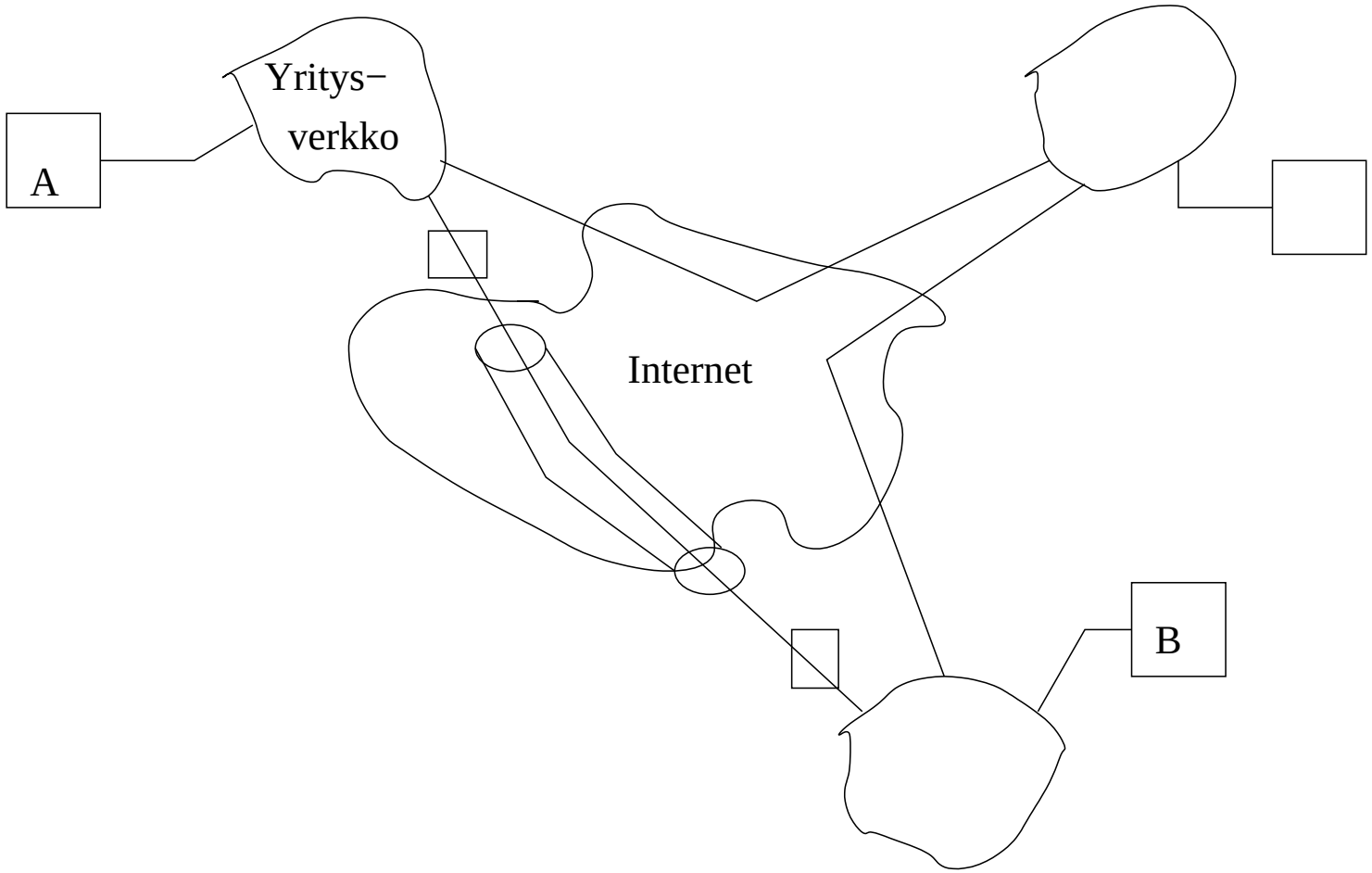


Kuva: Kuljetusmoodi

AH ja ESP kuvioina II

Kuvassa 12 puolestaan on toteutettu virtuaalinen yksityinen verkko IPSecin tunnelimoodin avulla.

