Ìpàrokò àti VPN

1 Ọ̀rọ̀ ìṣáájú

Ìpàrokò ni ohun èlò tí a máa sàbá lò fi dáàbòbò àwọn ìsọfúnni. Nígbà gbogbo Ìtòlẹ́sẹ̀ẹsẹ̀ (algorithm) ìpàrokò ni a máa ń lò fi pàrokò, àti fi ṣàtúpalẹ̀ àrokò. Àwọn ìtòlẹ́sẹ̀ẹsẹ wọ̀nyìí máa ń lò ìṣòro ìṣírò tó le láti rí abájáde rẹ̀, bíi ìsọdipúpọ̀ àwọn òǹkaye àkọ́kọ́, àwọn ìtòlẹ́sẹ̀ẹsẹ̀ afọyè wò. Kọ́kọ́rọ́ ìpàrokò àti ti àtúpalẹ̀ ni àwon ìtòlẹ́sẹ̀ẹsẹ̀ ti òde oní ń lò.

2 Àwọn ìtòlẹ́sẹ̀ẹsẹ̀ ìpàkorò oní kọ́kọ́rọ́ àṣírí tàbí alálọ́poméjì (symmetrical)

2.1 Ọ̀rọ̀ ìṣáájú

Àwọn kọ́kọ́rọ́ ìpàkorò àti ti àtúpalẹ̀ jẹ́ ọ̀kan náà fún àwọn ìtòlẹ́sẹ̀ẹsẹ̀ oní kọ́kọ́rọ́ àṣírí tàbí alálọ́poméjì. Ìdáàbòbò dúró lórí ìfipamọ́ àwọn kọ́kọ́rọ́ wọ̀nyìí, tàbí agbára ìdojúkọ àwọn ìtòlẹ́sẹ̀ẹsẹ̀ àtàkò tàbí ti àtúpalẹ̀ àrokò: àwọn ìtòlẹ́sẹ̀ẹsẹ̀ wọ̀nyìí ni (DES, IDE, RC2, RC4, àti AES).

2.2 Àwọn ìtòlẹ́sẹ̀ẹsẹ̀ ìpàrokò alálọ́poméjì

DES (Data Encryption : Ìpàrokò ìsọfúnni)
Ní ọdun 1974 ni IBM gbé e kalẹ̀, ìtòlẹ́sẹ̀ẹsẹ̀ yìí máa ń lò àpapọ̀ bíìtì 56, kọ́kọ́rọ́ yìí ni ìjọba lò fún ọpọ̀lọpọ̀ ìgbà kó tó di pé wọ́n parọ rẹ̀ pẹ̀lú AES.

IDEA (International Data Encryption Algorithm : Ìtòlẹ́sẹ̀ẹsẹ̀ Ìpàrokò Ìsọfúnni Káríayé).

Ní ọdun 1990 ni àwọn ọgbẹ́ni X.Lai àti J. Massy gbé e jáde. Bíìtì 128 ni máa ń lò, ìtòlẹ́sẹ̀ẹsẹ̀ yìí ti bọ sí àwujọ.

B+LOWFISH 1994 ọgbẹ́ni B. SCHNEIER ló gbé e jáde, ọgbẹ́ni yìí lò bíìtì 448.

SAFER (Secure and Fast Encrytion Routine) ọgbéni J. assey ló ṣàgbékalẹ̀ rẹ̀ bíìtì 64 ni ń lò.

RC5 (Rivest code 5) 1995, ọgbẹ́ni Rivest ló ṣàgbékalẹ̀ rẹ̀, gígun kọ́kọ́rọ́ yìí máa ń yípadà.

AES (Advance Encryption Standard : Gbèdéke Ìpàrokò)
Ọdun 2000 ti ọgbẹ́ni Doemen àti V. Rijimen gbé jáde, kọ́kọ́rọ́ ìpàrokò yìí lò bíìtì 128 tàbí 256. Èyí ni ìjọba ń lò lọ́wọ́ báyìí.

2.3 Àwọn ìtòlẹ́sẹẹsẹ̀ pàṣipàárọ̀ àwọn kọ́kọ́rọ́ alálọpoméjì

Diffie – Hellman, 1976 ọgbẹ́ni W. Diffie àti M. E. Hellman ni wọ́n gbé e jáde, ìtòlẹ́sẹẹsẹ̀ yìí fún wa ni àǹfààní láti ṣe pàṣipàárọ̀ kọ́kọ́rọ́ àṣírí lẹ́yìn pàṣipàárọ̀ àwọn ìsọfúnni. Kọ́kọ́rọ́ Diffie – Hellman dúró lórí ìṣòro àti ṣírò lógárítímù olóye.

RSA (Rivest Shamir Adleman), 1978
Àwọn ọgbẹ́ni R. Rivest , A. Shamir àti L. Adlman ni wọ́n gbé e kalẹ̀, lẹ́yìn paṣipàárọ̀ kọ́kọ́rọ́ àti ìsọfúnni. Ìdáàbòbò dúró lórí ìṣòro láti sọ àwọn òǹkaye àkọ́kọ́ di púpọ̀. Kọ́kọ́rọ́ yìí ti di ti àwùjọ.

Àwọn àlàkalẹ̀ ètò ìpàrokò oní ìlà ìrísí ẹ̀yin 1985 – 2005

- **ECMQV** (Elliptic Curve Menezes-Qu-Vanstone)
- **ECDH** (Elliptic Curve Diffie – Hellman)

Àwọn ọgbẹ́ni V. Miller àti N. Kollitz ni wọ́n gbé e jáde, wọ́n ti ṣèwádìí púpọ̀ sórí àwọn kọ́kọ́rọ́ wọ̀nyìí tí ìdáàbòbò wọn múnádóko, tí gígùn kọ́kọ́rọ́ kò pọ̀ jù tó sì yàtọ̀ sí àwọn ìtòlẹ́sẹẹsẹ̀ mì ín. Agbára ìdáàbòbò dúró sórí ìṣòro lógárídímù olóye.
Àfojúsùn àwọn ìfẹnukò tí òní ni ti pàṣipàárọ̀ àwọn kọ́kọ́rọ́ láàrin ojúmọ̀sọ̀rọ̀pọ̀ méjì fún sáà ni ọ̀nà ìdàábòbò tàbí fún àsìkò kan nínú sáà kan. Orí ìpele kéjì ni a yóò lò ìtòlẹ́sẹẹsẹ̀ ìpàrokò ìsọfúnni alálọ́poméjì tó sì yára jù ìtòlẹ́sẹẹsẹ̀ àìlọ́poméjì lọ.

<u>Àpẹẹrẹ</u>

Àwọn ìpele ìtòlẹ́sẹẹsẹ̀ Diffie – Hellman

1º Àlàbi pẹ̀lú Òjó mú òǹkàye àkọ́kọ́ p àti òǹkàye g tó kére sí p tó sì jẹ́ òǹkàye ojúlówó (g jẹ́ ojúlówó sí p nígbà tí : fún u láti 1 dé p-1 òǹkàye v kan wà tí g^v = u mod(p) nínú àkójọpọ̀ ìlọ́po (Z/pZ, *).

Nígbà tí a bá mú p = 11 tí g = 2 a lè rí dájú pé g jẹ́ ojúlówó sí p :

$2^{10} = 1$ mod(11), $2^1 = 2$ mod(11), $2^8 = 3$ mod(11), $2^2 = 4$ mod(11),
$2^4 = 5$ mod(11), $2^9 = 6$ mod(11), $2^7 = 7$ mod(11), $2^3 = 8$ mod(11),
$2^6 = 9$ mod(11), $2^5 = 10$ mod(11).

1. Àlàbí yàn kọ́kọ̀rọ́ àṣírí kan a = 5 tó sì fi í ránṣẹ́ sí Òjó.

$X = g^a$ mod(p) = 2^5 mod(11) = 10.

2. Òjó yàn kọ́kọ̀rọ́ àṣírí kan b = 7 tó sì fi í ránṣẹ́ sí Àlàbí

$Y = g^b$ mod(p) = 2^7 mod(11) = 7.

3. Àlàbí lè ṣírò kọ́kọ̀rọ́ àṣírí :

$(Y)^a$ mod(p) = (gb mod(p))^a mod(p) = (7)5 mod(11) = 10.

5. Òjó pẹ̀lú le ṣíró kọ́kọ̀rọ́ àṣírí:

$(X)^b$ mod(p) = (g^a mod(p))b mod(p) = (10)7 mod(11) = 10.

Fún àwọn ìwọ́pọ̀ tí àwọn àfidámọ̀ jẹ́ aláròpọ̀ àgbára, ìdọ́gba $(g^b)^a = (g^a)^b$ fẹsẹ̀múlẹ̀, àwọn apá méjèjì ní kọ́kọ̀rọ́ àṣírí. Ìdáàbòbò ìtòlẹ́sẹẹsẹ yìí dúró sórí ìṣòro láti rí àbájáde fún ìṣòro lógárítímù olóye. A ò lè mọ̀ a (tàbí b) pẹ̀lú g^a tàbí g^b tó ní ìbátan pẹ̀lú a, b, g, n tí a yàn, ìsòro tó lè gan an ni, tí ó sì ṣòro láti rí àbájáde tó dájú fun àwọn òǹkàye tó g a. Lọ́dún mélòó kan sẹ́yìn àṣàmúdọ́gba ìtòlẹ́sẹẹsẹ ètò Diffie–Hellman pẹ̀lú àwọn ìjọ mì ín ṣe ìgbéjáde ìtòlẹ́sẹẹsẹ ìpàrokò sórí ìlà ìrísí bíi ẹyin. Èrò tó wà lẹ́yin yìí ni kí a lò ìjọ G; ìjọ àwọn ojú àmì tó wà lórí ìlà ìrísí ẹyin. Lórí ìjọ tó níye. (ìjọ aláfikun (EC (GF(2m)), +).Kí a máa fà á gùn a ò mọ̀ ìtòlẹ́sẹẹsẹ àpọ̀júwọn tí ń rí àbájáde sí ìṣórò fún lógárídímù olóye ni ìpò yìí, èyí tó yàtọ̀ sí logárítímù olóye nínú ìjọ onílọ́po G, ìjọ ìníye onílọ́po (Z/pZ, *). Èyí fi yé wa wípé a lè lò kọ́kọ̀rọ́ ti kò gùn jù. Ní báyìí bíìtì 170 (ìjọ aláfikun (EC(GF(2m)), +) fi ní ìdáàbòbò tó péye jù kọ́kọ̀rọ́ Diffie–Hellman tí ń lò bíìtì 1024 (ìjọ onílọ́po (Z/pZ, *).
Àwọn ìtòlẹ́sẹẹsẹ ìpàroko àwùjọ tàbí àìlọ́poméjì jẹ́ àwọn ìtòlẹ́sẹẹsẹ ti a ń lò lóní, tí a fi dáàbòbò àwọn ìsọ́fúnni wa, tó sì yàtọ̀ sí ìtòlẹ́sẹẹsẹ ìpàrako àṣírí tàbí alọ́poméjì, kọ́kọ̀rọ́ méjì ni a máa ń lò fún olúmúlò (àṣírí, káríayé). Àwọn ìtòlẹ́sẹẹsẹ àìlọ́poméjì ni a ń lò púpọ̀ jù.

2.4 Ìtòlẹ́sẹẹsẹ ìpàroko òní kọ́kọ̀rọ́ káríaye tàbí àìlọ́poméjì

2.4.1 Ọ̀rọ̀ ìṣáájú

Fún àwọn ìtòlẹ́sẹẹsẹ̀ wọ̀nyìí, kọ́kọ́rọ́ ìpàrokò àti ti àtúpalẹ̀ àrokò yàtọ. Ìdáàbòbò dúró lórí àsìkò ti a yóò lò fi ṣírò kọ́kọ́rọ́ àsírí pẹ̀lú kọ́kọ́rọ́ káríayé, kò ṣeé ṣe, ó máa lè kí a rí àbájade fún ìṣóró yìí.

2.4.2 Àwọn kọ́kọ́rọ́ àìlọ́pọméjì :

RSA (Rivest Shamir Adeleman), àwọn onílà ìrísí ẹyin, Pohlig-Hellman, Eabin àti ElGomal.
Àwọn ìtòlẹ́sẹẹsẹ̀ alọ́pọméjì máa ń yara jù àwọn àìlọ́pọméjì tí a bá dán wọn wò. Àmọ́ a ò lè sọ pé ìtòlẹ́sẹẹsẹ̀ alọ́pọméjì ní ìdáàbòbò jù, tàbí kò níí ìdáàbòbò jù àwọn ìtòlẹ́sẹẹsẹ̀ àìlọ́pọméjì lọ, àmọ́ ìwúló wọn ló yàtọ̀. Ìsòró díẹ̀ tó wa fún ìtòlẹ́sẹẹsẹ̀ alọ́pọméjì ni kí àwọn apá ti ń ṣe pàṣipààrọ̀ ní láti ní kọ́kọ́rọ́. Tí a sì gbé àwọn ohun èlò kọ́kọ́rọ́ yìí gbànu ìsokọ́ra. Láti rí ọ̀nà àbáyọ fún ìṣòró yìí ni ìgbéjáde àwọn kọ́kọ́rọ́ àìlọ́pọméjì wáyé, àwọn kọ́kọ́rọ́ náà ni wọ̀nyìí :

RSA (Rivest Shamir Adeleman) Ní ọdun 1978 ni àwọn ọgbẹ́ni R. Rivest, A. Shamir, M. O Rabin ṣàgbékalẹ̀ ìtòlẹ́sẹẹsẹ̀ ìpàroko oní kọ́kọ́rọ́ oníyípadà àìlọ́pọméjì, ìdáàbòbò dúró sórí ìṣòro àti sọ àwọn òǹkàye àkọ́kọ́ di púpọ̀.

ROBIN ní ọdun 1979 ni ọgbẹ́ni M. O. Robin ṣàgbékalẹ̀ ìtòlẹ́sẹẹsẹ̀ ìpàroko oní kọ́kọ́rọ́ oníyípadà àìlọ́pọméjì yìí, ìdáàbòbò dúró sórí ìṣòrò láti ṣírò orísún onílọ́pọméjì móòdù òǹkàye ẹ̀ka òǹkàye.

EL Gamal 1985 tí ọgbẹ́ni T.ELGamal gbé kalẹ̀, alúgórídíìmù dúró sórí àwọn kọ́kọ́rọ́ oníyípadà, ìdáàbòbò dúró sórí àwọn kọ́kọ́rọ́ pẹ̀lú ìṣórò láti ṣírò àwọn lógárítímù olóye.

Ìtòlẹ́sẹẹsẹ ìpàroko oní ìrísí ẹyin, 1985 – 2005
ECIES (Elliptic Curve Integrated Encryption Standard)

Ìdáàbòbò RSA dúró sórí ìṣórò láti sọ òǹkàye n kan di púpọ̀ (Nígbà tí kọ́kọ́rọ́ àṣírí àti ti káríayé bá jẹ́ p àti q alátàkò láti sọ n di púpọ̀ fi fọ ìpàroko).
Àti rí àwọn ìlọ́po òǹkàye àkọ́kọ́ n (ti a sì mú n bó ṣe wú wa) jẹ́ ìṣòro tí àbájàde rẹ̀ ò ṣeé ṣe lọ́wọ́ lọ́wọ́ báyìí pẹ́lú ìdánilójú (ìṣòro ìṣírò).

Fún kọ́kọ́rọ́ RSA p àti q tí a máa mú, ó yẹ kí ìlọ́po àwọn òǹkàye méjèjì wà lọ́na tí ó máa jẹ́ bíìtì 1024. Lẹ́yìn ìṣòro ìsọdipúpọ̀ òǹkàye kan, ìṣórò mì ín ti a tún ní ni ìyọkúrò ìdọ́gba lógarítímù olóye. Ní òde oníí bíìtì 170 ni a ń fún kọ́kọ́rọ́ fi ní ìdáàbòbò kannáà pẹ̀lú bíìtì 1024 RSA.
Lónìí a máa ń lò àwọn ìtòlẹ́sẹẹsẹ̀ onílọ́pọméjì fún ìpàkòrò àwọn ìsọfúnni, a sì ń lò àwọn ìtòlẹ́sẹẹsẹ̀ àìlọ́pọméjì fún ìfàṣẹsí àti pàṣipààrọ̀ àwọn kọ́kọ́rọ́.

3 Àwọn ìtòlẹ́sẹẹsẹ̀ pàtàkì ìfọwọ́síwé olóǹkàye

RSA (Rivest Shamir Adeleman) 1978 ti àwọn ọgbẹ́ni R. Rivest, A. Shamir, M. O Rabin ló ṣàgbékalẹ̀ ìtòlẹ́sẹẹsẹ̀ ìpàrokò oní kọ́kọ́rọ́ oníyípadà àìlọ́pọméjì yìí, ìdáàbòbò dúró sórí ìṣòró àti sọ àwọn òǹkàye àkọ́kọ́ di púpọ̀.

DSA (Digital Signature Algorithm : Ìtòlẹ́sẹẹsẹ̀ Ifọwọ́síwé olóǹkàye) 1991 ọgbẹ́ni D. W Kravitz (N S A) ló ṣàgbéjáde ẹ, ètò yìí ni ìjọba ń lò fún ìfọ́wọ́síwé.

GOST (Gosudarstvennyi Standard of Russia Federation) 1994 ìtòlẹ́sẹẹsẹ̀ ti ẹ̀ka ilésẹ́ ìpàroko Rọsià gbé kalẹ̀, ìtòlẹ́sẹẹsẹ̀ yìí ni wọ́n lò fún ìfọ́wọ́síwé.

ESIGN 1990 àwọn ọgbẹ́ni A.Fujiaski àti T.Okamoto ni wọ́n gbé e jáde, àwọn iléṣẹ́ ẹ̀rọ ìbánisọ̀rọ̀ Japan NTT ni lò ó.

Àwọn ètò ìpàroko oní ìlà ìrísí ẹyin 1985 – 2005

– ECDSA (Elliptic Curve Digital Signature Algorithm)
– ECPVS (Elliptic Curve Pintsov Vanstone Signatures)
– ECNR (Elliptic Curve Nyberg Rueppel)

Àwọn ọgbẹ́ni V. Miller àti N. Koblitz ni wọ́n gbékalẹ̀, àwọn ìwádìí púpọ̀ ló lọ lórí rẹ̀, tí ìdáàbòbò wọn sì múnádókó ti wọn sì dójú kọ àwọn ìṣàtúpalẹ̀ àrokò àwọn alátákò, kọ́kọ́rọ́ wọn ò sì tún gùn jù. Ìdáàbòbò wọn dúró sórí ìṣòro ìṣírò lógárítímù olóye. Iléṣẹ́ Certicom ní ìjẹ́rìísí lọ́pọlọ́pọ̀.

4 Iṣé ààké

Iṣé ààké máa ń ṣàkójọ àmì àwọn àtòtẹ̀lé ìsọfúnni ti àyọkà, tí a sì tún lè dá padà sí orísun, ṣíṣeéṣe kí àwọn àtòtẹ̀lé ìsọfúnni méjì ní àmì kannáà kére jù.
A yóò lò àmì yìí fi ṣàyẹ̀wò pípeye iṣẹ́ẹ̀jẹ́ tí a firánṣẹ́:
A yóò ṣàkójọ àmì ti iṣẹ́ẹ̀jẹ́ kan, a máa fi àmì yìí ránṣẹ́ àti iṣẹ́ẹ̀jẹ́. Lẹ́yin ti a bá gbà iṣẹ́ẹ̀jẹ́ a yóò ṣírò àmì yìí, a sì máa fi wé àmì tí a gbà, tí àwọn méjèjì bá dọ́gba, Èyí túmọ̀ sí wípé àwọn iṣẹ́ẹ̀jẹ́ dọ́gba. Àwọn ojúlówó ìṣe ààké tí a ní ni MD5, RIPE-MD àti SHA-x (x=1, 256, 384, 512)

MAC (Message Authentification Code : ìtọ́sọ́nà ìfàṣẹsí iṣẹ́ẹ̀jẹ́)

Àmì ìfàṣẹsí ìṣẹ́ẹ̀jẹ́ ni abájáde iṣé ààké ni ìdárí kan tó níbatan pẹ̀lú kọ́kọ́rọ́ àṣírí, èyí tó túmọ̀ sí pé a lè ṣàkójọ MAC kan pẹ̀lú iṣé ààké tàbí ìtòlẹ́sẹẹ̀sẹ̀ ìpàrokò ni ìṣupọ̀ kan.
Ọ̀nà tó rọrùn láti lè fi ṣèyípadà ìṣe ààké oní ìdárí kan sí MAC ni kí a ṣèpàrokò àmì iṣẹ́ẹ̀jẹ́ pẹ̀lú kọ́kọ́rọ́ àṣírí.
Ọ̀nà ìṣírò MAC pẹ̀lú iṣé ààké tó tún ní agbára, tó sì tún dání lójú ni HMAC (RFC 2104) àlàkalẹ̀ HMAC máa fún wa ni àǹfààní láti lò ó pẹ̀lú àwọn iṣé ààké MD5 tàbí SHA-x.
Nǹkan ti a máa ń sàbá ṣé pẹ̀lú àwọn ìṣe ìṣírò MAC ni kí a gé ìwọ̀n kan nínú àbájáde, kí a sì mú ìdá kan nínú àwọn bíìtì dání. Pẹ̀lú HMAC a lè pínnu láti mú bíìtì mélòó kan ti apá òsì.
Àwọn kọ́kọ́rọ́ ni àtòtẹ̀lé àwọn bíìtì ti a mú pẹ̀lú ìṣe oní rúdurùdu ti a yàn. Pẹ̀lú ìtòlẹ́sẹẹ̀sẹ̀ DSA alọ́pọméjì, gbogbo àwọn kọ́kọ́rọ́ ti a ń lò kò jù 256 lọ.
Fún àwọn ìtòlẹ́sẹẹ̀sẹ̀ àìlọ́pọméjì bíi RSA, àwọn kọ́kọ́rọ́ wà láàrin àwọn òǹkaye àkọ́kọ́, àwọn wọ̀nyìí máa ń wà nínú àwọn kọ́kọ́rọ́ tí a ṣàkójọ wọn.
Àwọn kọ́kọ́rọ́ ìpàrokò lè fún wa ni ìṣòró, tí á sì di agbára ètò ìsiṣẹ́ wa kù tí a bá mú àwọn kọ́kọ́rọ́ a ní láti ṣÀkójọ kọ́kọ́rọ́ pẹ̀lú àwọn ìtòlẹ́sẹẹ̀sẹ̀ ìpàroko tó dájú, pẹ̀lú àwọn ohun èlò tó wà lórí ayélújara ní èéwu.

4.1 Ìṣàkójọ kọ́kọ́rọ́ òǹkaye oní àkọ́kọ́

Nígbà tó jẹ́ wípé àwọn kọ́kọ́rọ́ ti a ń lò, ìṣàkójọ wọn wá láti àwọn òǹkàye àkọ́kọ́, Àwọn òǹkaye wọ̀nyìí níye. Àwọn ọ̀jọ̀gbọ́n nínú ìṣírò mú àwójúùtù wa. Wọ́n fi yé wípé àwọn òǹkà wọ̀nyìí kò níí òpin, a lè ṣẹ̀dá 2151 nọ́mbà pẹ̀lú bíìtì 512.

4.2 Ìṣàtúpalẹ̀ àrokò àwọn ìtòlẹ́sẹẹ̀sẹ̀

Ìṣàtúpalẹ̀ òrokò ni kí a dá ìsọfúnni tí a pàrokò padà sí orísun. Àwọn ajalèlókun máa sàbá fi àwọn àtàkò lórísìrísì ránṣẹ́ fi ṣàtúpalẹ̀ ìpàrokò.

5 Ìfọ́wọ́síwé (olóǹkàye dígítà pẹ̀lú kọ́kọ́rọ́ onílọ́pọméjì káríayé/àṣírí)

5.1 Ọ̀rọ̀ ìṣáájú

Àwọn ìtòlẹ́sẹẹ̀sẹ̀ ìpàrokò oní kọ́kọ́rọ́ káríayé/àṣírí àìlọ́pọméjì ni a yóò máa lò ni òde òní láti fi ṣé pàṣipààrọ̀ àwọn kọ́kọ́rọ́ ti a pàrokò, àti fún ìfọwọ́síwé ìsọfúnni.
Èyí tó yàtọ̀ sí ìtòlẹ́sẹẹ̀sẹ̀ ìpàrokò alọ́pọméjì tàbí oní kọ́kọ́rọ́ àṣírí.
A máa ṣàkójọ kọ́kọ́rọ́ méjì fún olùmúlò kọ̀ọ̀kan (káríayé, àṣírí) a yóò ṣírò àwọn

kọ́kọ́rọ́ wọ̀nyìí pẹ̀lú ìlànà tó múnádóko tó jẹ́ ìlànà àwọn olóǹkaye.
Kọ́kọ́rọ́ àṣírí máa wà nípamọ́ tí a sì gbé ti káríayé síta.

5.2 Ìlànà ìṣiṣẹ́

Nígbà tí Àlàbi bá pinnu láti fi iṣẹ́ẹ̀jẹ́ ránṣẹ́ sí Fakoredé, Ó máa pàrokò iṣẹ́ẹ̀jẹ́ náà pẹ̀lú kọ́kọ́rọ́ káríayé ti Fakoredé. Nígbà náà Fakoredé nìkan ló lè ṣí iṣẹ́ẹ̀jẹ́ yìí.
Nígbà tí Fakorede bá fẹ́ fi iṣẹ́ẹ̀jẹ́ ránṣẹ́ sí Àlàbi ó yóò pàrokò èyí pẹ̀lú kọ́kọ́rọ́ káríayé Àlàbi, nígbà náà Àlàbi nìkan ló lè ka iṣẹ́ẹ̀jẹ́ náà.
Ìtòlẹ́sẹẹsẹ̀ ìpàrokò àìlọ́pọméjì kìí gbé kọ́kọ́rọ́ gbà inú ìsokọ́ra. Ìdáàbòbò àwọn alúgórídímù wọ̀nyìí dúró lórí pé kọ́kọ́rọ́ àṣírí ò jẹ́ mímọ̀ fún èèyàn kan, kò sí bọ síta, pẹ̀lú kọ́kọ́rọ́ káríayé ó ṣòrò láti ṣírò kọ́kọ́rọ́ àṣírí ní àkókó tó Kére.
Ìṣàkójọ àwọn kọ́kọ́rọ́ àṣírí/káríayé ní ètò tó péye tó sì dúró lórí àwọn òǹkàye àkọ́kọ́. Gbogbo àwọn kọ́kọ́rọ́ ti a lè ṣàkójọ wọn dúró lórí àwọn òǹkàye àkọ́kọ́.

Àpẹẹrẹ

A yóò lò RSA fi ṣe ìpàrokò àti ìṣàtúpalẹ̀ :
Nígbà tí a bá mú àwọn òǹkàye àkọ́kọ́ méjì wọ̀nyìí p = 47 àti q = 71
p x q = 3337
Nínú kọ́kọ́rọ́ káríayé (e, n), e jẹ́ òǹkàye àkọ́kọ́ sí :
(p -1) x (q – 1) = (47 – 1)(71 – 1) = 3220
Nígbà tí a bá mú e = 79 lọ́nà rúdurùdu làìyàn, ẹ jẹ́ ká rí pé 79 jẹ́ nọ̀mbà àkọ́kọ́ sí 3220, a máa ṣìró PGCD,GIAJ(3220,79) pẹ̀lú alúgórídímù Euclide.
Nígbà tí a bá fẹ́ ṣírò GIAJ (a, b)

$a = bq_0 + r_0$, $b = r_0q1 + r1$, …, $r_{n-1} = r_nq_{n+1} + r_{n+1}$, avec
$r_{n+1} = 0$, alors

GIAJ(a,b) = rn) :

(1) 3 220 = 79x40 + 60

(2) 79 = 60x1 + 19

(3) 60 = 19x3 + 3

(4) 19 = 3x6 + 1

79 jẹ́ nọ̀mbà àkọ́kọ́ 3 220.

La clé privée (d,n) est calculée à partir de la formule suivante :

d = e– 1 mod[(p – 1)(q – 1)] = 79– 1 mod(3 220) = 1 019 (relation de Bezout : si a est inversible dans Z/nZ, il existe u et v tels que axu+nxv=1).

Si nous partons de la division euclidienne précédente, nous pouvons construire la relation

de Bezout de la façon suivante :

(4) 19 – 3x6 = 1

(3) 3 = 60 – 19x3

(4) Combiné avec (3) : 19 – (60 – 19x3)x6 = 1

(4) – 60x6 + 19x19 = 1

(2) 79 – 60x1 = 19

(4) Combiné avec (2) : – 60x6 + (79 – 60x1)x19 = 1

(4) – 60x25 + 79x19 = 1

(1) 3 220 – 79x40 = 60

(4) Combiné avec (1) : – (3 220 – 79x40)x25 + 79x19 = 1

(4) – 3 220x25 + 79x(40x25 + 19) = 1

(4) – 3 220x25 + 79x1 019 = 1

1 019 est donc bien l'inverse de 79 dans Z/(p – 1)(q – 1)Z

Ìpàrokò / Ìṣàtupalẹ̀
Inú ìjọ ìlọ́po (Z/nZ, *) ni a ti máa ṣe ìṣírò.
Nígbà tí a bá fẹ́ pàrokò nọ́mbà m, a máa lò àlàkalẹ̀ yìí pẹ̀lú kọkọrọ káríayé
(e, n) : $c = m^e \bmod(n)$.
Nígbà tí m = 688 a máa ní ìdọ́gba :
$c = 688^{79} \bmod(3337) = 1570$
Nígbà tí a bá fẹ́ ṣètúpalẹ̀ àrokò yìí a máa lò àlàkalẹ̀ :
$m = c^d \bmod(n) = 1570^{1019} \bmod(3337) = 688$.

Nígbà tí e àti d jẹ́ ìyídà modulo sí ara wọn:
(p – 1)(q – 1), ed = 1 + k(p – 1)(q – 1) fún k kan.

Ìdáàbòbò RSA dúró sórí ìṣòrò láti sọ òǹkàye di púpọ̀ (Nígbà tí a ṣàkójọ àwọn kọ́kọ́rọ́ káríayé àti àṣírí pẹ̀lú àwọn p àti q àwọn ajalèlókun ní láti sọ n di púpọ̀ fi fọ kọ́kọ́rọ́ náà). Ìsórò gan an ni tí a ò mọ àgbéjáde rẹ̀ ni kí a rí àwọn olùsọdipúpọ̀ òǹkàye ńlá n. Lóde oníì a ní láti lò àwọn òǹkàye p àti q tí ìlọ́po wọn jẹ́ bíìtì 1024 fún RSA.

Àpẹẹrẹ mìn ín

Pẹ̀lú àwọn òǹkàye àkọ́kọ́ tó kére

1. A yàn òǹkàye àkọ́kọ́ $p = 3$, $q = 11$;
2. Ìlọ́po wọn $n = 3 \times 11 = 33$ ni ohun èlò ìpàrokò;
3. $\varphi(n) = (3 - 1) \times (11 - 1) = 2 \times 10 = 20$;
4. Nígbà tí a bá mú $e= 3$ (àkọ́kọ́ pẹ̀lú 20) bíi agbára ìpàrokò ;
5. Agbára àtúpalẹ̀de nit $d = 7$, alòdì 3 modulo 20 (lóòótọ́ $ed = 3 \times 7 \equiv 1 \bmod 20$).

Kọ́kọ́rọ́ káríayé Òjó ni $(n, e) = (33, 3)$, kọ́kọ́rọ́ àṣírí ni $(n, d) = (33, 7)$. Àlàbí yóò fi iṣéèjẹ́ ránṣẹ́ sí Òjó.

- Ìpàròko $M = 4$ pẹ̀lú kọ́kọ́rọ́ káríayé òjó $4^3 \equiv 31 \bmod 33$, àròko ni $C = 31$ tí Àlàbí yóò fi ránṣẹ́ Òjó;
- Àtúpalẹ̀ $C = 31$ tí yóò ṣe pẹ̀lú kọ́kọ́rọ́ àṣírí rẹ̀: $31^7 \equiv 4 \bmod 33$, Òjó máa rí iṣẹ́ẹ̀jẹ́ orísún $M = 4$.

Le mécanisme de signature par Alice, à l'aide de sa clé privée, est analogue, en échangeant les clés.

5.3 Ìyọkúrò àwọn lógárítímù olóye

Lẹ́yìn ìṣòró ìsọdipúpọ̀ òǹkàye odidi, nínú ètò ìpàrokò, àwọn ìṣọ̀ró mì ín ni kí a ṣèyọkúrò lógáritímù olóye tí a ṣàlàyé báyìí:

Bí **àpẹẹrẹ:** àwọn ìpele pàṣipàárọ̀ tí ń fún wa ní àǹfààní láti ṣèpàrokò àti fọwọ́síwé iṣẹ́ẹ̀jẹ́ pẹ̀lú ìtòlẹ́sẹẹsẹ̀ RSA.

1. Nígbà ti a ṣàkójọ àwọn kọ́kọ́rọ́ (àṣírí / káríayé), Àlàbi lè ṣàkójọ ìfọwọ́síwé olóǹkàye iṣẹ́ẹ̀jẹ́ rẹ̀, fún ìjẹ́rìísí pé òun ló ní iṣẹ́ẹ̀jẹ́ tó fẹ́ firánṣẹ́, ó máa gbé iṣẹ́ẹ̀jẹ́ yìí gbànu iṣé ààké láti ṣàmì ìdánimọ̀ sí lórí.

2. Àlàbí yóò pàrokò iṣẹ́ẹ̀jẹ́ alámì yìí pẹ̀lú kọ́kọ́rọ́ àṣírí rẹ̀, kó fi ní ìfọwọ́síwé olóǹkàye nígbà tí kọ́kọ́rọ́ Àlàbi ti jẹ́ àkànṣe tí kò sì bọ́ síta, Àlàbi nìkan ló lè ní ìfọwọ́síwé yìí lọ́wọ́.
3. Lẹ́yìn ìfọwọ́síwé Àlàbi máa fi iṣẹ́ẹ̀jẹ́ àti ìfọwọ́síwé ránṣẹ́ sí Òjó, Àlàbí tún lè pàkorò iṣẹ́ẹ̀jẹ́ pẹ̀lú kọ́kọ́rọ́ káríayé Òjo kó fi bo ó ní àṣírí.
4. Fi rí dájú pé ìfọwọ́síwé olóǹkaye yìí ti Àlàbí ni, Òjó máa gbé e gbànu iṣẹ́ ààké kannáà tí Àlàbí lò.
5. Nígbà kannáà ó máa ṣàtúpalẹ̀ àrokò ìfọwọ́síwé Àlàbi pẹ̀lú kọ́kọ́rọ́ káríayé rẹ̀.
6. Àwọn ìgbésẹ̀ méjèjì wọ̀nyìí máa jẹ́ kó ní àwọn iṣẹ́ẹ̀jẹ́ alámì méjèjì lọ́wọ́: Àmì iṣẹ́ẹ̀jẹ́ tó firánṣẹ́ àti àmì iṣẹ́ẹ̀jẹ́ ìfọwọ́síwé tó gbà. Tí àwọn méjèjì bá dọ́gba, èyí túmọ̀ sí wí pé iṣẹ́ẹ̀jẹ́ Àlàbi ni, bí kò bá jẹ́ bẹ́ẹ̀ ìṣòró máa wà. A lè lò ìtòlẹ́sẹẹsẹ̀ tó wà nínú étò ìṣiṣẹ́ fi ṣàyẹ̀wó iṣẹ́ẹ̀jẹ́ bíi ètòlẹ́sẹ̀sẹ̀ imel.