AH ja ESP kuvioina III

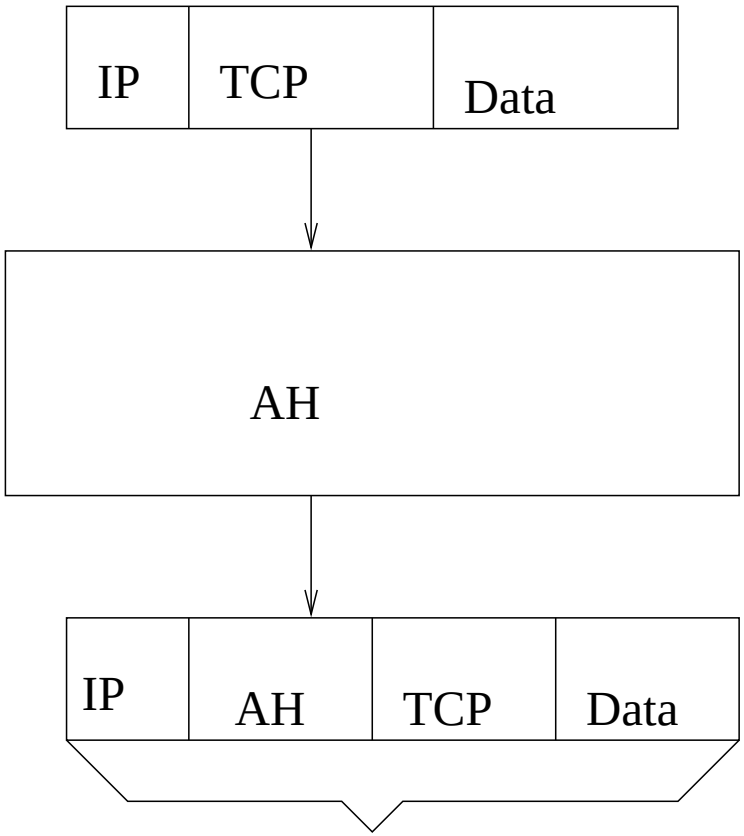


Kuva: Tunnelimoodi

AH ja ESP kuvioina IV

Kuvasarja 13...20 puolestaan esittää pakettien muodostumista eri moodeissa. Aluksi AH ja ESP ovat erillään, mutta viimeisissä kuvissa käsitellään näiden yhdistämistä.