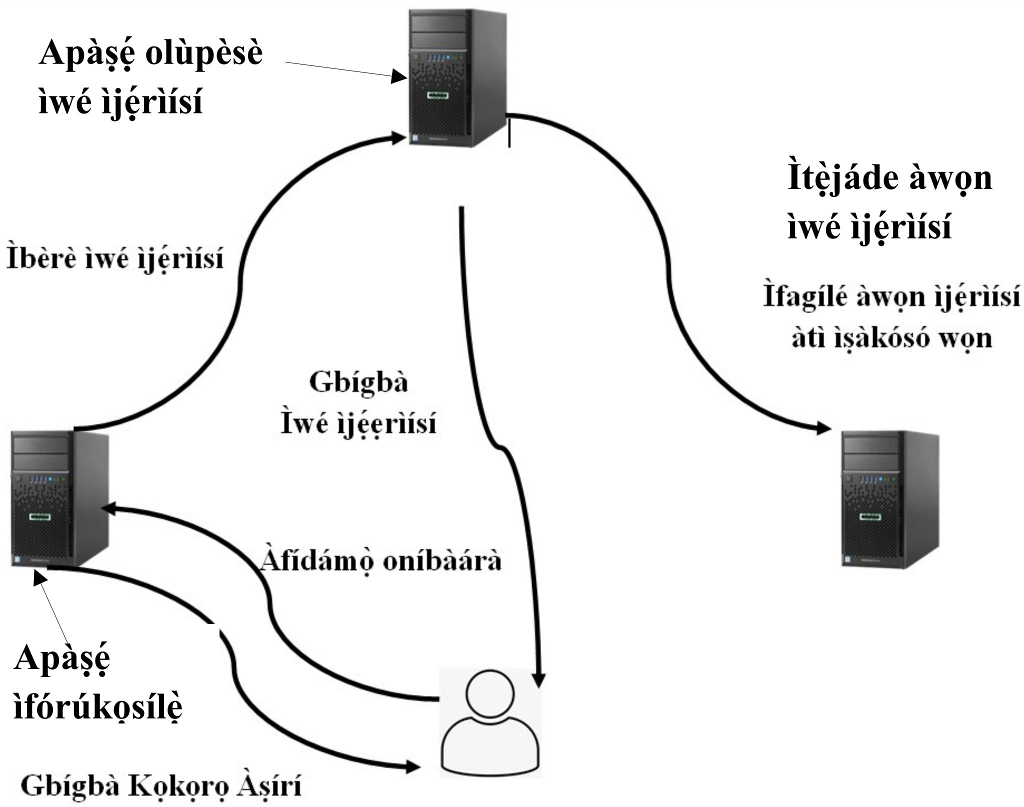
V Ìjẹ́rìísí olóǹkàye (digital certificat)

Ìjẹ́rìísí jẹ́ ìwé ìdánilójú fún ìdámọ̀ olóǹkàye èèyàn kan tàbí ti àgbékalẹ̀.
Àwọn amáyédẹrùn :
PKI (Public Key Infrastrucutre : Amáyédẹrùn Káríayé kọ́kọ́rọ́).
PKI jẹ́ àwọn ẹ̀rọ kọ̀ńpútà, àwọn ètòlẹ́ṣẹ̀sẹ̀, àlànà àti àwọn àlàkalẹ̀...
Iṣẹ́ PKI:

- Ìforúkọsílẹ̀ àwọn olùmúlò, tàbí àwọn ilẹ́ṣẹ́ tó fẹ́ gbà ìjẹ́rìísí .
- Àkójọ àwọn kọ́kọ́rọ́ oníméjì : kọ́kọ́rọ́ káríayé àti àṣírí
- Ìṣàrídájú àwọn kọ́kọ́rọ́ káríayé láti fi ṣé ìjẹ́rìísí olóǹkàye àti ìpologo wọn sórí àwọn àkójọpọ̀ káríayé bíi apèsè LDAP
- Ìfagílé àwọn ìjẹ́rìísí àtì ìṣàkóso àwọn àtòkọ wọn.
- Láti gbà ìwé ìjẹ́rìísí a ní láti tẹ̀lé àwọn àlàkalẹ̀ kan àti àwọn òfin tó jẹ́ dandan tí a sàlàyé wọn :
    1. Olùmúlò tó fẹ́ ní ìwé ìjẹ́rìísí láti béèrè lọ́dọ àwọn apàṣẹ́ ìforúkọsílẹ̀ EA
    2. Nígbà tí wọ́n bá ti ṣàyèwó ìwé ìdánimọ̀, EA máa ṣàkójọ kọ́kọ́rọ́ méjì (àṣírí / káríayé), tó sì máa fi kọ́kọ́rọ́ àṣírí ránṣẹ́ sí olùmúlò gbọ̀nà ààbò tó dájú.
    3. Apàṣẹ́ ìforúkọsílẹ̀ (EA) máa ṣàrídájú kọ́kọ́rọ́ káríayé tí yóò sì ṣèfọwọ́síwé olóǹkàye sórí ìwé ìjẹ́rìísí.
    4. Ìwé ìjẹ́rìísí máa wà ni ìṣàgbékalẹ̀ lórí àkójọpọ̀ tí gbogbo èèyàn sì lè wò ó. Ìwé ìjẹ́ẹ̀ìísí tàbí ìwéìrìnnà olóǹkàye máa ń ní gbogbo àwọn ìsọfúnni ti ìdànímọ̀ tàbí àwọn ẹ̀ka mì-ín :

- Òǹkàye àgbéjáde tó somọ̀ ìwé ìjẹ́rìísí : àpẹẹrẹ X.509.V3
- Òǹkàye àtòtẹ̀lé tí EA fún
- Ìtòlẹ́sẹẹsẹ tí wọ́n lò
- Orúkọ apàṣẹ́ tó ṣàgbéjáde ìwé ìjẹ́rìísí
- Ọjọ́ ìparí ìwé ìjẹ́rìísí
- Orúkọ ẹni tí yóò gbà ìwé yìí
- Kọ́kọ́rọ́ káríayé ẹni tó ní ẹ̀tọ́ láti gbà ìwé yìí

Apàṣẹ́ ìwé ìjẹ́rìísí máa ṣàyẹ̀wò gbogbo àwọn ìwé wọ̀nyìí pẹ̀lú ọjọ́ tó máa pari. Apàṣẹ́ ìwé ìjẹ́rìísí máa ṣàgbékalẹ̀ ìṣàmìsí pẹ̀lú gbogbo àwọn ìsọfúnni tí yóò sì lò ìtòlẹ́sẹẹsẹ aláàké. Lẹ́yìn èyí, yóò pàrokò ìṣàmìsí yìí pẹ̀lú ìtòlẹ́sẹẹsẹ̀ àìlọ́pọméjì pẹ̀lú kọ́kọ́rọ́ àṣírí apàṣẹ́ ìwé ìjẹ́rìísí, gbogbo èyí máa jẹ́ kí ìṣàgbékalẹ̀ ìfọwọsí ìwé ìjẹ́rìísí wáyé.
Láti ṣàyèwò ìfọ́wọ́sí apàṣẹ́ ìwé ìjẹ́rìísí a yóò mú gbogbo àwọn ìsọfúnni àfídámọ̀ ìwé ìjẹ́rìíṣí làì lò ìfọwọ́sí, fi ṣàgbékalẹ̀ ìṣàmìsí àti fi ṣàtúpalẹ̀ ìfọ́wọ́sí apàṣẹ́ ìwé ìjẹ́rìísí láti pẹ̀lú kọ́kọ́rọ́ káríayé rẹ̀ láti fi rí ìfọwọ́sí orísun, lẹ́yìn èyí a yóò fi àwọn ìfọwọ́sí méjèjì wé ara wọn, tí ìdọ́gba bá wà, èyí yóò túmọ̀ sí pé ìwé ìjẹ́rìísí jẹ́ ojúlówó, bí kò jẹ́ bẹ́ẹ̀ a ò lè fijẹ́rìí sí ìwé náà.
Ìwé ìjẹ́rìísí máa ń wà ni àgbáyé, àmọ̀ kọ́kọ́rọ́ àṣírí tó somọ̀ yóò wà ní ìdáàbòbò, ní ààbò tó múnádóko lórí àwọn ẹ̀rọ ẹrun ìdáàbòbò pẹ̀lú àmì òǹkàye PIN fún ìṣèdámọ̀ oní nǹkan.
Lílò kọ́kọ́rọ́ onílọpoméjì káríayé àti ìpologo wọn gbà ká ní ìgbàgbọ gidi lórí àwọn kọ́kọ́rọ́ wọ̀nyìí.
Ìpologo kọ́kọ́rọ́ ogunlọ́gọ̀ máa ń lò àwọn ètòlẹ́sẹ̀sẹ̀ alákojọpọ̀ LDAP (Lghtweight Directory Access protocol : Ìfẹ́nukò ìmúlò àkójọpọ̀ ìsọfúnni fífúyẹ́) nínú àfẹ́nukò RFC 2251.
Àwọn ìjẹ́rìísí àfagilé máa wà nínú àkójọpọ̀ kan tí a ń pè ni CRL (Certificat Revocation List : àtòkọ ìfagilé ìwé ìjẹ́rìísí).
Àwọn àkójọpọ̀ ìsọfúnni tí ìfọwọ́síwé wà lórí ìgúnrege ètò X.509v2. ìgúnrege yìí lè mú kí wọ́n ṣàtẹ́jáde wọn lórí àwọn ètò LDAP bíi Netscape Directory Server d'iPlanet. Àgbékalẹ̀ PKI jẹ́ iṣẹ́ àkànṣe tí iṣẹ́ jẹ́ %10. %, 90 tún kù fún ètò oríṣiríṣi ní ilé̩ṣẹ́ apàṣẹ́ ìwé ìjẹ́rìísí.



6 Ìdári ìmúlò àwọn àsopọ̀ kọ́ńpútà agbègbè

Ìfẹ́nukò IEEE 802.1 X ni kó fún àwọn olùmúlò ni àṣẹ láti lò àwọn àsopọ̀ ẹ̀rọ kọ́ńpútà lẹ́yìn ìdámọ̀ (àsopọ̀ lè jẹ́ àìlówáyà tàbí olókun).
Àwọn ẹ̀ka ẹ̀rọ tí a máa ń lò fún ètò yìí ni : ẹ̀rọ tí a fẹ́ fún láṣẹ, àwọn ojú ìwọ́lé àsọpọ̀ (onípàpodà (switch), àlànà (Router) ...etc) àti apèsè ìfàṣẹsí. Nígbà tí ìfàṣẹ́sí kò bá ti wáyé ìmúlò àsopọ̀ kò lè ṣeé ṣe , àfi pàsipààrọ̀ láàrin apèsè àti àwọn ẹ̀rọ mì ín.

Nínu àsopọ̀ olókun, ìbásọ̀rọ̀ láàrin àwọn ẹ̀ka àtì ojú àkànpọ̀ ìgbọ́rọ̀wọlé máa ń lò ìfẹ́nukò EAP.
EAP (Extensible Authentification Protocol : Àfikún ìfẹ́nukò ìfàṣẹsí), ìfàṣẹsí ètò máa wáyé pẹ̀lú (EAP over LAN : EAP lórí àsopọ̀ agbègbè). Àmọ̀ ojú ìwọlé àti apèsè máa sọ̀rọ̀ pẹ̀lú EAP over Radius (Remote Authentification Dial-In User Service : Ìpèsè ìfàṣẹsí olùmúlò òkèrè).
Àwọn ìpele ìṣiṣẹ́ EAP jẹ́ mẹ́rin : ìbéèrè fún, èsì, àṣeyọrísírere, àìyégé.
Ìfẹ́nukò 802.1 X kò dúró sórí àlàkalẹ̀ ìfàṣẹsí ọ̀kan ṣoṣo, àmọ̀ sórí oríṣiríṣi ọ̀nà ìfàṣẹsí tó jẹ́mọ ìfẹ́nukò EAP , àwọn ni wọ̀nyìí :

EAP–MD5 Kò sí ìfàsẹsí àpapọ̀, àmọ̀ ìfàsẹsí máa dúró sórí ọ̀rọ̀ aṣínà.

- LEAP Ìfẹ́nukò cisco tó dúró sórí ìfàṣẹsí irú ìbéèrè / èsì tó kúrò ní MS-CHAP ti Microsoft tó jẹ́ ìdámọ̀ / ọ̀rọ̀ aṣínà.
- **EAP-TLS** (Transport Layer Security : Ìpele ìṣípòpadà ààbò) : Ìdámọ̀ láàrin oṣojú àti apèsè ìjẹ́rìísí.
- **EAP-TTLS** (Tunneled Transport Layer Security) : Ìdámọ̀ láàrin apèsè àti aṣojú, tó dúró sórí ìwé ìjẹ́rìísí lọ́dọ̀ apèsè pẹ̀lú ìdámọ̀ / ọ̀rọ̀ aṣínà, lẹ́yìn náà ọ̀nà-abẹ́lẹ̀ TLS máa wáyé, kí aṣojú tó lè fi iṣẹ̀ẹ̀jé ìdámọ̀ pẹ̀lú àwọn ohun oníméjì (ìdámọ̀ / ọ̀rọ̀ aṣínà)
- **EAP-FAST** (Flexible Authentification Via Secur Tuneling) Iléṣẹ́ Cisco ló gbé e jáde ní ọdun 2004, ti ń lò kọ́kọ́rọ́ ìpàrokò alọ́poméjì làárin apèsè àti aṣojú fi ṣèdásílẹ̀ ọ̀nà-abẹ́lẹ̀ TLS nígbà tí àwọn méjèjì ń ṣé ìdámọ̀ aṣojú. Lẹ́yìn ìgbà tí ìdámọ̀ bá ṣàṣeyọri pẹ̀lú irú ẹ̀rọ tó wà lójú ìwọ̀lé, a lè ṣé ìdáàbòbò ìwọlé bíi VLAN(àfinuwò àsopọ̀ agbègbè).

7 Ìṣàrìdájú ìdári wíwọlé òkèrè

Wíwolé àsopọ̀ iléṣẹ́ kan máa béèrè fún ìdákoja àsopọ̀ gbogboogbo**,** àwọn àsopọ̀ máa ń fún wa ni àǹfààní láti ṣàsopọ̀ àwọn kọ̀ńpútà tí wọ́n jìnnà sí ara wọn tí owó ẹ kò sì pọ̀ jù. Àwọn àsopọ̀ wọ̀nyìí lè jẹ́ àsopọ̀ fóònù tàbí íntánẹ̀ẹ̀tì, tàbí xDSL, Numeris tàbí alásopọ̀ àwọn iléṣẹ́ ẹ̀rọ ìbáraẹnisọ̀rọ̀.
Àwọn alásopọ̀ tí a ń pe ni ìsokọ́ra títì ni àwọn ti ń lò ìfẹ́nukò X.25, TCP/IP tí wọ́n sì sọmọ́, àsọpọ̀ gbogbogbo. Ó ti di dandan ká dáàbò bó àwọn kọ̀ńpútà alégbéka àwọn olùmúlò tó wà ní àsopọ̀ fún wíwọlé wọn tàárà láti òkèrè, pẹ̀lú àkóràn (virus) tó lè mú ki wọn jí àwọn ọ̀rọ̀, pẹ̀lú ọ̀nà ìdámọ̀ tí a ò rò.
A máa dáàbòbò àwọn kọ̀ńpútà pẹ̀lú ògiri-iná (firewall) pẹ̀lú àwọn àlàkalẹ̀ tó múnádóko àti àwọn ètò tí ń dá àwọn àkóràn dúró tí a ń ṣàmúdójúwọ̀n nígbà gbogbo. Gbogbo àwọn ohun èlò wọ̀nyìí láti lè wà ní abẹ́ ìṣàkóso alákóso kan kí àṣìṣe máa báà wà fún àgbékalẹ̀ ètò olùmúlò kan. Nígbà tí a bá fẹ́ yàn ọ̀nà-abẹ́lẹ̀ tí a ní lò, ó yẹ kí a mú èyí tí kò níí mú ìṣòro dáni. A lè yàn ọ̀nà-abẹ́lẹ̀ tí ìpele 3 nítorí a ò nímọ̀ àwọn ohun èlò àsopọ̀ ìsokọ́ra iléṣẹ́ wa.

7.1 Àwọn àfidámọ̀ àwọn ìfẹ́nukò wíwọlé òkèrè L2TP

Ọ̀nà ìṣiṣẹ́	aṣojú apèsè, ọ̀nà-abẹ́lẹ̀
Ìmúlò	wíwọlé òkèrè gba ọ̀nà-abẹ́lẹ̀
Ìfẹ́nukò ìṣípòpadà	IP, IPX, NetBEUI, ...etc
Ìpèsè ọ̀nà-abẹ́lẹ̀	ojúàmì-sí-ojúàmì
Ìpele OSI	2 (ìsúnkí sínú IP)
Ìpín ọ̀nà-abẹ́lẹ̀	bẹ́ẹ̀ ni
ìdámọ̀ olùmúlò	PAP, CHAP, EAP, SPAP
Ìdámọ́ èdìdì	Ìdámọ̀ ọ̀nà-abẹ́lẹ̀ lè wáyé
Ìpàrokò èdìdì	bẹ́ẹ̀ ni gbọ́nà ọ̀nà-abẹ́lẹ̀ IPsec
Àsomọ́ òpópónà aládáṣe	bẹ́ẹ̀ ni (PPP, NCP)
Àkósó àwọn kọ́kọ́rọ́	bẹ́ẹ̀ kọ́
Ìdójúkọ àtàkò	bẹ́ẹ̀ kọ́

7.2 Àwọn àfidámọ̀ àwọn ìfẹ́nukò wíwọlé òkèrè PPTP

Ọ̀nà ìṣiṣẹ́	aṣojú apèsè, ọ̀nà-abẹ́lẹ̀
Ìmúlò	wíwọlé òkèrè gbọ̀nà ọ̀nà-abẹ́lẹ̀
Ìfẹ́nukò Ìṣípòpadà	IP, IPX, NetBEUI, ...etc
Ìpele OSI	2 (ìsúnkí sínú IP)
Ìpèsè ọ̀nà-abẹ́lẹ̀	ojúàmì-sí-ojúàmì
Ìpín ọ̀nà-abẹ́lẹ̀	bẹ́ẹ̀ ni
ìdámọ̀ olùmúlò	PAP, CHAP, EAP, SPAP
Ìdámọ́ èdìdì	Ìdámọ̀ ọ̀nà-abẹ́lẹ̀ lè wáyé
Ìpàrokò èdìdì	bẹ́ẹ̀ ni gbọ́nà ìpele MPPE ti Microsoft
Àsomọ́ òpópónà aládáṣe	bẹ́ẹ̀ ni (PPP, NCP)
Àkósó àwọn kọkọrọ	bẹ́ẹ̀ kọ́
Ìdójúkọ àtàkò	bẹ́ẹ̀ kọ́

7.3 Àwọn àfidámọ̀ àwọn ìfẹ́nukò wíwọlé òkèrè IPsec

Ọ̀nà ìṣiṣẹ́	aṣojú-apèsè, ọ̀nà-abẹ́lẹ̀
Ìmúlò	wíwọlé òkèrè gbọ̀nà ọ̀nà-abẹ́lẹ̀
Ìfẹ́nukò ìṣípòpadà	IP, IPX, NetBEUI, ...etc
Ìpele OSI	3 (ìsúnkí sínú IP)
Ìpèsè ọ̀nà-abẹ́lẹ̀	ojú-àmì púpọ̀
Ìpín ọ̀nà-abẹ́lẹ̀	bẹ́ẹ̀ ni

ìdámọ̀ aṣojú	bẹ́ẹ̀ kọ́
Ìdámọ̀ èdìdì	bẹ́ẹ̀ ni, pẹ̀lú àkọsórí AH
Ìpàrokò èdìdì	bẹ́ẹ̀ ni pẹ̀lú àkọsórí ESP
Àsomọ́ òpópónà aládáṣe	Látórí ìṣàgbékalẹ̀
Àkósó àwọn kọkọrọ	IKE, SKIP
Ìdójúkọ àtàkò	bẹ́ẹ̀ ni

8 PPP (Point-to-Point Protocol : ojúàmì-sí-ojúàmì Ifẹ́nukò)

8.1 Ọ̀rọ̀ ìṣáájú

Àwọn ìfẹ́nukò tí a máa sábà lò fún wíwọlé àti òkèrè ni àwọn ti ojúàmì-sí-ojúàmì tàbí ti ọ̀nà-abẹ́lẹ̀.
Àwọn ìfẹ́nukò wọ̀nyìí kájú iṣẹ́ yìí láti gbé àwọn ìgbì sáà gbánu àwọn ìsokọ́ra kọ̀ńpútà pẹ̀lú ìṣàkósó ọ̀pọ̀ ìfẹ́nukò tó yàtọ̀ sí ara wọn bíi (IP, IPX, NetBEUI) lẹ́ẹ̀kan náà.
Ìfẹ́nukò PPP lè ṣèsúnkì àwọn ìfẹ́nukò wọ̀nyìí.
Nínú àsomọ́ àtòkèrè, ìfẹ́nukò láàrin kọ̀ńpútà alágbéká tó ní módẹ́mù pẹ̀lú àsopọ̀ kọ̀ńpútà máa ń jẹ́ ìfẹ́nukò PPP oní ìsúnkì èdìdì, ó tún ní àwọn ìfẹ́nukò abẹ́nu ti ìdárí àti àsopọ̀ LCP (Link Control Protocol : ìfẹ́nukò ìdárí àsopọ̀) àti ìdárí àsokọ́ra NCP (Network Control Protocol: ìfẹ́nukò ìdárí ìsokọ́ra) ìdári àsokọ́ra NCP tún ní àwọn ìfẹ́nukò abẹ́nu:

CHAP (Challenge Handshake Authentification Protocol : Ìdójúkọ ọwọ́ bíbọwọ́ Ìfàṣẹsí Ìfẹnukò)

EAP (Extensible Authentification Protocol : Àfíkun ìfàṣẹsí ìfẹ́nukò)

8.2 Àwọn Ìfàṣẹsí ìfẹnukò PPP

Àwọn àlàkalẹ̀ ìfàṣẹsí pọ̀ fún ìfẹ́nukò PPP, àwọn ìfàṣẹsí wọ̀nyìí bẹ̀rẹ̀ láti ọ̀rọ̀ aṣínà dé ìfàṣẹsí pẹ̀lú kọ́kọ́rọ́ :

PAP (Password Authentication Protocol : Ìfẹ́nukò Ifàṣẹsí Ọ̀rọ̀ aṣínà) jẹ́ ìfẹnukò tí ń lò ọ̀rọ̀ aṣínà pẹ́lù àyọkà pọ́nńbélé, ìfẹ́nukò yìí kò níí agbára.