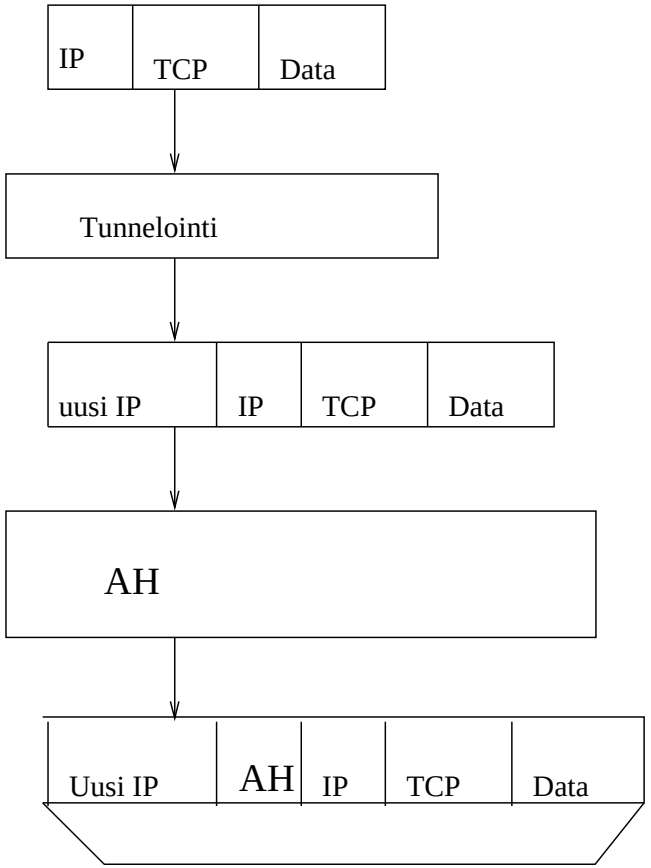
AH ja ESP kuvioina V



Todennus

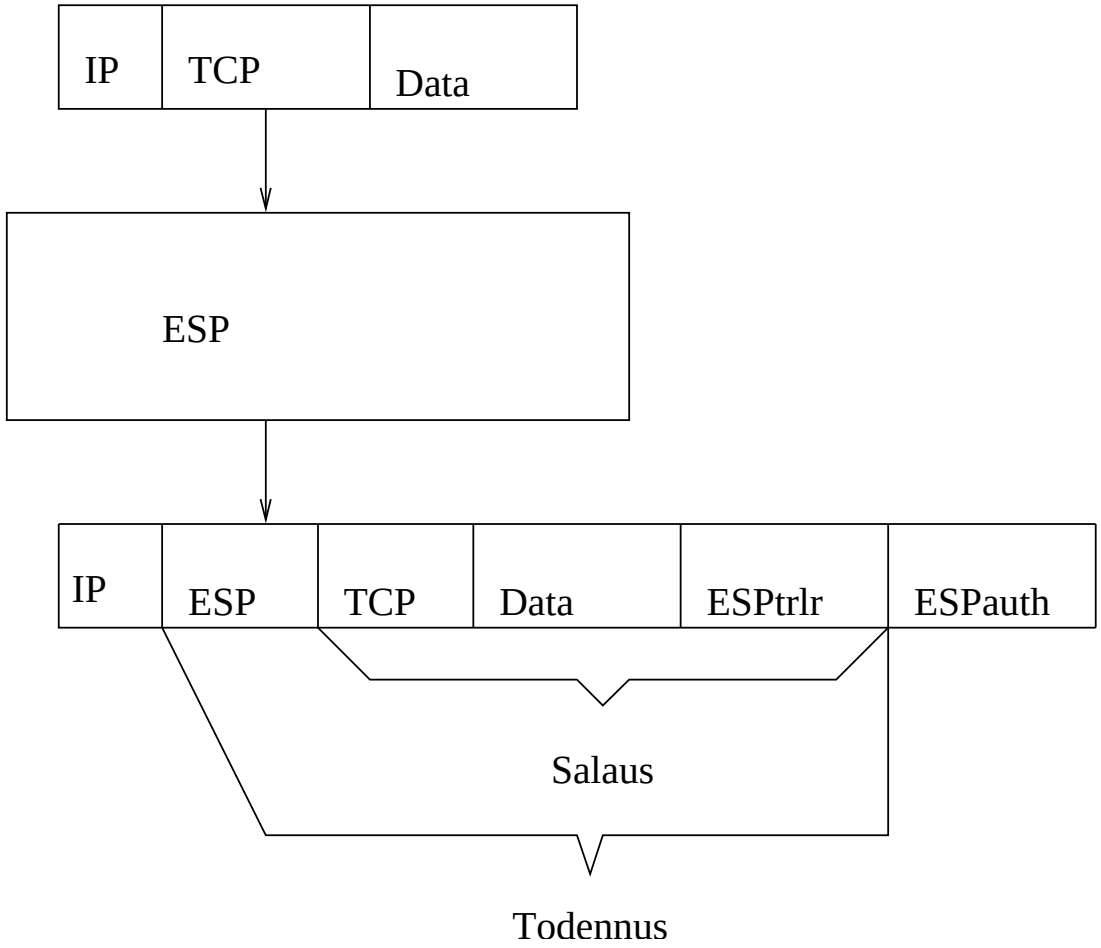
Kuva: AH kuljetusmoodissa

AH ja ESP kuvioina VI



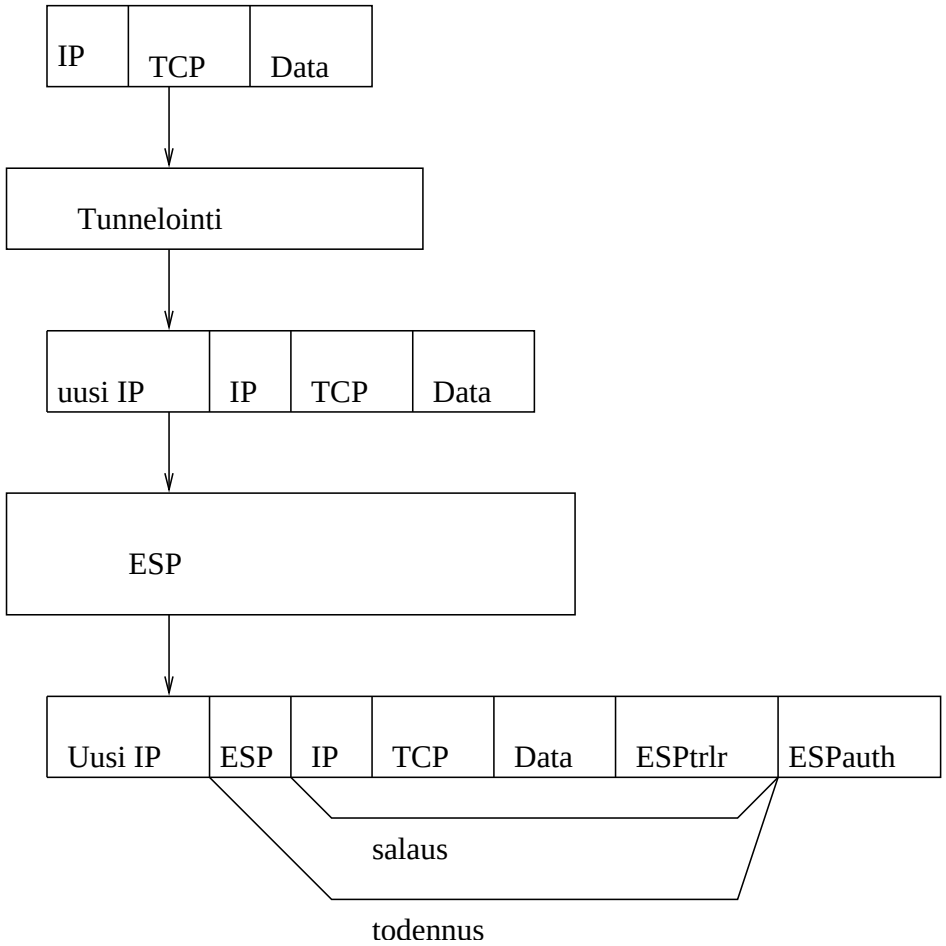
Kuva: AH tunnelimoodissa

AH ja ESP kuvioina VII



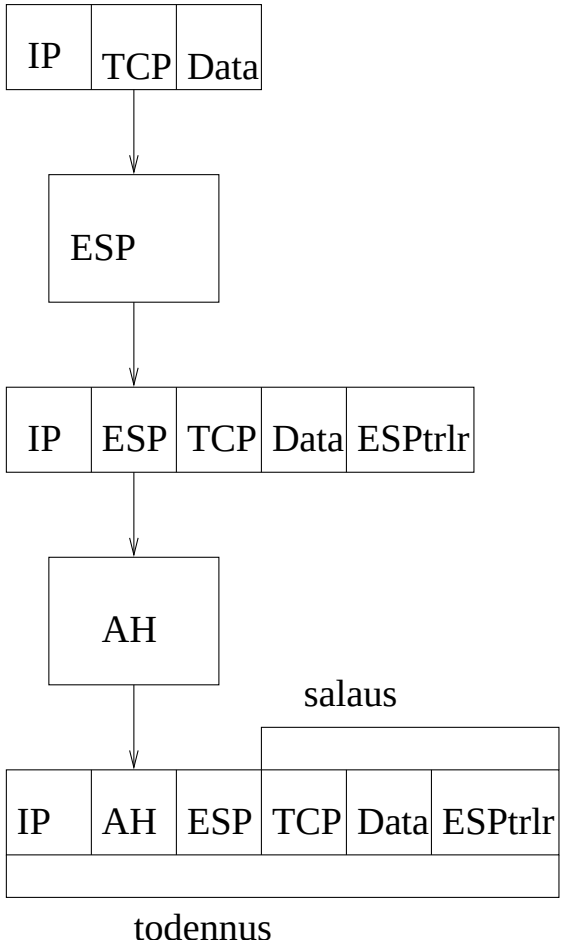
Kuva: ESP kuljetusmoodissa

AH ja ESP kuvioina VIII