MS-CHAP jẹ́ àlàkalẹ̀ ìdámọ̀ tó dúró lórí àbáṣepọ̀ pẹ̀lú ìpàrokò ní ìdárí kan ọ̀rọ̀ aṣínà. Àwọn ìpele àlàkalẹ̀ náà ni wọ̀nyìí :
1) Aṣojú máa béèrè fún àṣopọ̀ pẹ̀lú apèsè ìfàṣẹsí wíwọlé òkèrè.

2) Apèsè wíwọlé òkèrè máa fi ìbéèrè ránṣẹ́ sí aṣojú fún ìdámọ̀, tó jẹ́ òǹkàye sáà àti àtòtẹ̀lé ìró ìbéèrè láìnítúmọ̀.

3) Aṣojú máa fèsì ránṣẹ́ pẹ̀lú orúkọ olùmúlò, ìpàrokò àsopọ̀ ìró tó gbà lọ́nà ìdári kan àsopọ̀ àtì ọ̀rọ̀ aṣínà olùmúlò.

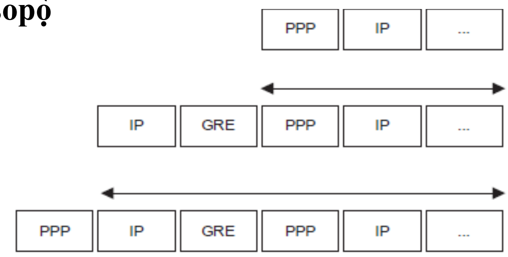
4) Apèsè ìfàṣẹsí máa ṣàyẹ̀wò èsì aṣojú pẹ̀lú ìpàrokò kannáà ní ìdári kan, nígbà tó ti mọ̀ ọ̀rọ̀ aṣínà olùmúlò tó wà nínú àkójọpọ̀ ìsọfúnni. Yóò fèsì ránṣẹ́ tí àṣèyọri rere bá wáyé tàbí ti àkùnà pẹ̀lú èsì ìfàṣẹsí tó jẹ́ àsopọ̀ ìró tó ti firánṣẹ́.

5) aṣojú máa ṣàyẹ̀wò ésì ìdámọ̀ tó bá dọ́gba, yóò wá lò àsopọ̀. Tí ìbéèrè bá jẹ́ àkùnà, yóò dá àsopọ̀ dúró. Microsoft ló ṣàgbékalẹ̀ MS-CHAP tó sì wá láti ìfẹ́nukò CHAP pélú ọ̀rọ̀ aṣínà tí a pàrokò lọ́nà ìdárí kan.
Àwọn àkójọpọ̀ ìsọfúnni aṣefàṣẹsí ò níí ọ̀rọ̀ aṣínà ní pọ́ńbélé. Láì mọ́ fẹ́ ṣàgbékalẹ̀ àwọn ìfẹ́nukò mì-ín EITF pinnú láti ṣe àwọn òfin tí kò somọ́ ìfẹ́nukò kan.

Ìfẹ́nukò EAP (Extensible Authentification Protocol: ìfẹ́nukò ìámọ̀ àfikún)) gbà àwọn àlànà tó sì fún wa ni àǹfààní láti ṣe ìṣípòpadà ìsọfúnni ìfàṣẹsí láàrin aṣojú àti apèsè. A lè pààrọ̀ àlànà ìfàṣẹsí láì pààrọ̀ ìfẹ́nukò EAP.
EAP jẹ́ ìfẹ́nukò ìsúnkì nìkan tí a máa sábà lò nínú agbègbè PPP àti IEEE 802.11. Ìpele mẹ́rin ló ní (ìbéèrè, èsì, àṣeyọrirere, ìkùnà). Àmọ́ ọ̀pọ̀lọ́pọ̀ àlànà ìdámọ̀ ló wà : MD5-Challenge, OTP (One Time Password)....
A ṣàgbékalẹ̀ ìfẹnukò EAP fi tẹ́ àwọn olùmúlò lọ́rùn tí wọ́n béèrè fún àlànà ìfàṣẹsí òkèrè tí a sì lò àwọn ẹ̀rọ ìdáàbòbò tí kò lò ọ̀rọ̀ aṣínà. Ìfẹ́nukò yìí fún wa ni àǹfààní láti lò oríṣiríṣi àlàkalẹ̀ ìfàṣẹsí :

Owó àmì, ọ̀rọ̀ aṣínà ọlọ́kan, ìdámọ̀ pẹ̀lú kọkọrọ káríayé, àwọn káàdì ẹ̀run. Àa máa lò apèsè fi ṣàgbékalẹ̀ àwọn ètò ìdámọ̀, apèsè lè máa fi àwọn ohun ìdámọ̀ ránṣẹ́.

Ìsunkì àwọn alásopọ̀ PPP sínú GRE



PPP

PPTP lórí IP

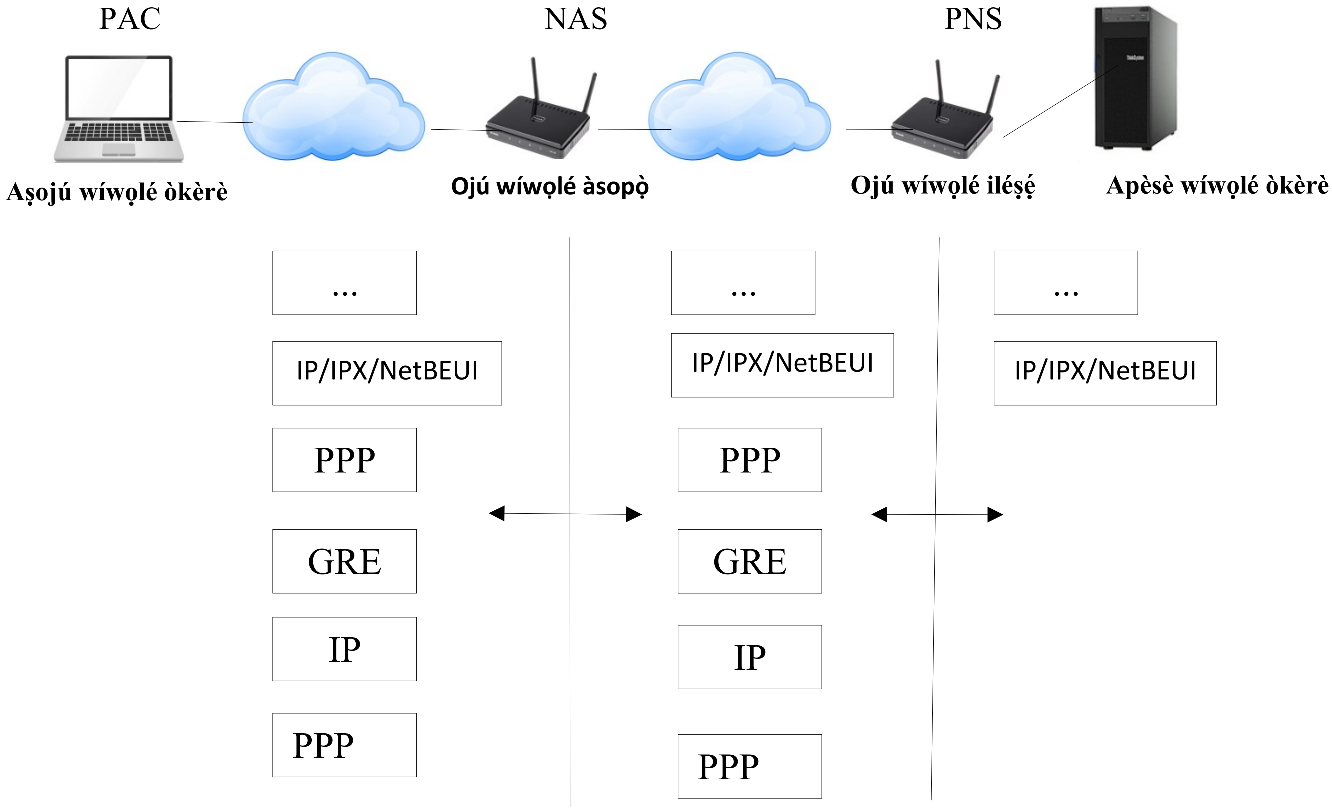
PPTP lórí ìwọlé òkèrè Àti IP

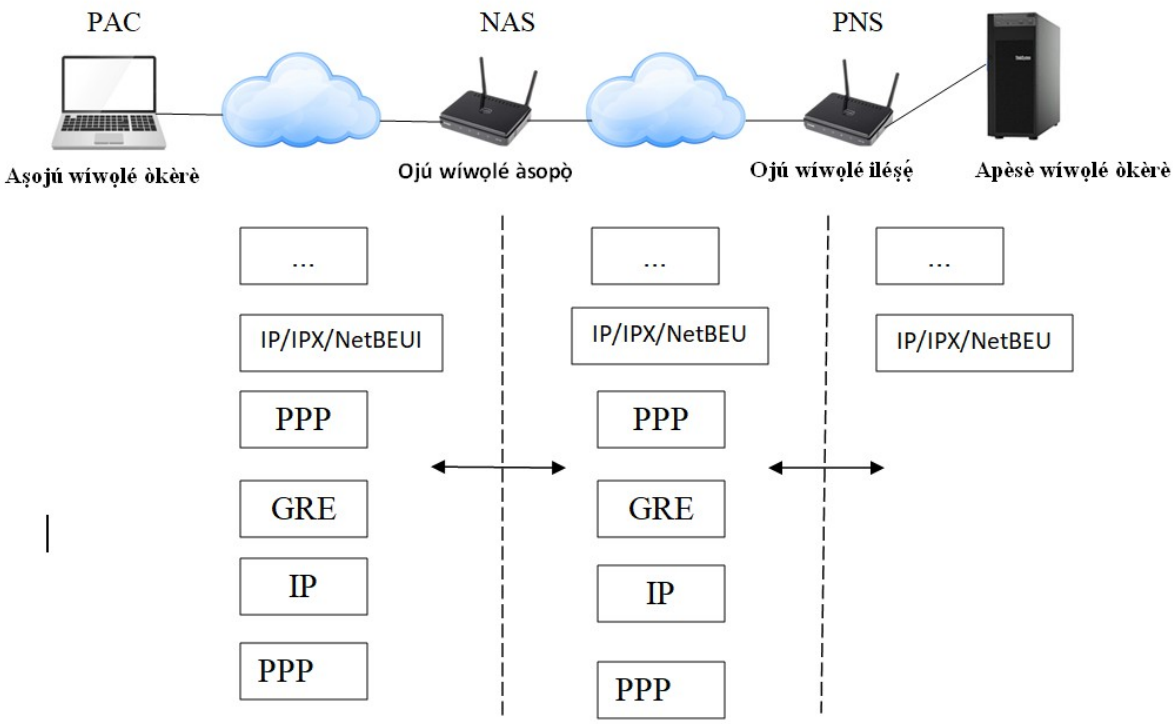
9 PPTP (Point-to-Point Tunneling Protocol : ojúàmì-sí-ojúàmì ìfẹ́nukò ọ̀nà abẹ́lẹ̀)

Ìfẹ́nukò PPTP máa fún wa ni àǹfààní láti ṣègbékalẹ̀ àsopọ̀ agbègbè àfinumọ̀. Microsoft ló gbé e kalẹ̀ pẹ̀lú Ascend àti 3 com. PPTP máa ń ṣé ìsúnkì pẹ̀lú ọ̀nà abẹ́lẹ̀, àwọn ìfẹnukò IP, IPX àti NetBEUI, tí àwọn náà wà ní ìsúnkì nínú àwọn èdìdì PPP, nítorí èyí ni wọ́n fi lò ìfẹ́nukò GRE (Generic Routing Encapsulation: àfirọpò ìsúnkì alànà)

MMPE (Microsoft Point-to-Point Encryption : ìpàrokò ojúàmì-sí-ojúàmì Microsoft) máa ń pàrokò àwọn ìsọfúnni àwọn àsopọ̀ kọ̀ńpútà wíwọlé òkèrè tàbí àsopọ̀ VPN PPTP. Àwọn alànà ìpàkorò MPPE máa lò kọ́kọ́rọ́ bíìtì 40 dé 128. Ìpàrokò RC4 ni a máa lò fi pàrokò.
MPPE máa ń dáàbò bó àwọn ìsọfúnni láàrin àṣopọ̀ aṣojú òkèrè (àsopọ̀ PPTP) pẹ̀lú apèsè, àwọn alànà ti PPTP jógun, àwọn alànà ìdámọ̀ PPP.
Fi ṣàgbékalẹ̀ sáà PPTP, kọ̀ńpútà aṣojú tàbí PAC (PPTP Access Concentrator), máa ṣàsopọ̀ láti òkèrè gbọ́nà ìfẹ́nukò PPP pẹ̀lú alákópọ wíwọlé NAS (Network Access Server) ti FA(ilésẹ́ olùpèsè ayélujára).
Ó tún máa ṣàgbékalẹ̀ sáà kèjì pẹ̀lú apèsè alásopọ̀ PPTP tàbí (PPTP Network Server) fi ṣé ìdúnà-dùrà àwọn ìfẹnúkò ti ọnà-abẹ́lẹ̀ PPTP, ó máa béèrè ìfàṣẹsí olùmúlò fi fàṣẹ̀ sí sáà wíwọlé, tí a sì máa lò àwọn alànà ti a jógun lọ́dọ̀ PPP.
Ọ̀nà abẹ́lẹ̀ tí yóò gbékalẹ̀ sórí alásopọ̀ IP jẹ́ ìsúnkì ìpele 3 pẹ̀lú ìfẹnukò IP/GRE àwọn èdìdì PPP.PPTP máa tún lò àsopọ̀ ìdári nígbà kannáà láàrin PAC-PNS gbọ̀nà sáà TCP lórí ojú ìkànpọ̀ tí òǹkàye rẹ̀ jẹ́ 1723 láti máa ṣèfiránsẹ̀ àwọn ìsọfúnni ìdárí àti ìṣàkósó àwọn ìpè PPTP àti ọ̀nà-abẹ́lẹ̀ láàrin PAC-PNS fún ìṣípòpadà àwọn èdìdì PPP ti a súnkì pẹ̀lú GRE.

Ìpàroko ìsọfunni Ipsec VPN Ipsec VPN





10) L2TP (Layer 2 Tunneling Protocol : Ìpele 2 ọ̀nà-abẹ́lẹ̀ ìfẹ́nukò)
L2TP jẹ́ ìfẹ́nukò ọ̀nà-abẹ́lẹ̀ tó fẹ̀ẹ̀ jọ̀ ìfẹnukò PPTP tó sì ní ìdápọ̀mọ́ra àwọn PPTP àti L2F.
L2TP jẹ́ ìsúnkì pẹ̀lú ọ̀nà-abẹ́lẹ̀ àwọn ìfẹnukò IP, IPX, NETBEUI tí àwọn náà wà ní ìsúnkì PPP. Ó máa ń lò àwọn èdìdì IP/UDP lórí àwọn àsopọ̀ IP fún ìṣípòpadà fún àwọn ọ̀nà-abẹ́lẹ̀ L2TP.
L2TP kìí lò MPPE fi pàrokò àwọn èdìdì PPP, àmọ́ máa ń lò ìdáàbòbò IPsec ìsúnkì àwọn èdìdì L2TP sínú IPsec.
Àwọn alànà ìfàṣẹsí ti L2TP máa ń jógun àwọn alànà ìfàṣẹsí ti ìfẹnukò PPP. Pẹ̀lú alákójọpọ̀ wíwọlé L2TP, tàbí LAC (L2TP Access Network Server : L2TP Wíwọlé Àsopọ̀ Apèsè), ti FAI (OWI Onípèsè Wíwọlé Íntánẹ́ẹ̀tì) Eléyìí máa ṣàgbékalẹ̀ ọ̀nà-abẹ́lẹ̀ àsopọ̀ pẹ̀lú apèsè alásopọ̀ L2TP tàbí (L2TP Apèsè Àsopọ̀) ti a máa ṣe pẹ̀lú ẹ̀rọ alànà. A tún lè ṣé ìṣe LAC pẹ̀lú ẹ̀rọ ìṣe aṣojú. A máa béèrè ìfàṣẹsí sáà ìwọlé níbi ti a jógun alànà ìfàṣẹsí láti ọ̀dọ PPP.
Ọ̀nà–abẹ́lẹ̀ ìgbékalẹ̀ lórí alásopọ̀ jẹ́ ìsúnkì ìpele kẹ́ẹ̀ta 3 pẹ̀lú ìfẹnukò IP/UDP àwọn èdìdì PPP ni L2TP máa lò nígbà kannáà, ọ̀nà-abẹ́lẹ̀ láàrin LAC-PNS, àwọn iṣẹ́ẹ̀jẹ́ sáà pẹ̀lú àwọn èdìdì PPP tá súnkì sínú L2TP tó sì dúró sórí UDP.
Nígbà tí aṣojú ṣàkósó ìṣe L2TP, oní láti ṣàkósó sáà méjì PPP : ọ̀kan pẹ̀lú ojú Wíwọlé alásopọ̀ àti èkèjì pẹ̀lú ojú wíwọlé.

11 SSH (Secure Shell)

SSH máa fún wa ni àǹfàání láti dárí àwọn ìgbì TCP ni ọ̀nà-abẹ́lẹ̀ nínú sáà SSH. Ìfẹnukò PPP, tí a máa ń lò fún àsopọ̀ àwọn kọ̀ńpútà alásopọ̀ ní àti òkèrè tó sì wà ni ìpele kéjì ni máa ń fún wà láǹfàání láti ṣàkójọ ọ̀nà-abẹ́lẹ̀ láàrin kọ̀ńpútà méjì tó wà ni àsopọ̀, ó ṣeé ṣe kí a ṣàkójọ onà-abẹ́lẹ̀ IP pẹ̀lú SSH, pẹ́lú ìsúnkì IP sínú èdìdì PPP kí a sì dárí àwọn èdìdì PPP sínú sáà SSH tí a ti ṣẹ̀dá. Èbúté kèjì máa ṣé iṣẹ́ àlòdì fí rí àwọn èdìdì IP orísun. Àṣàyàn ti ń fún wa ni àǹfàání láti ṣàfirọ́pò àwọn èdìdì ní ìpele IP láti lè wà ní ìṣẹ́.

<table>
<tr><td>SSH User
Authentication Protocol
Authenticates the client-side
User to the server

Ìfàṣẹ́sí ní ẹgbẹ̀ aṣojú
Olùmúlò fún apèsè</td><td>SSH
Connection Protocol
Multiplexes the encrypted
tunnel into several logical
channels

Pínpín ìpárokò ọ̀nà-
abẹ́lẹ̀ sí ọ̀pọ̀ òpópónà</td></tr>
<tr><td colspan="2">SSH Transport Layer Protocol
ìpele àfẹ́nukò Ìṣípòpadà</td></tr>
<tr><td colspan="2">TCP</td></tr>
<tr><td colspan="2">IP</td></tr>
</table>

PPP Ìfẹ́nukò ojú-àmì sí ojú-àmì

Itọkasí	Àdírẹ̀ẹ̀sì	Ìṣàkóso	Ìfẹ́nukò	Ìsọfúnni	FCS
1 báìtì	1 báìtì	1 báìtì	2 báìtì	1 báìtì	2 tàbí 4 báìtì

Ìtọ́kasí : bíìtì ẹyọ kan**,** máa tọ́ka sí ìbẹ̀rẹ̀ tàbí òpin férèmù (ìsàlẹ̀ alásopọ̀), àtòtẹ̀lé bíìtì 01111110.

Àdírẹ̀ẹ̀sì : bíìtì ẹyọ kan, inú ààyè yìí a ní àdírẹ̀ẹ̀sì ìtànkalẹ̀, PPP, kìí fún àdírẹ̀ẹ̀sì kọ̀ńpútà kan.

Ìṣàkóso : Àtòtẹ̀lé àlákóméjì 00000011, yóò béèrè fún ìfiránṣẹ́ àwọn ìsọfúnni òlùmúlò nínú férèmù tí wọ́n ò tò tẹ̀ló ara wọn.

Ìfẹ́nukò : báìtì méjì, yóò tọ́ka sí ìfẹ́nukò tí PPP súnkí sí ààyè àwọn ìsofúnni.

12 SSL (Secure Socket Layer : ìpele ààbò ìsopọ̀)
A máa lò SSL fi ṣàgbékalẹ̀ sáà láàrin ojúṣe àti apèsè oní ààbò ní ìpele sáà OSI. Ìfẹ́nukò PPP ni a máa ń lò fi ṣàgbékalẹ̀ àsopọ̀ òkèrè pẹ̀lú alásopọ̀ tó sì máa wà lórí ìpele 2 OSI. Ó máa fún wa ni àǹfààní bíi tàtẹ́yìn wá láti ṣàkójọ ọ̀nà-abẹ́lẹ̀ láàrin àgbékalẹ̀ méjì tá sopọ̀. Fi ṣàkójọ ọ̀nà abẹ́lẹ̀ pẹ̀lú SSL, a máa ṣé ìsúnkì ìgbì IP sínú èdìdì PPP ká sì dárí àwọn èdìdì PPP sínú SSL.

<table>
<tr><td>SSL Handshake Protocol
Ìfẹ́nukò bíbọwọ́</td><td>SSL Change Cipher Spec Protocol
Ìfẹ́nukò Aṣàtúnṣe àfidámọ̀ ìpàrokò</td><td>SSL Protocol</td><td>HTTP</td></tr>
<tr><td colspan="4">SSL Record Protocol</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

13 Àwọn ìfẹ́nukò ìmúlò wíwọlé òkèrè

Ìdámọ̀ ni ìgbésẹ̀ àkọ́kọ́ fi ṣàgbékalẹ̀ wíwọlé òkèrè, kí a tó wá rí àwọn ìpele ìfàṣẹsí àti ìṣàkọsílẹ̀ àwọn ìdúnádùrà.
Àwọn ìfẹ́nukò mélòó kan ni a ń lò ṣègbékalẹ̀ wọn bíi TACAS+,
RADIUS (Remote Authentification Dial-I User Server : apèsè ìfàṣẹsí àwọn olùmúlò òkèrè), Kerberos, ...etc.

Àwọn ìfẹ́nukò RADIUS àti TACAS+ ni àwọn ilé̩ṣé̩ ẹ̀rọ ìbáàranisọ̀rọ̀ ńlá ńlá ní lò wọn nítórí ìgbékalẹ̀ wọn rọ̀rùn. Kerberos ni a máa sàbá lò fún ìdámọ nínú àwọn àgbékalẹ̀ ìlò àwọn ìsọfúnni.
Ká tó máa ṣàlàyé àwọn ìfẹ́nukò, ó yẹ ká mọ̀ ìyàtọ̀ láàrin olùmúlò àti ojúṣe TACAS+ tàbí RADIUS, nítórí nígbà gbogbo, aṣojú TRACAS+ tàbí RADIUS kìí ṣiṣẹ́ lórí kọ̀ńpútà olùmúlò. Olùmúlò máa ṣàsopọ̀ láti òkèrè ní ojú ìwọlé ìsokọ́ra

pẹ̀lú ìfẹ́nukò PPP, aṣojú TACAS+ tàbí RADIUS máa ń ṣiṣẹ́ lójú ìwọlé fi gbé ìbéèrè lọ fún apèsè TRACAS+ tàbí RADIUS.

13.1 RADIUS

Iléṣẹ́ Livingston ló ṣàgbékalẹ̀ RADIUS tí àfẹ́nukò IETF (Internet Engineering Task Force : ẹlẹ́rọ agbára ìsẹ́ Ayélujárá) gbà á wọlé. Ó sì máa ń lò ìfẹ́nukò UDP pẹ̀lú ojú àsopọ̀ (port) 1645. Àmọ̀ orí ojú àsopọ̀ (port) 1812 láni láti ṣàtòpọ̀ rẹ̀. Àwọn iṣẹ́ méjì ní ń ṣé (ìfàṣẹsí, ìfúnláṣẹ) lápapọ̀ pẹ̀lú ẹkẹ́ẹ̀ta tó jẹ́ ìṣírò lọ́tọ̀ọ̀.pẹ̀lú ìṣàkósó àkọọ́lẹ̀ lọ́tọ̀ọ̀. Iṣẹ́ mí-ìn tí ìfẹnukò ni kó máa ṣàgbélọ ìfáṣẹsí dé ọ̀dọ àwọn apèsè mí-ìn tó lè jẹ́ RADIUS tàbí (AXENT, Secure ID) ...bẹ́ẹ̀, bẹ́ẹ̀ lọ, Èyí yóò fún wa ni àǹfààní láti lò apèsè ẹ̀yìn fi ṣàgbékalẹ̀ àwọn ohun èlò ìdánilójú mì-ín, nígbà ti apèsè àkọ́kọ́ máa ṣèfiránsẹ́ àwọn ohun tí wọ́n fàṣẹsí.

Bíi TRACACS+ RADIUS jogun àwọn àlàkalẹ̀ ifẹ́nukò ìfàṣẹsí PPP, àwọn pàṣipàárọ̀ dúró lórí ìbéèrè ojúṣe àti èsì láti ọ̀dọ apèsè.
Ìkójọpọ̀ ìsọfúnni tó wà lórí apèsè ìwọlé òkèrè tí RADIUS yóò ṣàkósó àwọn olùmúlò RADIUS pẹ̀lú àwọn àfidámọ̀ wọn. Ìgbésẹ̀ àkọ́kọ́ ni kí ìfàṣẹsí àti ìfunláṣẹ olùmúlò wáyé.
A máa ń jèrè iṣẹ́ẹ̀jẹ́ pàsipàárọ kan láàrin ojúṣe àti apèsè, èyí tó yàtọ̀ sí TRACAS+

14 Ìdarí wíwọlé òkèrè WI-FI

Àwọn wíwọlé àsopọ̀ aláìlówáyá, wáyé ni 1997 pẹ̀lú àfẹ́nukò IEEE 802.11. Èyí máa ń lò àwọn ìpele àsopọ̀ MAC àti àwọn ohun èlò aláridìmú ìbánisọ̀rọ̀ láàrin ìsokọ́ra aláìlówáyá pẹ̀lú ojú wíwọlé tàbí ẹ̀rọ ìsokọ́ra aláìlówáyà méjì (peer-to-peer : ọ̀kan náà sí ọ̀kan náà).
Àwọn ohun-èlò àsopọ̀ aláìlòwáyá ni wọ̀nyìí :

- Ojú wíwọlé : wà bíi ojú àkànpọ̀ láàrin àsopọ̀ aláìlókùn pẹ̀lú àsopọ̀ olókùn.
- Káàdì WI-FI tí a máa ń fi sínú agbékalẹ̀ tí a fẹ́ somọ́ àsopọ̀.
- SSID (Service Set Identifier : Ìpèsè (Ìpèsè ìtọ́kasí ẹ̀rọ)
  Ìdámọ̀ àsopọ̀ àìlòwáyá tá ṣàsopọ̀ rẹ̀ sórí ojú wíwọlé tàbí tí ojúṣe kọ́ ní aládáṣe. Ní ọ̀nà ààbò, àfẹ́nukò 802.11 ṣàlàyé.

4.1WEP (Wire Equivalent Privacy : ààbò ìdọ́gba àìlówáyà)

Ìfẹ́nukò 802.11 gbé àwọn ìlànà kalẹ̀ fún ìdáàbòbò pẹ̀lú ìpíye ìsọfúnni, Ó tún gbé àwọn ìlànà mì ín kalẹ̀ fún ìdárí wíwọlé pẹ̀lú ìfàṣẹsí kọ́ńpútà olùmúlò, ìfàṣẹsí tí

yóò lò kọ́kọ́rọ àṣírí tí a pín).
Àwọn ìkùnà àfẹ́nukò 802.11 ni. :

- Àwọn ohun ìpìlẹ̀ tí a lò fún ìpàrakò àwọn ìsọfúnni kéré jù, ó ṣeé ṣe kí a mọ̀ ọ.
- Kọ́kọ́rọ́ pàtàkì tí a lò fún ìpàrokò kére jù
- Kò sí àkóso aládàṣé àwọn kọ́kọ́rọ́
- Ìfẹ́nukò ìfàṣẹsí tí a lò kò níí agbára tó. Àyẹ̀wó pípé ìsọfúnni máa ń lò checksum , ìdí èyí àwọn ìwàdìí lọ́pọ̀lọ́pọ̀ wáyé nínú ìjọ (WI-FI alliance: àjọṣepọ̀ àìlókun)

  Láti dáàbòbò tó péye bó ìsokọ́raWI - FI àwọn ni wọ̀nyìí :

  1. WPA (WI – FI Protected Access : Ìdáàbòò Wíwọlé WI - FI) pẹ̀lú àwọn àlàkalẹ̀ wọ̀nyìí :
     - àlàkalẹ̀ dúnádùrà ti ìfàṣẹsí dúró sórí EAP tàbí

     PSK (Pre-shared key : Pàṣipàárọ kọ́kọ́rọ́ ìbẹ̀rẹ̀).
     - àlàkalẹ̀ àkóso àti pàṣipàárọ̀ pínpín àwọn kọ́kọ́rọ́

     TKIP (Temporal key Integrity Protocol : Ìfẹnukò kọkọrọ pípé ìgbà kan)
     - Àlàklẹ̀ pípé férèmù TKIP pẹ̀lú ìtòlẹ́sẹẹsẹ Michael
     - Ìbáramú ohun-èlò alárídìmú tó tí wà nílẹ̀, ìséyípadà àwọn ètòlẹsẹ̀ẹsẹ̀ nìkan ló lè ṣeé ṣe.
     - Ìbáramu pẹ̀lú kọ́kọ́rọ́ WEP
     - Ìfẹnukò túntún ìpàrokò àyẹ̀wó pípé

15 Àwọn àfidámọ̀ ti ìdáàbòbò WI–FI

WEP

Ìpàrokò	RC4
Gígun kọkọrọ	40 / 104 bíìtì
Ìṣàrídájú ìsọfúnni	CRC – 32
Ìṣàrídájú àkọsórí	bẹ́ẹ̀ kọ
Ìṣàyẹ̀wó àtàkò pẹ̀lú àtúngbá (rejeu)	bẹ́ẹ̀ kọ
Gígùn ìdárí ohun èlò ìbẹ̀rẹ̀	24 bíìtì

WPA

Ìpàrokò	RC4
Gígun kọkọrọ	128 bíìtì
Ìṣàrídájú ìsọfúnni	Michael
Ìṣàrídájú orí	Michael
Ìṣàyẹ̀wó àwọn kọ́kọ́rọ́	Ohun-èlò ìbẹ̀rẹ̀
Ìṣàkósó kọ́kọ́rọ́	802.1 X
Gígùn ohun èlò ìbẹ̀rẹ̀	48 bíìtì
Kọ́kọ́rọ́ lórí èdìdì	bẹ́ẹ̀ ni

802.11

Ìpàrokò	AES
Gígun kọkọrọ	128 bíìtì
Ìṣàrídájú ìsọfúnni	CBC-MAC
Ìṣàrídájú orí	CBC-MAC
Ìṣàyẹ̀wó àwọn kọkọrọ	Ohun-èlò ìbẹ̀rẹ̀
Ìṣàkósó kọkọrọ	802.1 X
Gígùn ohun èlò ìbẹ̀rẹ̀	48 bíìtì
Kọkọrọ lórí èdìdì	bẹ́ẹ̀ ni

16 Àwọn àfidámọ̀ àwọn ìfàṣẹsí EAP

EAP – MD5
Ìṣàtúnṣe àwọn ìfẹnukò CHAP ti PPP ni. olùmúlò yóò lò orúkọ / ọ̀rọ̀ aṣínà fi béèrè ìfàṣẹsí. Bó tilẹ̀ jẹ́ pé ọ̀rọ̀ aṣínà kan kò jáde síbìkan nígbà ìfàṣẹsí, èyí kò túmọ̀ sí pé ìfẹ́nukò yìí múnádókó, kìí lè dójúkọ àwọn àtàkò tí yóò lò ìwé àṣàjọ ọ̀rọ̀.

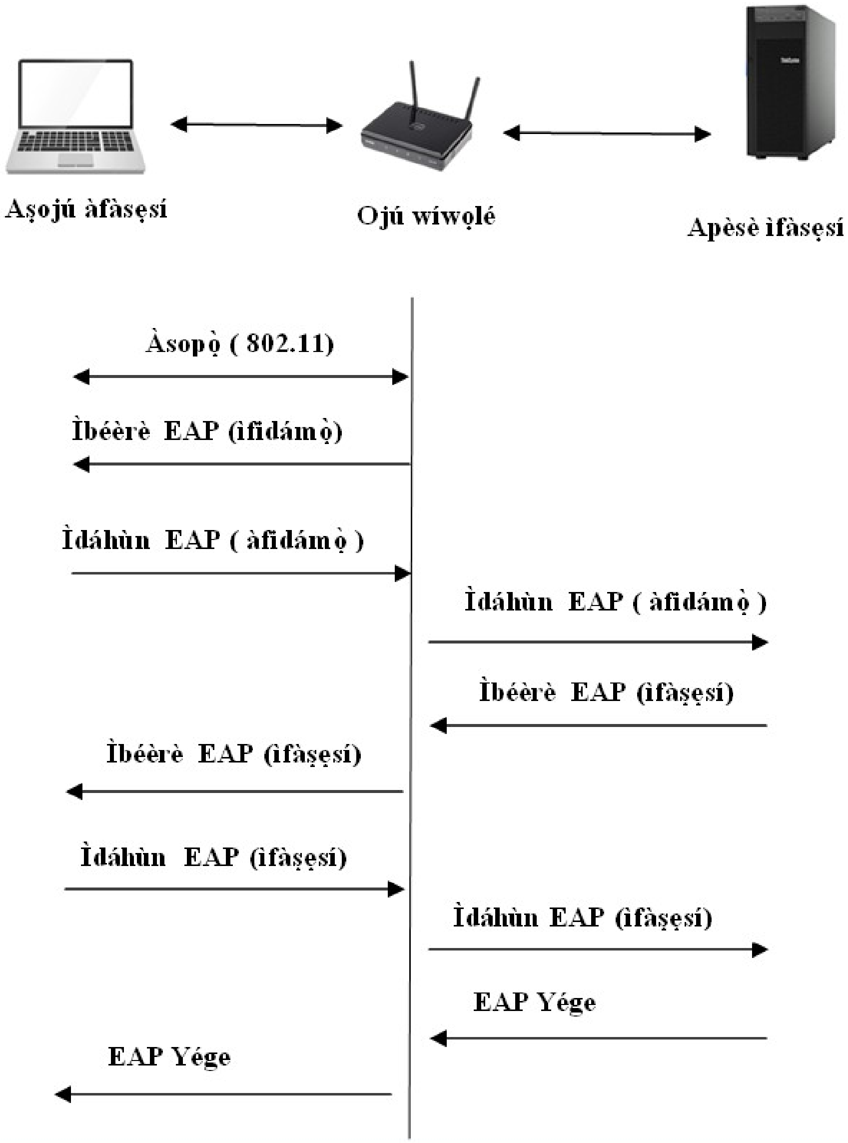
EAP – LEAP (Light Weight EAP : EAP Fúfuyẹ)
Àgbéjáde EAP-MD5 kìí lè dójúkọ àwọn àtàkò tí yóò lò ìwé àṣàjọ ọ̀rọ̀.

EAP – TLS (Transport Level Security : ìpele ìṣípòpadà ààbò)
aṣojú àti apèsè máa ṣàdámọ̀ láàrin ara wọn pẹ̀lú ìjẹ́rìísí X.509, ọ̀nà – abẹ́lẹ̀ TLS máa wáyé fún pàṣipàárọ̀ àwọn ìsọfúnni àṣírí.

EAP – TTLS (Ọ̀nà-abẹ́lẹ̀ ìpele ìṣípopadà ààbò)
Jẹ́ àfikún EAP – TTLS jẹ́ àfikún EAP-TLS tí ìwọlé àsopọ̀ TLS wáyé láàrin ojúṣe àti apèsè. Aṣojú lè ṣé ìdámọ̀ pẹ̀lú orúkọ / ọ̀rọ̀ aṣínà wíwọlé.

EAP – PEAP (Protected EAP : onídáàbòbò EAP)

EP–PEAP jẹ́ EP-TTLS pẹ̀lú ìṣí ọ̀nà-abẹ́lẹ̀ TLS láti fi dáàbòbò àwọn ohun èlò ìfàṣẹsí tí ojúṣe firánṣẹ́ sí apèsè.
Àwọn WPA àti 802.11 máa lò àwọn èlò EAP fi ní agbára fikún. Pẹ̀lú àwọn ìdámọ̀ wọ̀nyìí.
Pàṣipàárọ̀ máa wáyé láàrin ojú Wíwọlé aṣojú àti ìfaṣẹsí wíwọlé.
Bó tilẹ̀ jẹ́ pé àwọn ìsokọ́ra àìlówáyé dójúkọ wàhálà ìdáàbòbò púpọ̀, àmọ́ ti àwọ̀n òde oní ti ní àwọn ìdáàbòbò tó ṣe mú yàngàn.
àmọ́ kò yẹ kí a máa lò àsopọ̀ àìlówáyà nínú gbogbo ilésẹ̀, àwọn ohun ìdábòbò bíi Ògiri-iná lè má dá àwọn alátàkò dúró, nǹkan tí kò níí dáàbò bó ilésẹ̀ tí kò sì ni dára.
Àwọn àfikun ìsokọ́ran nínú àwọn ilésẹ̀ jẹ́ ká mọ̀ pé ó pọn dandan ká ṣàgbékalẹ̀ àwọn ohun èlò ìdáàbòbò bíi (IDS : àgbékalẹ̀ ìwoṣẹ́ ajálèlókùn).