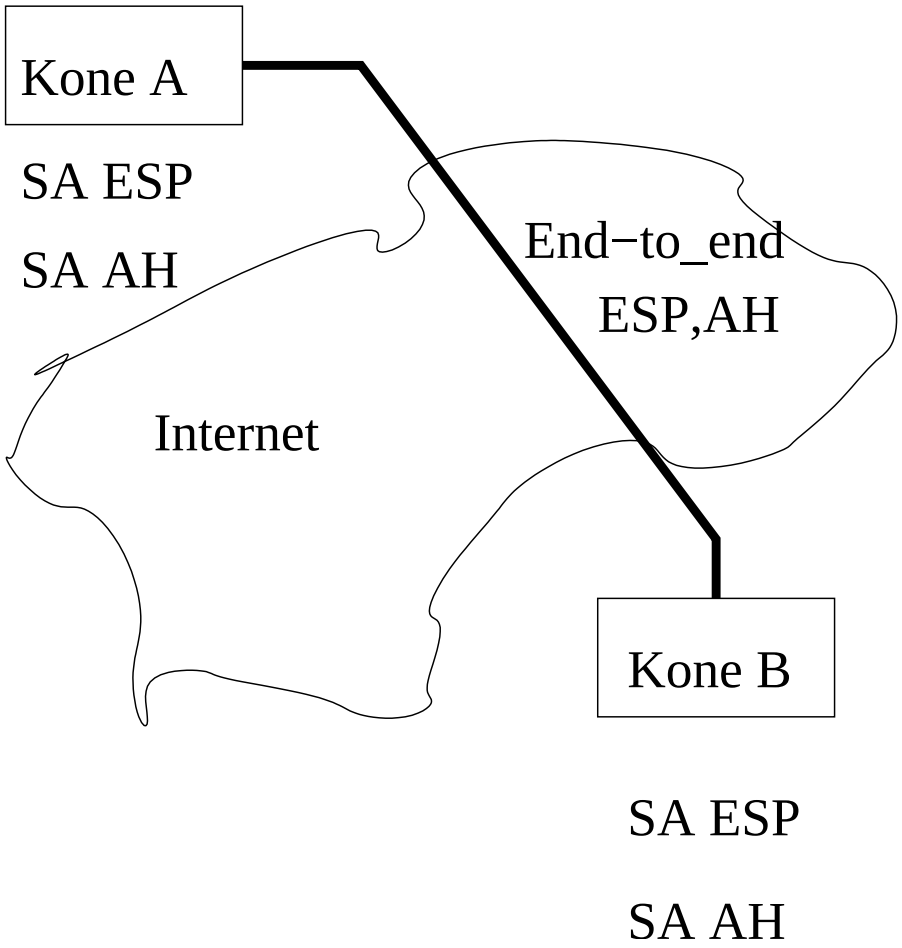
Kuva: ESP tunnelimoodissa

AH ja ESP kuvioina IX



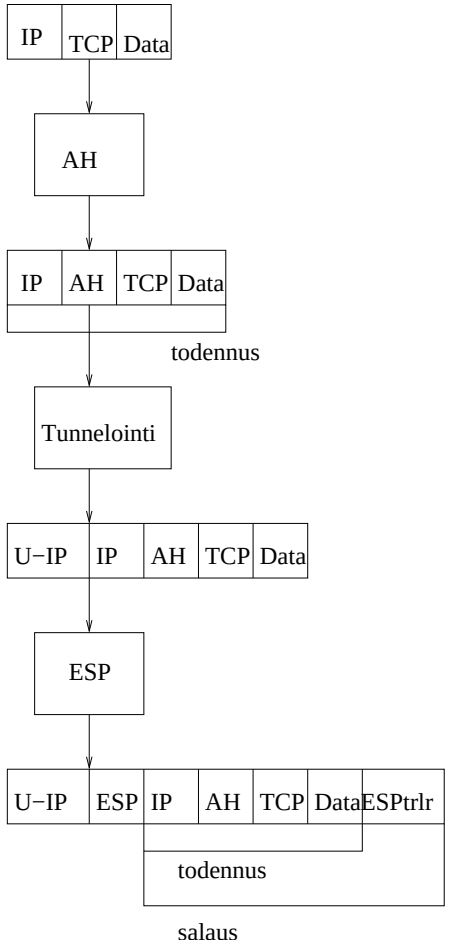
Kuva: ESP ja AH, molemmat kuljetusmoodissa

AH ja ESP kuvioina X



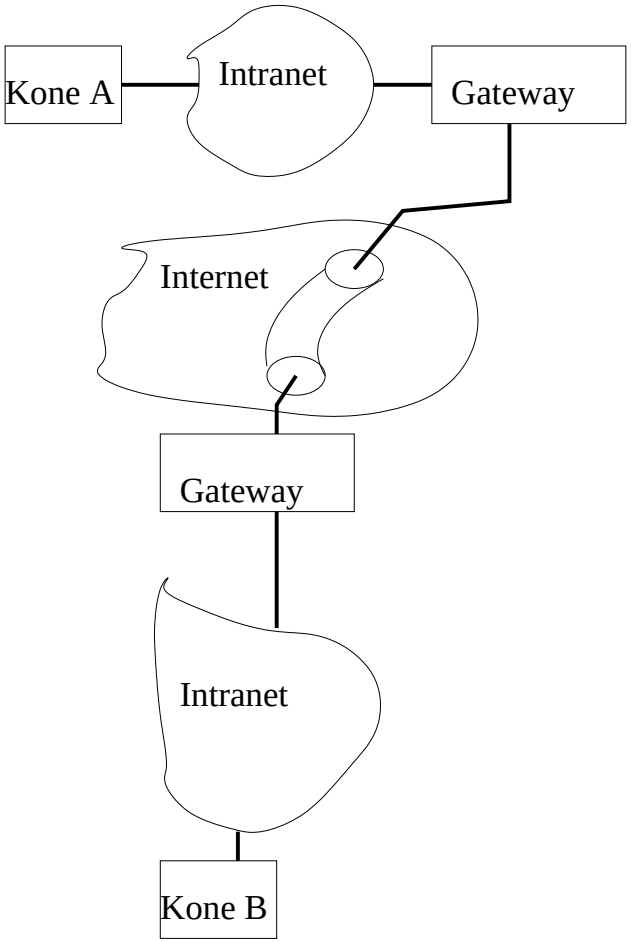
Kuva: ESP ja AH -yhdistelmän sovellustilanne

AH ja ESP kuvioina XI



Kuva: AH kuljetus- ja ESP tunnelimoodissa

AH ja ESP kuvioina XII



Kuva: AH-kuljetus, ESP-tunneli: sovellustilanne

IPSec:in kritiikkiä I

- IPSec on syntynyt komiteatyönä, jossa mukana on ollut useita tahoja. Tämä on johtanut siihen tyypilliseen tilanteeseen, että yhteen ja samaan protokollaan on sovitettu monia piirteitä ja näkökantoja.
- Tällainen suunnittelu on johtanut IPSec:in ja monen muunkin protokollan (erityisesti ISOn OSI-protokollat aikoinaan) yhteydessä laajuuteen ja monimutkaisuuteen, joka ei enää palvele käyttäjiä.
- Näyttääkin siltä, että parempi tulos saavutetaan kilpailujen avulla kuten AES:n yhteydessä. Tällöin yksi ja sama, suppeahko tiimi suunnittelee protokollan, jolloin sen koko pysyy kohtuullisena.

Opetus 1. Kryptografisia protokollia ei pitäisi suunnitella komiteatyönä.

- Seuraavassa käsitellään IPSec:in ongelmia kohta kohdalta Niels Fergusonin ja Bruce Schneierin artikkelin *A Cryptographic Evaluation of IPSec* pohjalta .

IPSec:in kritiikkiä II

- Esityksessä keskitytään vain varsinaiseen toimintaan. IPSec:in avaintenhallinta oli pitkään kehityksen kohteena ja artikkelin kirjoituksen aikana se oli erityisen sekavaa. Siitä syystä emme käsittele artikkelin avaintenhallintaan kohdistuvaa kritiikkiä.
- Artikkelin kaikki suositukset on esitetty myös tässä. Toisaalta ei ole aivan selvää, että kaikki olisivat artikkelin ehdotuksiin tyytyväisiä. Erityisesti käytännön verkkosuunnittelijan näkökulma saattaa olla toinen kuin pelkästään tietoturvaihmisten.

IPSec:in dokumentointi I

- IPSecin dokumentteja on hyvin vaikea ymmärtää. Niissä ei yleensä ole yleiskatsausta tai johdantoa. Siten ei ole uskottavaa, että kukaan oppisi IPSeciä virallisista dokumenteista.
- Tässä yhteydessä erityisesti mainitaan alustava avaintenhallintaprotokolla ISAKMP, jonka dokumentointi sisältää virheitä, josta monet oleelliset selitykset puuttuvat ja joka on sisäisesti ristiriitainen.
- Dokumenteista ei käy selville protokollan tavoite. Tällöin protokollan analysointi on hankalaa. Samoin sunnittelijan, joka yrittää soveltaa IPSec:iä käytäntöön, työ vaikeutuu.
- IPSec tuottaa IP-tason turvallisuutta ja on siten oleellisesti VPN-protokolla. Kuitenkin on ollut tapauksia, jossa protokollaa on käytetty sovellustason turvallisuuden saavuttamiseen kuten esimerkiksi henkilön todentamiseen, kun tämä yrittää lukea sähköpostiaan.