17 IPsec

Àwọn ọ̀nà ìpàrokò tí a sọ̀rọ̀ wọn lẹ́yìn wá ni a ń lò nínú àwọn ìfẹnukò ààbò bíi IPsec, SSH, SSL, ...etc.

Láti dójúkọ àwọn ìkùnà IPV4 (Ìkùnà ìfàṣẹsí àwọn èdìdì IP, ìkùnà IP ...bẹ́ẹ̀, bẹ́ẹ̀ lọ). A gbé ìfẹ́nukò ààbò jáde, tí a pè ni IPsec (IP Security) tí àwọn IETF (Internet Engineering Task Force) fún ìṣe ìpàrokò àti ìfàṣẹsí.

àwòrán tó wà nísàlẹ̀ máa ṣàfihan ọ̀nà ìṣiṣẹ́ rẹ̀.

Ìfẹnukò yìí wà ní ìpele IP fi pèsè ààbò. Ó ṣeé ṣe kí a má lò IPsec, IPsec wáyé láti ìwádìí lórí ìfẹnukò tuntun IPv6 tí a ń pè IPNG (IP ìgbà tuntun); àwọn étò ìgbékalẹ̀ ti òdè oní gbogbo ní lò IPsec (Solaris, Windows, Cisco, ...etc).

Àwọn ààbò wọ̀nyìí ni yóò fún wa láǹfààní láti lè ṣàgbékalẹ̀ àwọn àsopọ̀ aládání aláfojúinúwò sórí íntánẹ̀ẹ̀tì (VPN).
IPsec máa tún fún wa ní àǹfààní láti ṣe ìdárí àwọn ìwọlé, pípé ìsọfúnni, ìfàṣẹsí orísun àwọn ìsọfúnni, ìdójúkọ àwọn àtàkò, àwọn èdìdì àtúngbá, àti ààbò.
IPsec máa ń ṣé ìsúnkì àwọn ìfẹnukò IP (TCP, UDP, ICMP, ..etc.) àwọn iṣẹ́ pàtàkì IPsec ni ìpàrokò àti ìfàṣẹsí.
ESP (Encapsulating Security Payload : Ìsúnkì ààbò isọfúnni pààpàá) máa fún wa ni àǹfààní láti pàrokò àti ìfàṣẹsí àwọn ìsọfúnni èdìdì IP.
AH (Authentification Header : àkọsórí ìfàṣẹsí) Ìfàṣẹsí sórí èdìdì IP (làìsí àwọn ààyè tí máa ń yípadà).
Àwọn ìpèsè méjèjì ni a lè papọ̀ fi ṣàkójọ èdìdì IP ti a pàrokò àti ti a fàṣẹsí. Àwọn ìpèsè méjèjì máa ń lò ìtòlẹ́sẹẹsẹ ìpàrokò fún ààbò.

17.1 Ìsopọ̀ ààbò

Ìgbékalẹ̀ sáà ààbò pẹ̀lú IPsec yóò fẹ́ àlàyé ìsopọ̀.
SA (Security Association : ìṣopọ̀ ààbò) fún àsopọ̀ alátagbà àti agbàsọfúnni.
Ọ̀nà ìdárí kan ló wà, tó sì ṣàlàyé àwọn ìpèsè ààbò tí àwọn AH tàbí ESP máa lò.
SA máa ń ṣàlàyé àwọn ààtò tó wúlò fún àwọn ìfẹnukò (ESP tàbí AH) àmọ́ kìí ṣe fún àwọn méjèjì lẹ́kannáà.

17.1.1 Ìṣipòpadà tó so pọ̀ mọ́ra :
Máa fún wa ni àǹfààní láti lò ìfẹnukò méjì fún ìwọ́ (frame) ìsọfúnni kọ̀ọ̀kan ìpári-sí-ìpári (àgbékalẹ̀ sí àgbékalẹ̀) ní ọ̀nà ìṣípòpadà (a ṣàgbépamọ ìwọ́ ìsọfúnni).
17.1.2 Àṣetúnṣe ọ̀nà-abẹ́lẹ̀ :
Ọ̀nà ìsopọ̀ yìí máa jẹ́ kí SA púpọ̀ ní ọ̀nà ọ̀nà-abẹ́lẹ̀ láàrin àwọn àgbékalẹ̀. Bíi àpẹrẹ (ìwọ́ ìsọfúnni IP orísun máa wà ni ìsúnkì pátápátá nínú ìwọ́ ìsọfúnni mì-ín).
Ó ṣeé ṣe kí a ṣèsúnkì ọ̀nà-abẹ́lẹ̀ kan sínú omìí.

17.2 Àsopọ̀ ààbò ní àwọn ẹ̀yà wọ̀nyìí :

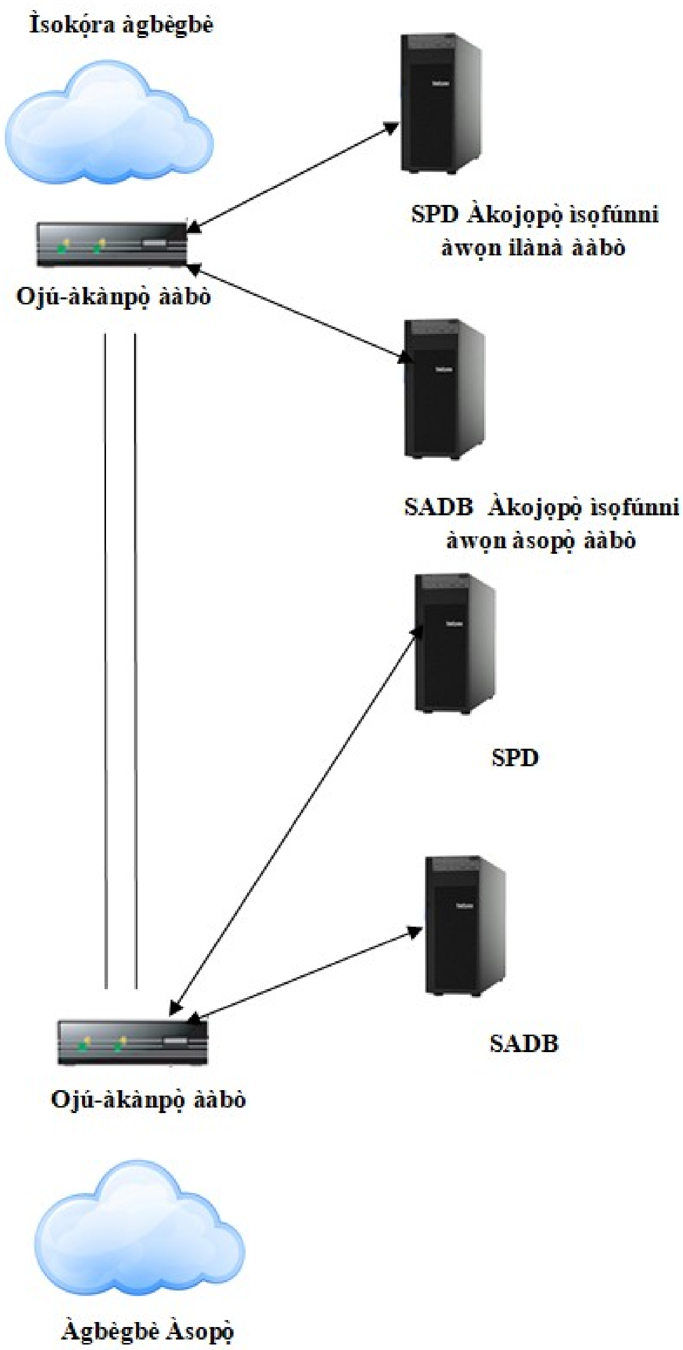
- Ìtọ́ka sí àwọn ààtò ààbò : òǹkàye kan tí a yàn lọ́nà rúdurùdu tó sì jẹ́ ti agbègbè nìkan, a yóò fi bọ àwọn ààyè AH àti ESP.
- Àdírẹ́ẹ̀sì èbúté : máa sàpèjúwé ibi òpin SA.
- Irúfẹ ìfẹ́nukò ààbò : AH tàbí ESP
- Òǹkàye ìtòlẹ́sẹẹsẹ̀ : Òǹkàye yìí ò níí jẹ́ kí a ní àwọn èdìdì alátúngbá àwọnÒǹkàye wọ̀nyìí máa wà nínú àwọn ààyè AH àti ESP.

- Àkúnwọ́sílẹ̀ òǹkàye ìtòlẹ́sẹẹsẹ : Ṣàpèjúwé nǹkan tí a máa ṣé tí òǹkàye yìí bá pọ̀jù. Àwọn òǹkàye wọ̀nyìí wà láàrin 232 – 1. Nígbà tí a bá ti lò gbogbo àwọn òǹkàye tán, a ní láti ṣé ìdúnádùrà SA mì-ín
- Fèrèsé àìlètúngbá : Nígbà tí ìfẹnukò IP kò lè jẹ́ kí a lè mọ̀ tí àwọn èdìdì bá máa tò tẹ̀lé ara wọn ; a máa ń lò fèrèsé ìsun fi ṣàtúntò ìfẹnukò IP. A ní láti yàn fèrèsé yìí lọ́nà tó yẹ pẹ̀lú àkíyèsí.
- Ààyè **AH** : Inú ààyè yìí, a á rí àwọn ààtò ìtòlẹ́sẹẹsẹ ìfàṣẹsí tí a lò pẹ̀lú àwọn kọ́kọ́rọ́ tó so mọ́.
- Ààyè **ESP** : Inú ààyè yìí ni a máa rí àwọn ààtò tó so mọ́ ìtòlẹ́sẹẹsẹ̀ ìpàrokò tí a lò pẹ̀lú àwọn kọ́kọ́rọ́ ìsomọ́ rẹ̀.
- Ìgbà àsopọ̀ ààbò : àkọ́kọ́ tó máa tó kí ìdúnádùrà àsopọ̀ mì ín máa wáyé.
- Irúfẹ́ ìfẹnukò : ìṣípòpadà , tàbí ọ̀nà-abẹ́lẹ̀
- Ọ̀nà MTU (Maximum Transmission Unit : Gíga jù ìwọpọ̀ Ìfiránṣẹ́) gígùn jù èdìdì kan.

Nígbà tí a bá ti ṣègbákalẹ̀ àsopọ̀ ààbò, gbogbo àwọn èdìdì IP tí yóò gbà sáà IPsec máa ní àsopọ̀ ààbò ọ̀kan tàbí mélòó pẹ́lú àdírẹ́ẹ̀sì IP èbútú. Èyí túmọ̀ sí pé a mọ́ gbogbo àwọn ìpèsè ààbò tó wà lórí èdìdì tí a lò kan tí ìsopọ̀ ààbò máa wáyé fún wọn pẹ̀lú àdírẹ́ẹ̀sì èbúté wọn ; a máa wá àwọn irúfẹ́ ààbò èdìdì kọ̀ọ̀kan. Gbogbo àwọn SA (Àsopọ̀ ààbò) ni ṣàkójọ wọn sínú àtòkọ àkojọ̀pọ̀ ìsọfúnni àwọn àsopọ̀ ààbò ti a ń pè ni SADB (Security Association Database : Ààbò àkopọ̀ àtòkọ àkójopọ̀ ìsọfúnni). Inú èyí ni a yóò rí àwọn ààtò gbogbo tó jẹ́mọ SA kọ̀ọ̀kan. A yóò ṣàyẹ̀wò rẹ̀ fi mọ́ bí a ṣe fẹ́ ṣàkóso èdìdì kọ̀ọ̀kan tí a gbà tàbí tí a fẹ́ fìránṣẹ́.
máa rí ìfẹ́nukò ISAKMP (ínternet Security Association and Key Management Protocol : ìfẹnukò ìṣàkóso Ààbò Íntẹ́ẹ̀nẹ́tì àsopọ̀ àti kọ́kọ́rọ́ ìṣàkósó) níwájú máa tọ́ka bíi ti ẹ̀yà kọ̀ọ̀kan ṣe ṣàsopọ̀ tí yóò sì ṣàlàyé bí tí àwọn ìṣipòpadà ìpele ṣe fún ààbò tó péye.
Ó máa fún wa àwòṣe àpapọ̀ tí ń lò àwọn ìfẹ́nukò bíi SKEME (Secure Key Exchang Mechanism : Ọ̀nà ìpàṣipàárọ̀ kọ́kọ́rọ́ ààbò) tàbí Oakley fi ṣàlàyé pàṣipàárọ̀ ìfàṣẹsí kọ́kọ́rọ́...bẹ́ẹ̀ bẹ́ẹ̀ lọ.

IK ìfẹ́nukò pàṣipàárọ̀ kọ́kọ́rọ́ IPsec dúró lórí àwọn ìfẹ́nukò ISAKMP, SKEME àti Oakley. Àlàkalẹ̀ ààbò IPsec dúró lórí àkójọpọ̀ ìsọfúnni SPD (Security Policy Database : àtòkọ àkójọpọ̀ ìsọfúnni àlàkalẹ̀ ààbò).
Inú àkójọpọ̀ yìí ni a máa rí àwọn àlàkalẹ̀ tí yóò jẹ́ kí a mọ̀ tí a bá pèsè ààbò fún èdìdì kan tàbí tí a bá máa yọ ọ́ kalẹ̀.
Inú àwòràn tó wà nísàlẹ̀ a yóò rí àwọn ohun èlò sáà IPsec. A tún lè ṣàsòpọ̀

ìdáàbòbò a máa rí níwájú bí a ṣe lè ṣàpapọ̀ sáà pẹ̀lú àwọn ìyàn ìṣípòpadà tàbí ọ̀nà-abẹ́lẹ̀.

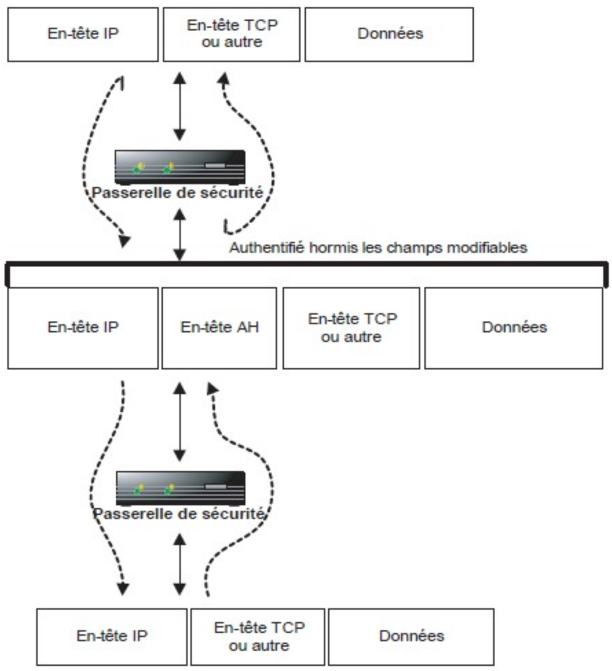


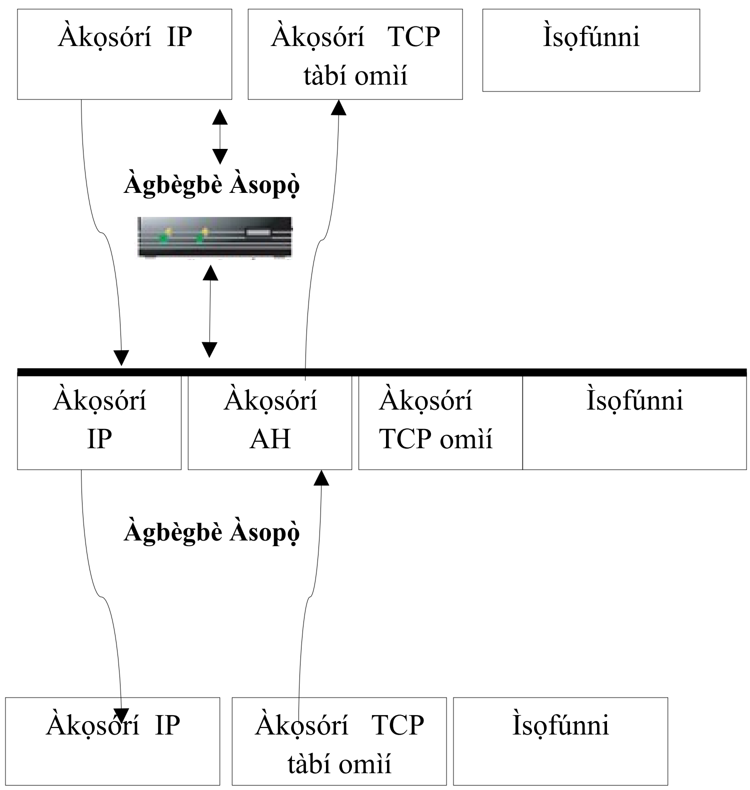
17.3 Ìsúnkì àwọn ìsọfúnni ààbò (ESP : Encapsulating Security Payload)

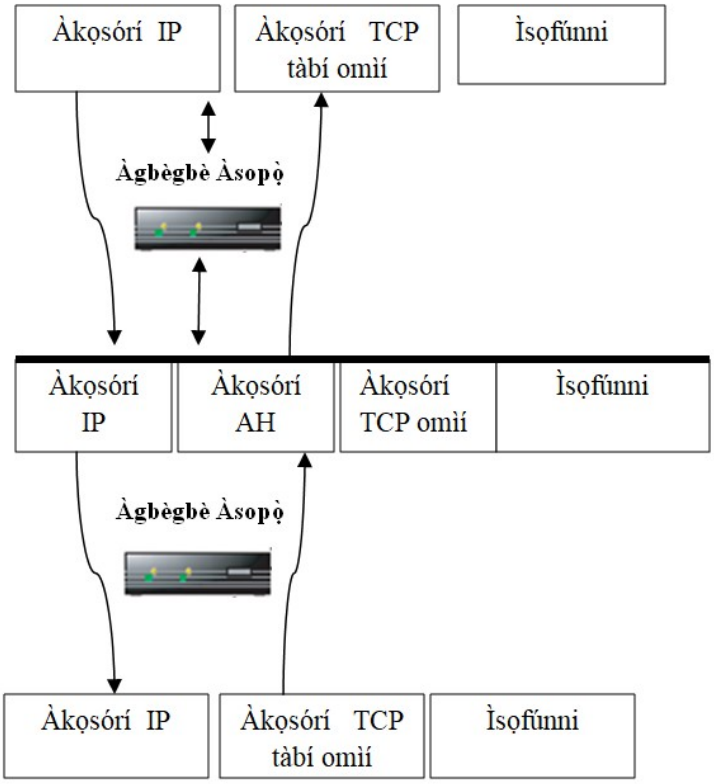
Ìsúnkì àwọn ìsọfúnni ààbò máa pèsè àwọn àṣírí ìsọfúnni tó wà nínú èdìdì IP tí a firánṣẹ́.
Máa ṣàfihàn bí tí a ṣàyípadà èdìdì IP pẹ̀lú àfikún àkọ́sórí ESP (ní ọ̀nà ìṣípòpadà, láì fọwọ́ kan ìwọ́ IP orísún).
Àkọ́sorí ESP ni a fikún ìwọ́ ìsọfúnni IP ti ìbẹ̀rẹ̀ láàrin ojú àkànpọ ìsokọ́ra méjì tí ń ṣàgbékalẹ̀ sáà IPsec. Nígbà tí a ò ti fọwọ́ kan àkọ́sórí IP ìlànà àwọn èdìdì IPsec ṣe kedere fún ìsokọ́ra tí ń firánṣẹ́ (intẹ̀ẹ̀nẹ́tì ...)