IPSec:in dokumentointi II

- IPSec perustaa pakettien todennuksen siihen, että paketti on lähtenyt joltakulta, joka tuntee salaisen avaimen. Kuitenkin monet näyttävät uskovan, että se todentaa lähettävän IP-osoitteen, jota sitten voidaan käsitellä palomuurissa.
- Dokumentit eivät myöskään sisällä selityksiä tai perusteluja valinnoille, joita on tehty. Vaikka nämä eivät ole niin tärkeitä kuin tavoitteet, ne ovat myös oleellisia.

Opetus 2. Systeemin dokumentin tulisi sisältää johdattelevaa materiaalia, yleiskatsaus niille, jotka tutustuvat asiaan ensimmäistä kertaa, asetetut tavoitteet ja perustelut.

Datan käsittely: Moodit I

Turvaomisuuksien kannalta katsottuna tunnelimoodi sisältää kuljetusmoodin (verkkokerroksesta katsoen tilanne saattaa olla päinvastainen). Kuljetusmoodi kuluttaa tosin vähemmän kaistanleveyttä. Tunnelimoodiakin voitaisiin tehostaa, joten tekijät suosittavat

Suositus 1. Kuljetusmoodi voidaan jättää pois.

Dokumenteissa ei perustella kahden moodin olemassaoloa. Kuljetusmoodin poisjättäminen välttäisi myöskin koneiden jakamisen kahteen luokkaa, isäntäkoneisiin ja turvayhdyskäytäviin. Näiden pääero näyttää olevan, etteivät turvayhdyskäytävät voi käyttää kuljetusmoodia.

Datan käsittely: AH ja ESP I

- Dokumentit eivät selitä, miksi IP-otsakkeet pitää todentaa. Hyötykuorman todennus takaa, että kuorma tulee sellaiselta, joka tuntee salaisen avaimen. IP-otsakkeeet vain auttavat pakettia menemään vastaanottajalle, eikä niiden pitäisi vaikuttaa paketin tulkintaan.
- AH todentaa alempien kerrosten IP-otsakkeita. Tämä selvästi rikkoo protokollapinon modulaarisuutta. Se aiheuttaa monia ongelmia, koska jotkut kentät muuttuvat matkan aikana. Siten AH:n täytyy tuntea kaikki alempien kerrosten dataformaatit, jotta muuttuvat kentät voidaan välttää. Tämä ei tunnu järkevältä.

Suositus 2. Jätetään AH pois.

- ESP sallii hyötykuorman salauksen ilman todennusta. Hyvin harvoin salaus ilman todennusta on hyödyllistä.

Datan käsittely: AH ja ESP II

- IPSecin yhteydessä tällainen tilanne on kuljetusmoodissa, jossa ESPin todennus ei ole kovin kattava ja on käytettävä lisäksi AH:ta. Jos kuljetusmoodi ja AH jätettäisiin pois, voitaisiin suositella:

Suositus 3. Muutetaan ESPiä siten, että se tuottaa aina todennuksen; vain salaus voisi olla valinnainen.

Operaatioiden järjestys I

- Kun käytetään sekä salausta ja todennusta, IPSec salaa ensin ja todentaa sitten. Tämä on Fergusonin ja Schneierin mukaan väärä järjestys. Todentaa pitäisi se, mitä tarkoitetaan, ei sitä, mitä sanotaan.
- IPSecin todennus mahdollistaa myös hyökkäyksen. Oletetaan, että kaksi konetta ovat neuvotelleet AH:ta käyttävän SA:n, jossa avaimet on jaettu manuaalisesti.
- Merkitään tätä SA:ta symbolilla $\mathrm{SA}_{\mathrm{AH}}$. Koska avaimet on sovittu manuaalisesti, AH ei tarjoa suojaa uusintahyökkäyksille.
- Oletetaan nyt, että koneet neuvottelevat kuljetusmoodin ESP:n, jossa käytetään vain salausta. Merkitään vastaavaa turvayhteyttä symbolilla $\mathrm{SA}_{\mathrm{ESP1}}$.
- Tietoa välitettäessä käytetään kimppua, joka koostuu näistä kahdesta turvayhteydestä. Sovellus voi olettaa saavansa tällä tavalla luottamuksellisuuden ja todennuksen, mutta ei suojaa uusinnoilta.