17.3.1 Àwọn ààyè àkọ́sórí ESP

- Ìtọ́kasí àwọn ààtò ààbò (bíìtì 32) : Máa tọ́kasí àsopọ̀ ààbò tí ń ṣàlàyé àwọn ààtò ààbò tó somọ́ sáà kan.
- Òǹkàye àwọn àtòtẹ̀lé èdìdì (bíìtì 32) : Òǹkàye tí kò níí jẹ́ kí àtúngba èdìdì lè ṣeé ṣe.
- Ìsọfúnni pàápàá tàbí tí a dáàbòbò pẹ̀lú ìpàrokò : Inú èyí ni àwọn ààyè èdìdì ti a pàrokò wà.
- Àfikún (0 dé 255 bíìtì) : Máa jẹ́ kí a ṣàfikún àyọkà ti a ti pàrokò kí a sì rí dájú pé àyọkà tí a pàrokò jẹ́ ìlọ́po báìtì kan tí àwọn ìfẹ̀nukò kan béèrè fún, ó sì tún máa jẹ́ kí a ṣèpamọ gígùn àyọkà náà.
- Gígùn àfikún (8 bíìtì) : Yóò fún wa ni iyé báìtì tí a lò fún àfikún.
- Ìtọ́kasí àkọsórí tó tẹ̀lé (bíìtì 8) :
  tọ́ka sí ìfẹ̀nukò tí yóò wà ní wájú nínú ààyè àwọn ìsọfúnni pàápàá.
- Ìsọfúnni ìfàṣẹsí (oníyípadà) : Inú èyí ni àbájadé ìdánilójú pípé ìsọfúnni ti a ṣíròwà láti ESP láì ka ààyè ìfàsẹsí àwọn ìsọfúnni mọ́.
  Àwọn ìtòlẹ́sẹẹsẹ ìpàrokò tí àwọn kọ́kọ́rọ́ àṣírí tó dúró lórí àwọn ìtòlẹ́sẹẹsẹ̀ DES, RC5, IDEA, CAST, BLOUFISH àti AES.
  Ìtòlẹ̀sẹẹsẹ̀ ìrídájú àwọn ìsọfúnni dúró lórí HMAC tí ń lò àwọn ìtòlẹ̀sẹẹsẹ̀ ààké bíi MD5 àti SHA-x.


En-tête IP
En-tête TCP ou autre
Données
Passerelle de sécurité
Authentifié hormis les champs modifiables
En-tête IP
En-tête AH
En-tête TCP ou autre
Données
Passerelle de sécurité
En-tête IP
En-tête TCP ou autre
Données


Àkọsórí IP
Àkọsórí TCP tàbí omìí
Ìsọfúnni
Àgbègbè Àsopọ̀
Àkọsórí IP
Àkọsórí AH
Àkọsórí TCP omìí
Ìsọfúnni
Àgbègbè Àsopọ̀
Àkọsórí IP
Àkọsórí TCP tàbí omìí
Ìsọfúnni



17.3.2 Àkọ́sórí ìfàṣẹsí (AH)

Bí a tí rí lórí àwòrán àkọ́sórí ìfàsẹsí AH (Authentification Header) máa fún wa ni àwọn ìpèsè fún pípé àwọn ìsọfúnni àti ìfàṣẹsí àwọn èdìdì IP (ọ̀nà ìṣípòpadà a máa ṣàfipamọ IP orísun).
Bíi àkọ́sorí ESP a ṣàfikún àkọ́sórí AH sínú ìwọ́ ìsọfúnni IP orísun ti ìbẹ̀rẹ̀ láàrin ojú àkànpọ ìsokọ́ra méjì tí ń ṣàgbékalẹ̀ sáà IPsec. Nígbà tí a ò ti fọwọ́ kan àkọ́sórí IP ìlànà àwọn èdìdì IPsec ṣe kedere fún ìsokọ́ra tí ń firánṣẹ́ (intẹ́ẹ̀nẹ́tì ..)

Àkọsorí AH ni àwọn ààyè wọ̀nyìí :

- Àkọsórí àtẹ̀lé (bíìtì 8) : Tọ́kasí irúfẹ́ àkọsórí tí ń tẹ̀lé àkọsórí AH.
- Gígùn àkọsórí ìfàṣẹsí (8 bíìtì): Tọ́kasí iye ọ̀rọ̀ bíìtì 32 tí àkọsórí AH
- Àyọsílẹ̀ (bíìtì 16) : Fún ìwúlò wájú
- Ìtọ́kasí àwọn ààtò ìdáàbòbò (32 bíìtì) Tọ́kasí ìdáàbòbò àsopọ̀ ààbò, yóò ṣàlàyé àwọn ààtò sáà kan.
- Òǹkàye ìtòléra àwọn èdìdì (32 bíìtì), Òǹkàye yìí máa jẹ́ kí àtúngbá èdìdì má wáyé.
- Ìsọfúnni ìfàṣẹsí (oníyípadà) : Máa fun wa ni ìṣíròò pípé àyẹ́wò tí a ṣé lórí èdìdì IP orísún.

A ṣé àwọn ìṣírò wọ̀nyẹn sórí àwọn ààyè tí kò níí láti yípadà nígbà ti édìdì IP bá gbánú ìsokọ́ra. Nígbà tí MAC (àmì ìfàṣẹsí iṣẹ́ẹ̀jẹ́) bá wà lórí àwọn ààyè oníyípadà bíi ìgbà ìwúlò èdìdì IP, Olùgbà máa rí wípé àyẹ̀wó àkọ́sórí jẹ́ alòdì. Ìtòlẹ́sẹẹsẹ̀ ìṣàyẹ̀wò pípé dúró lórí HMAC, tí ń lò àwọn ìtòlẹ́sẹẹsẹ ààké MD5 àti SHA-x.

18 Àkóso àwọn kọ́kọ́rọ́

Ìfẹnukò IKE (Internet Key Exchange : Pàṣipàárọ̀ Kọ́kọ́rọ́ Íńtẹ́nẹ́tì) ni a gbéjáde fún IPsec, ìdií èyí ni kó fún wa ni alàkalẹ̀ ìfàṣẹsí, àti pàṣipàárọ̀ kọ́kọ́rọ́. Ó wá láti ISAKMP fún àsopọ̀ ààbò pẹ̀lú ìfẹ́nukò Oakley àti SKEME (Secure key Exchange Mechanism : Alàkalẹ̀ pàṣipàárọ̀ kọ́kọ́rọ́ ààbò) ti iléṣẹ́ NSA, ìfẹnukò ISAKMP máa ń ṣàlàyé ìgúnrege èdìdì, àwọn wákàtí àtúnfiránṣẹ́..bẹ́ẹ̀ bẹ́ẹ̀ lọ fún àgbékalẹ̀ sáa pẹ̀lú ààbò. Fún pàsipàárọ̀ àwọn kọ́kọ́rọ́ sáà ìfẹnukò IKE máa ń lo ìfẹnukò pàṣipàárọ̀ kọ́kọ́rọ́ Oakley fi fún ìfẹnukò Diffie-Hellman ní agbára. Àwọn nǹkan tó di agbára ìfẹnukò ni àì sí ìfàṣẹsí lórí àfidámọ̀ olùmúlò, tí àwọn alátàkò máa ń lò bíi àtakò man-in-themiddle (èèyàn ni àárin) àti àwọn àtàkò ìkọ̀jálẹ̀ ìpèsè (denial of service attack) sórí ìpèsè kọ́kọ́rọ́ aláàṣe tó wáyé ṣíwájú ìfàṣẹsí pàápàá. Ockley máa ń lò cookies (kú kísì) ti kò sì nídìí kí a tún ṣírò àṣírí pínpín Diffie-Hellman kí ìfẹ́nukò tó dé òpin. Iṣẹ́ Oakley ni kó ridájú pé ìpín àwọn ohun èlò ìsọfúnni tó jẹ́mọ sáà kọ́kọ́rọ́ ṣé gbẹ́kẹ̀lé : Orúkọ kọ́kọ́rọ́, kọ́kọ́rọ́ àṣírí, àfidámọ̀ àwọn èèyàn, ìtòlẹ́sẹẹsẹ̀ ìfàṣẹsí àti iṣẹ́ ààké: ìdúnádùrà IKE fún àsopọ̀ ààbò máa ń wáyé ní ìpele méjì :

- **Ọ̀nà gbogbonṣe**

Ìpele ìgbékalẹ̀ àsopọ̀ ààbò ISAKMP máa fún wa ni àǹfààní láti dúnádùrà àwọn àfidámọ̀ wọ̀nyìí:
Ìtòlẹ́sẹẹsẹ̀ ìpàrokò, iṣẹ́ ààké, alàkalẹ̀ ìfàṣẹsí pẹ̀lú àkójọpọ̀ fún Diffie-Hellman tàbí fún ìlà ìrísí bíi ẹyín.
Ọ̀ń méta ni a máa fi ṣé ìfàṣẹsí.

- **Pínpín àṣirí ìbẹ̀rẹ̀.** A máa pàá láṣẹ kí a ṣègbékalẹ̀ kọ́kọ́rọ́ kannáà sórí àwọn ẹ̀rọ tí wọ́n fẹ́ ṣàsopọ̀ sáà IPsec. Wọ́n máa ṣé ìfàṣẹsí láàrin ara wọn pẹ̀lú iṣẹ́ ààké (HMAC-MD5, HAC-SHA-x) pẹ̀lú kọ́kọ́rọ́ àṣírí.
- Ìfọwọ́sí olóǹkàye : Kọ́kọ́rọ́ méjì ni a máa ń pín (káríayé, àṣírí) ìfàṣẹsí dúró lórí pàṣipàárọ̀ àwọn ìsọfúnni ti àwọn ẹ̀yà méjèjì fọwọ́sí pẹ̀lú ìtòlẹ́sẹẹsẹ ìfọwọ́sí olóǹkàye (RSA , DSS) pẹ̀lú ìfọwọ́síwé àìmálèjiyàn
- Ìdámọ̀ pẹ̀lú ìpàrokò kọ́kọ́rọ́ káríyé. Àwọn ẹ̀yà ẹ̀rọ kọ̀ọ̀kan láti ní kọ́kọ́rọ́ (káríayé, àṣírí). Ìfàṣẹsí dúró lórí pàṣipàárọ̀, àwọn ìsọfúnni pẹ̀lú

ìfọwọ́síwé ẹ̀yà kọ̀ọ̀kan pẹ̀lú ìtòlẹ́sẹẹ̀sẹ̀ ìfọwọ́síwé olónkàméjì (RSA ,DSS)

Ìfàṣẹsí ọ̀nà ìpàrokò oní kọ́kọ́rọ́ káríayé

Pàá lásẹ kí ẹ̀rọ ètò àlàkalẹ̀ kọ̀ọ̀kan ní àwọn kọ́kọ́rọ́ alákóméjì (Káríayé, àṣírí). A máa ń ṣe ìfàṣẹsí pẹ̀lú pàṣipàárọ̀ àwọn ìsọfúnni tí a pàkorò pẹ̀lú kọ́kọ́rọ́ àìlọ́pọméjì (RSA) ní èbúté àwọn ẹ̀yà méjèjì ti sáà IPsec. Àlàkalẹ̀ yìí, kìí fún wa ni àìmálèjiyàn fún àwọn ẹ̀yà méjèji. Ọ̀nà àbáyọ ni ìwé ìjẹ́rìísí olónkàye, tí àpaṣẹ́ ìwé ìjẹ́rìísí kan fọwọ́sí.

- Ọ̀nà yìí ń lò èdìdì mẹ́fa (ìpele pàṣipàárọ̀ mẹ́ta) tó fún wa ní àǹfààní láti dáàbòbò àfidámọ̀ àwọn olùkópa. A tún lè lò ọ̀nà oníjàgíjàgan tí yóò lò èdìdì mẹ́ta, àmọ́ kò níí ààbò tó péye.

. Ọ̀nà ìyára : **Quick Mode**

Ìpele yìí máa jẹ́ kí a ṣàgbékalẹ̀ àsopọ̀ ààbò AH àti/tàbí ESP tí yóò sì dùnádùrà pẹ̀lú àwọn ààtò ìfẹ́nukò abẹ́nu, àwọn ìdúnádùrà máa yọrí sí kéretan SA méjì, ọ̀kan fún ìdárí àsopọ̀. Àsopọ̀ ààbò ISAKMP tí ìdúnàdùrà ìbẹ̀rẹ̀ ni yóò dáàbòbò ṣíṣàjọpín sáà náà.

Ìfẹnukò IKE tún ní ọ̀nà mì ín fún ìsopọ̀ àti ìtúndúnàdùrà àwọn kọ́kọ́rọ́ tí a ti lò fi pàrokò àwọn ìsọfúnni pẹ̀lú ìtòlẹ́sẹẹ̀sẹ alọ́pọméjì. Ó ṣeé ṣe kí a lò àwọn àfidámọ̀ ìfẹ́nukò PFS(Perfect Forward Secrecy : Àsírí ìfiránṣẹ́ tó dára) pẹ̀lú ẹ̀yàn yìí ayóò rí dájú pé àwọn kọ́kọ́rọ́ tí a pèsè, ọ̀kan kò níí ìbatan pẹ̀lú òmìràn, méjì ò jọ ara wọn. èyí tó túmọ̀ sí pé agbára ààbò yóò tún ga tún ga fikún. Gbogbo ètò àlàkalẹ̀ ti gbogbo àwọn kọ́kọ́rọ́ alálọ́pọméjì kúró ní kọ̀kọ̀rọ̀ àṣírí kannáà kò ní àwọn afidámọ̀ ìfẹ́nukò PFS.

Àwọn ọ̀nà ìfaṣẹsí mì ín

IPsec máa ṣàgbékalẹ̀ ọ̀nà-abẹ́lẹ̀ aláàbòò pẹ̀lú àwọn àlàkalẹ̀ ìfàṣẹsí tó dúró lórí àṣírí tí a pín tàbí àwọn ìwé ìjẹ́ẹ̀rìísí.

Àmọ́ àwọn ìgbékalẹ̀ wíwọlé àti òkèrèsínú àwọn ìsokọ́ra ilésẹ̀ kò dúró lórí àwọn àlàkalẹ̀ ìfàṣẹsí wọ̀nyìí, wọn kò ní ìdọ́gba pẹ̀lú ọ̀nà ìfaṣẹsí tí IKE ń lò ní gbèdéke.

Pẹ̀lú ìṣàkósó àwọn kọ́kọ́rọ́ PKI (Public Key Infrastructure: Kọ́kọ́rọ́ káríayé ìgbékalẹ̀) tún dídíjú jù ìṣàkósó àkójọpọ̀ ìsọfúnni orúkọ / ọ̀rọ̀ ìṣínà.

Láti rí àbájáde fún ìṣòrò yìí a gbé àwọn ìfẹnukò Xauth pẹ̀lú ọ̀nà ìfàṣẹsí àdàpọ̀àti ẹ̀yàn ìdámọ̀ IKE ni a máa lò

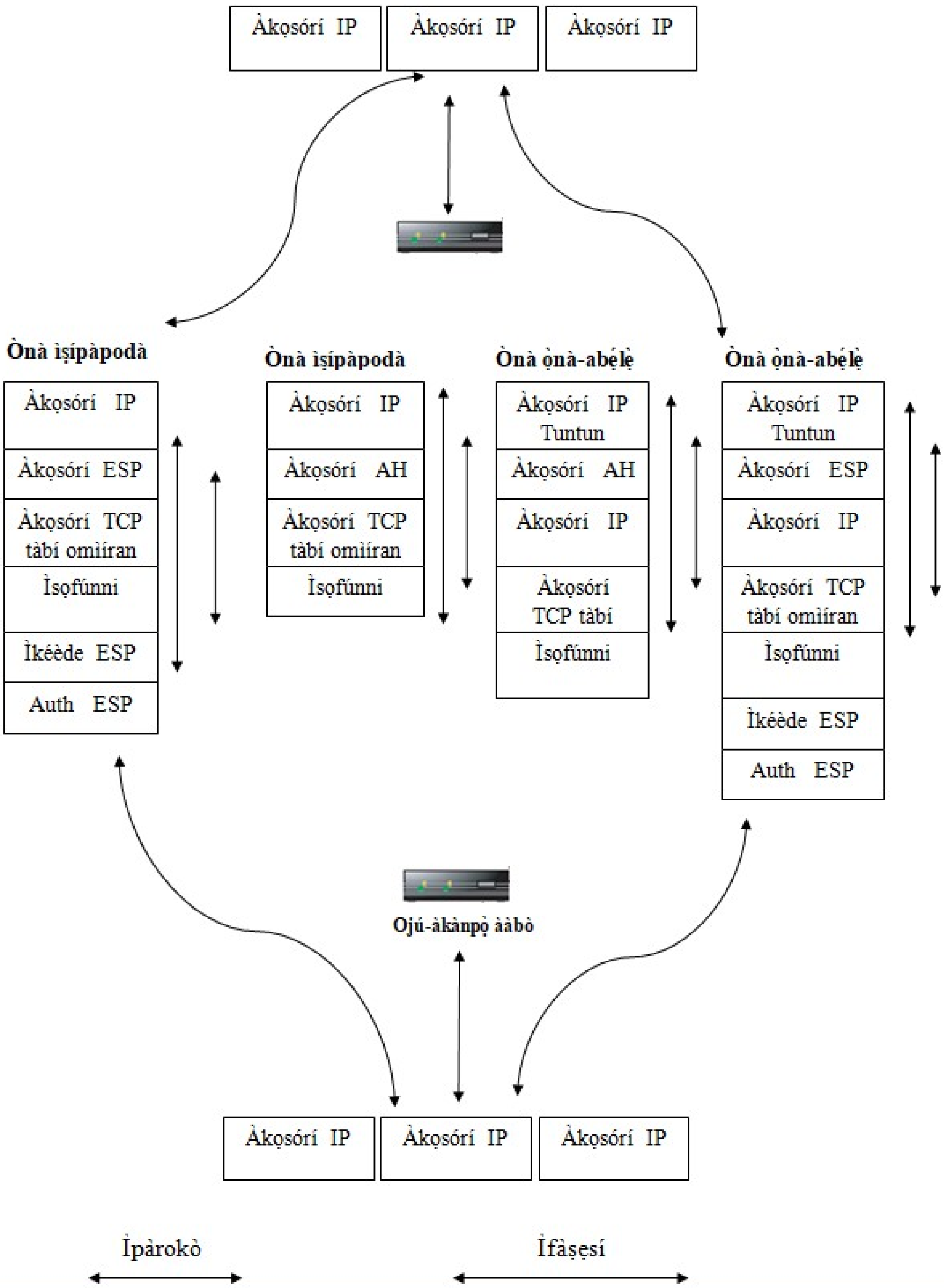
- Xauth : Ìpele àkọ́kọ́ ti ìfẹnukò IKE máa jẹ́ kí aṣojú àti apèsè ṣe pàṣipàárọ̀ kọ́kọ́rọ́ ìpàrokò àti ìfàṣẹsí láàrin àwọn méjèjì. lẹ́yìn èyí ni àsopọ̀ ààbò

máa wáyé tí á sì máa lò ní ìpele kèjì II.
Ní ìpele kèjì yìí Xauth máa fún olùmúlò ní àǹfààní láti lò àwọn ẹ̀yàn ìfàṣẹsí mí ìn tó yàtọ̀ sí àwọn ìfẹ́nukò gbèdéke.