Operaatioiden järjestys II

- Kun kimppuun perustuva yhteys lopetetaan, turvayhteys $\mathrm{SA}_{\mathrm{ESP1}}$ puretaan. Muutamia tunteja myöhemmin samat koneet neuvottelevat taas uuden kuljetumoodin ESP:n, jossa on vain salaus ($\mathrm{SA}_{\mathrm{ESP2}}$) ja vastaanottaja valitsee saman SPI:n arvon kuin edellisen ESP:in yhteydessä.
- Dataa välitetään taas kimpun avulla, joka sisältää sekä $\mathrm{SA}_{\mathrm{ESP2}}$:n että $\mathrm{SA}_{\mathrm{AH}}$:n.
- Hyökkääjä ujuttaa sanomien joukkoon nyt jonkin vanhan paketin edellisestä istunnosta. Tämä paketti oli salattu $\mathrm{SA}_{\mathrm{ESP1}}$:n avulla ja todennettu $\mathrm{SA}_{\mathrm{AH}}$:n avulla. Vastaanottaja toteaa todennuksen päteväksi. (Koska uusintojen suojausta ei käytetä, järjestysnumerokenttää ei käytetä.)
- Vastaanottaja purkaa sitten salauksen käyttäen $\mathrm{SA}_{\mathrm{ESP2}}$:ta, mikä tuottaa eri tuloksen kuin jos olisi käytetty $\mathrm{SA}_{\mathrm{ESP1}}$:tä.

Operaatioiden järjestys III

- Seurauksena on, että vastaanottaja hyväksyy todennetun paketin, purkaa sen väärällä avaimella ja luovuttaa vääristyneen datan sovellukselle. Eli todennus on epäonnistunut.

Opetus 3. Älä todenna pelkästään sanomaa, vaan kaikki se, mitä käytetään sanoman merkityksen määräämiseksi.

- Salatekstin todennus tekee mahdolliseksi hylätä paketteja nopeasti käyttämättä aikaa salauksen purkamiseen.
- Tämä auttaa konetta palvelunestohyökkäyksissä. Mikäli tämä koetaan tärkeäksi, salatekstin todennus voidaan säilyttää, mutta vain jos samalla todennetaan purkuavain.
- Tämä olisi mahdollista, mutta se sotisi pahasti modulaarisuutta vastaan, kun AH joutuisi kaivamaan ESP:n rakenteista salausvaimen.

Suositus 4. Modifioi ESP:tä siten, että todentaa datan lisäksi hyötykuorman salauksen purkuavaimen.

Turvayhteydet I

On aika vähän tilanteita, joissa kone lähettää IP-paketin toiselle, mutta vastausta ei lähetetä eikä oleteta. On myös vähän tilanteita, joissa täytyy turvata liikenne yhteen suuntaan, mutta ei vastakkaiseen suuntaan. Siten lähes kaikissa tilanteissa SA:t esiintyvät pareittain muodostaen symmetrisen kaksisuuntaisen kanavan. Olisi siten selvempää, että SA:t olisivat kaksisuuntaisia.

Turvapolitiikat I

- Turvapolitiikan tietokanta SPD sallii monien valitsimien käytön päätettäessä, mihin pakettiin sovelletaan mitäkin SA:ta. On mahdollista, että yksi SA hoitaa kaiken liikenteen kahden koneen välillä tai että kullakin sovelluksella on oma SA:nsa.
- Mikäli ylläpidon pitää luokitella paketit sen mukaan, mitkä vaativat IPSec-prosessointia ja mitkä eivät, vaaditaan ehkä jo liian paljon.
- Kun lisäksi ylläpidon pitää asettaa lukuisia muita IPSec-asetuksia salaus- ja todennusmenetelmistä alkaen, on todennäköistä että monet konfiguraatiot sisältävät heikkouksia.