- IKE (RADIUS, CHAP, OTP, SIKEY ....) ìfẹnukò yìí máa wa láàrin ìpele I àti II ti IKE tó sì ni ààbò pẹ̀lú ìdùnádùrà ti ìpele I. Àmọ́ tó bá ṣàfikún ìfàṣẹsí, ìṣàkóso pínpín àsírí tàbí ìjẹ́rììsí pọn dandan lórí aṣojú àti orí apèsè. ó máa ṣàfihàn ìdámọ̀ olùmúlò àti ìṣàkósó ìpín àṣírí tàbí ti ìwé ìjẹ́rììsí ni èbúté ojúṣe àti apèsè.
- IKE (Hybrid : Àpàpọ̀) ọ̀nà ìfàṣẹsí yìí máa ń fún wa ní àǹfààní láti ṣàpàpọ̀ ọ̀nà ìfàṣẹsí méjì tó yàtọ̀ láàrin aṣojú (Àpẹẹrẹ orúkọ / ọ̀rọ̀ aṣínà) àti apèsè (iwé ìjẹ́rììsí). Ní òpin ìpele I ìfènukò IKE, ọ̀nà-abẹ́lẹ̀ kan wáyé bó tílẹ̀ jẹ́ wípé aṣojú ṣàdámọ̀ apèsè pẹ̀lú ìwé ìjẹ́rììsí, tí kò sí rí bẹ́ẹ̀ pẹ̀lú apèsè lọ́dọ̀ aṣojú. Ní ìpele yìí Xauth máa jẹ́ kí a ṣèfàṣẹsí aṣojú lọ́dọ̀ apèsè.
Fún ìfẹ́nukò IKEv2 ọ̀nà àbáyọ tí a rí ni ìfàṣẹsí tó dúró lórí ìfẹ́nukò EAP (Extensible Authentifiction Protocol)

Ọ̀nà ìṣípopadà àti ọ̀nà-abẹ́lẹ̀.

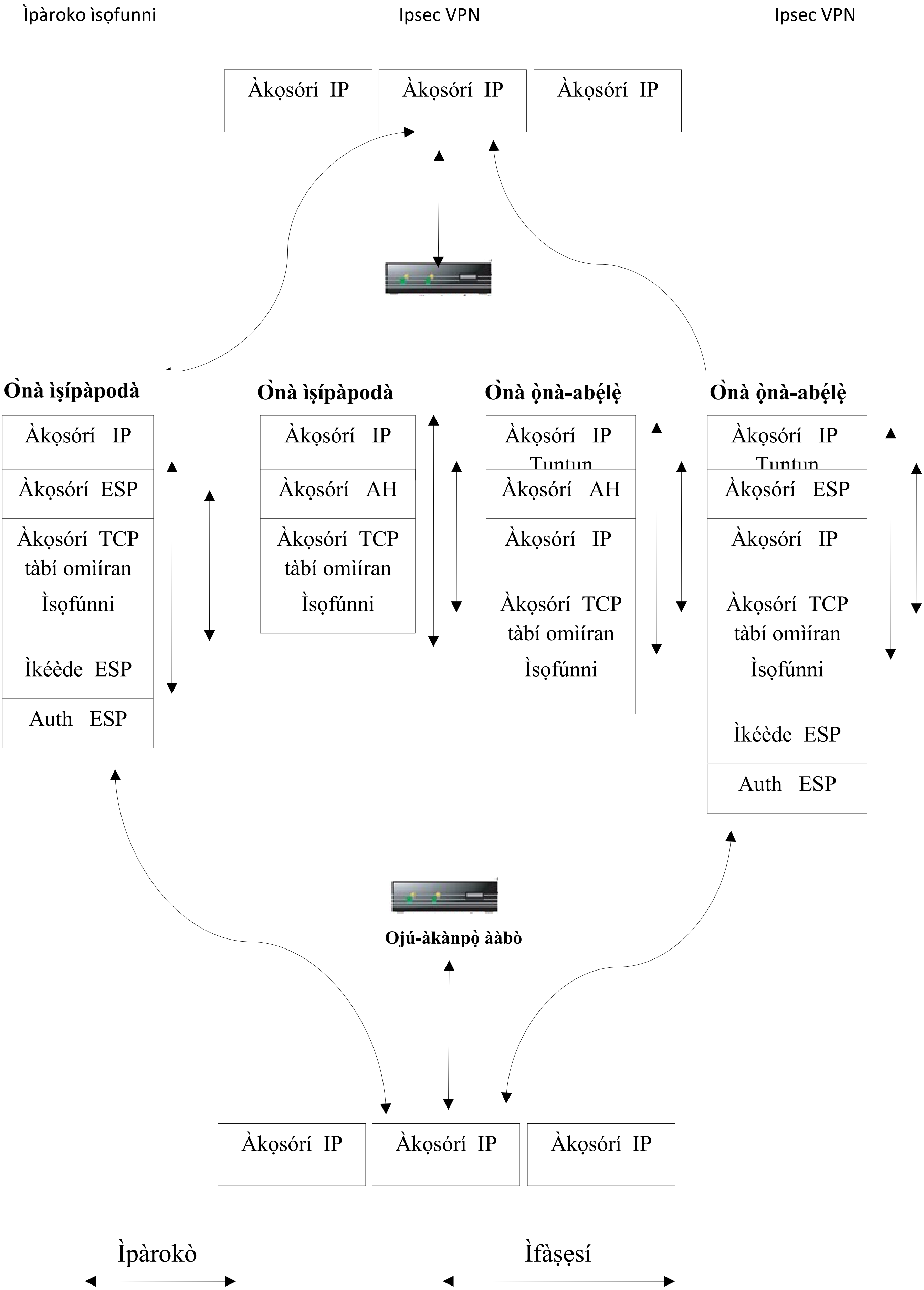
Ọ̀nà ìṣípopadà méjì ni IPsec ń lò fikún àwọn ẹ̀yàn tí a ti rí : ọ̀nà ìṣípopadà àti ọ̀nà-abẹ́lẹ̀.

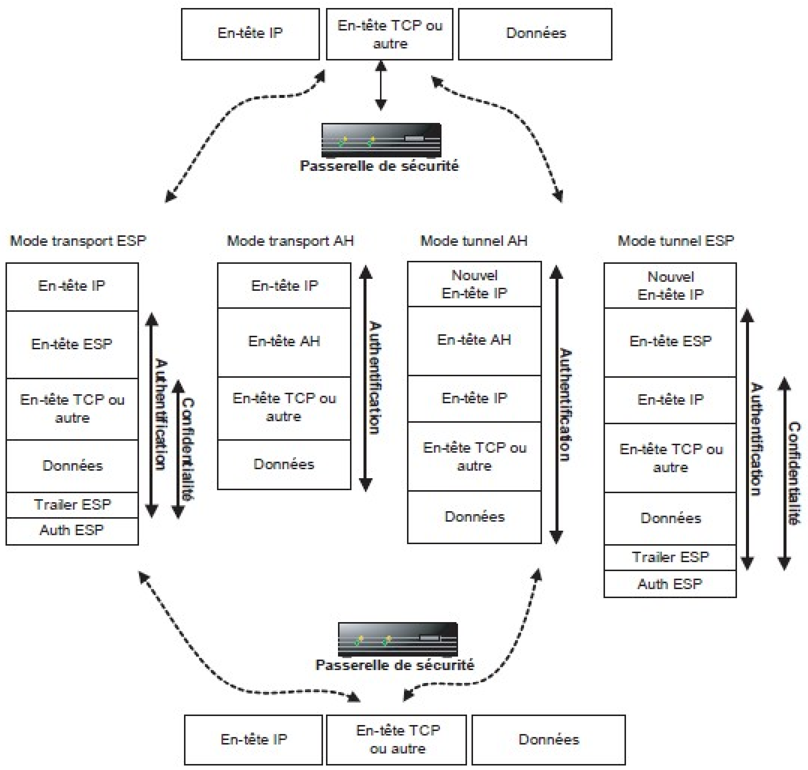


Ọ̀nà-abẹ́lẹ̀ máa ń ṣàkójọ èdìdì túntún pẹ̀lú ìsúnkì èdìdì orísun fi dáàbòbò bó wọn, àwọ àdírẹ́ẹ̀sì èbúté àti ti orísun èdìdì tuntun máa yàtọ̀ sí ti orísun Èyí ni yóò fún ààbò ní agbára.
Àwọn àsopọ̀ ààbò lè wáyé ní ẹ̀yàn ọ̀nà-abẹ́lẹ̀ tàbí ọ̀nà ìṣípòpadà. Ọ̀nà mẹ́rin ni a yóò lò fi ṣàgbékalẹ̀ sáà aláàbò :

- Àsopọ̀ sáà aláàbò láàrin ẹ̀rọ ètò ilànà tí a á sì lò AH ní ọ̀nà ìṣípòpadà, tàbí ESP ní ọ̀nà ìṣípòpadà, tàbí ESP ní ọ̀nà ìṣípòdadà nínú AH ní ọ̀nà ìṣípòpadà, tàbí AH nínú ESP ní ọ̀nà abẹ́lẹ̀...

- Àsopọ̀ sáà aláàbò láàrin ojú àkànpọ̀ méjì ní ọ̀nà abẹ́lẹ̀ (gbogbo ìgbà ESP ní ọ̀nà abẹ́lẹ̀ fún àṣírí àwọn ìsọfúnni pẹlú ìfipamọ àwọn àdírẹ́ẹ̀sì orísun)
- Àsopọ̀ sáà aláàbò ní ọ̀nà ọ̀nà-àbẹ́lẹ̀ ẹ̀rọ ètò ìlànà méjì gbà inú sáà aláàbò láàrin ojú àkànpọ̀ méjì ní ọ̀nà ọ̀nà-abẹ́nu. A lè rí gẹ́gẹ́ bíi àpàpọ̀ 1 àti 2
- Àsopọ̀ sáà aláàbò ní ọ̀nà ọ̀nà-àbẹ́lẹ̀ (gbogbo ìgbà ESP ní ọ̀nà abẹ́lẹ̀ fún àṣírí àwọn ìsọfúnni pẹlú ìfipamọ àwọn àdírẹ́ẹ̀sì orísun) mọ́ ojú àkànpọ̀, àmọ́ pẹ̀lú àsopọ̀ sáà aláàbò láàrin ẹ̀rọ ètò ìlànà gbànu sáà aláàbò pẹ̀lú àkànpọ̀.
  A ní láti lò sáà ọ̀nà ọ̀nà-abẹ́lẹ̀ fún àsopọ̀ ààbò tí ń gbà ìsokọ́ra káríayé tí a kò sì ní lò ó fún ìsokọ́ra tí gbànu ilé̩ṣẹ́.
  Èyí ni ìsokọ́ra àdání tí àwọn iléṣẹ́ ẹ̀rọ ìbáraẹnisọ̀rọ̀ ń lò lórí íntẹ́nẹ́ìtì.
  Tàbí lórí ìsokọ́ra ìpèsè ìmọ́ ẹ̀rọ MPLS / VPN. Ìmọ́ ẹ̀rọ MPLS (MultiProtocol Label Switching : Ìyípopadà Ìṣàmìsí Ọ̀pọ̀ Ìfẹ́nukò) kìí pèsè ìpàrokò àwọn èdìdì kan.
  Fún àwọn àsopọ̀ ìsokọ́ra lórí ìsokọ́ra MPLS, A yóò ṣàgbékalẹ̀ àwọn ojú àkànpọ̀ IPsec tí yóò fún wa ní àǹfààní láti gbé àwọn sáà aláàbò ní ọ̀nà ọ̀nà-abẹ́lẹ̀kalẹ̀ìtàkùrọ̀sọ àwọn ojú àkànpọ̀ IPsec tí á fún wa ni àǹfààní kí a tò àwọn àsopọ̀ pẹ̀lú ẹ̀yàn ọ̀nà-abẹ́lẹ̀ kalẹ̀ pẹ̀lú ESP àti ìfàṣẹsí tó pọn dandan.
- A yóò lò ojú àkànpọ̀ fún ìṣàkósó àwọn sáà aláàbò fún ìgbà ìdákùn tó kúrú jù. abẹ́nu iléṣẹ́ máa ń lò àsopọ̀ ààbò ni ẹ̀yàn ìṣípopadà.
  Ìyàn ẹ̀yàn AH àti ESP lè ṣeé ṣe nígbà tí a bá yàn wọn.


Ìpàroko ìsọfunni
Ipsec VPN
Ipsec VPN
Àkọsórí IP
Àkọsórí IP
Àkọsórí IP
Òǹà ìṣípàpodà
Àkọsórí IP
Àkọsórí ESP
Àkọsórí TCP tàbí omìíran
Ìsọfúnni
Ìkéède ESP
Auth ESP
Òǹà ìṣípàpodà
Àkọsórí IP
Àkọsórí AH
Àkọsórí TCP tàbí omìíran
Ìsọfúnni
Òǹà ọ̀nà-abẹ́lẹ̀
Àkọsórí IP Tuntun
Àkọsórí AH
Àkọsórí IP
Àkọsórí TCP tàbí omìíran
Ìsọfúnni
Òǹà ọ̀nà-abẹ́lẹ̀
Àkọsórí IP Tuntun
Àkọsórí ESP
Àkọsórí IP
Àkọsórí TCP tàbí omìíran
Ìsọfúnni
Ìkéède ESP
Auth ESP
Ojú-àkànpọ̀ ààbò
Àkọsórí IP
Àkọsórí IP
Àkọsórí IP
Ìpàrokò
Ìfàṣẹsí



IP Dátágrámù

Nígbà tí fẹ́ kẹ́kọ́ IPsec láti òkè dé ilẹ̀, a máa mú àsìkò díẹ̀ láti padà sórí ẹ̀kọ́ àkọsórí IP tí ń ṣẹ̀ṣípopàdà àwọn ìgbì ìsọfúnni tí afẹ́ kọ́ ẹ́kọ́ ẹ. Àmọ́ a ò fẹ́ tú ẹ̀kọ́ àkọsórí IP délẹ̀.

ver Ẹ̀yà ìfẹnukò ni, ibi 4 = IPv4

hlen Gígùn àkọsórí IP ló jẹ́ tó sì jẹ́ 4 bíìtì nínú ọ̀rọ̀ 32 bíìtì tó sì tún wà láàrin 0 dé 15 bíìtì. Gígùn àkọsórí IPv4 máa sàbá jẹ́ 20 báìtì (ọ̀rọ̀ 5 ti 32 bíìtì). Pẹ̀lú àwọn ẹ̀yàn IP gígùn lè dé 60 báìtì tí kò sì lè jù bẹ́ẹ̀ lọ, nínú gígùn yìí a ò ka àwọn ìsọfúnni mọ́.

TOS Irúfẹ́ ìpèsè èdìdì náà, ní ààyè yìí a máa rí àwọn bíìtì ìbojú tí ń tọ́ka sí àwọn ìpèsè tí Dátágrámù yìí lè gbà : fífẹ́ ojúnà détà, ìgbà ìretí, owó Kékeré, ìgbẹ́kẹ̀lé.

pkt len Gígùn èdìdì pátápátá ní iye báìtì tó lè gùn dé 65535 báìtì. Ẹ̀yí tó túmọ̀ sí pé gígùn àwọn ìsofúnni máa di 20 báìtì tó jẹ́ gígùn àwọn àkọsórí. Àmọ́ gígùn máa sàbá kére púpọ̀ sí iye yìí.

ID A máa lò ààyè yìí fún mọ́mbà àjákù èdìdì tí pín sí yẹ́lẹyẹ̀lẹ nígbà tí gígùn èdìdì yìí ò lè gbanu àsopọ̀.

flag àsá ti a máa fi dárí ìpínyẹ́lẹyẹ́lẹ àwọn èdìdì, àmì àsìá lè jẹ́ èyí tó gbà ìpínyẹ́lẹyẹ́lẹ, tó kọ̀ ọ́ tàbí èyí tí ń sọ fún wa pé àjákù mì-ín tún wà lẹ́yìn.

frag ààfò Nígbà tí a bá pín èdìdì kan yẹ́lẹyẹ́lẹ pẹ̀lú ààfò yìí ni a máa mọ́ ààyè àjákù èdìdì nínú èdìdì odidi.

TTL ìgbésí-ayé èdìdì, a máa ń ṣèyọkúró ọ̀kan nínú ìgbà ìgbésí-ayé, gbogbo ìgbà tí èdìdì bá dá alànà kan kọjá. Tí nọ́mbà yìí bá di òdo èdìdì yìí parẹ kó máa ba máa yí làìnítúmọ̀.

Proto Ìfẹ́nukò tí a ń ṣèṣípòpadà rẹ̀ ni. Nígbà ti dátágrámù náà bá jẹ́ ti IP, ìfẹnukò yìí tún ṣèsípòpadà fún àwọn ìfẹnukò abẹ́nu bíi (TCP, UDP, ICMP...).

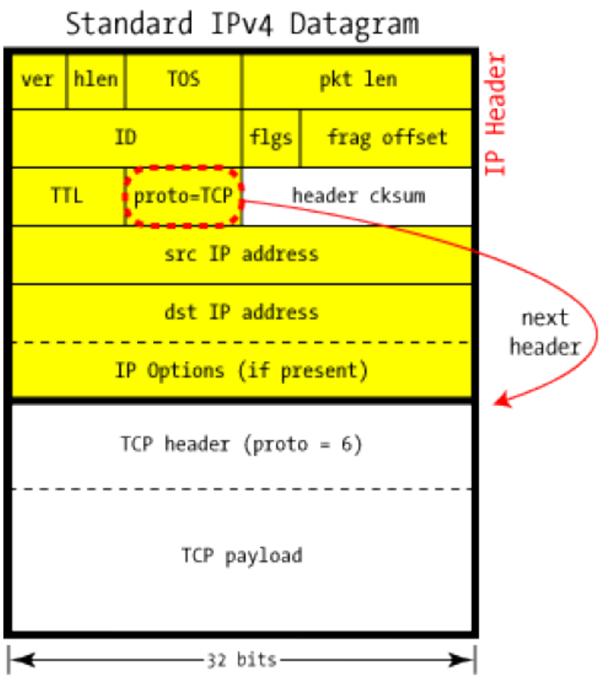
Header cksum Inú ààyè yìí , a máa rí gbogbo àwọn ìsọfúnni ìṣàrídájú èdìdì náà, a máa lò wọ́n fi mọ̀ àwọn àkùnà tó wáyé nígbà ìṣípòpadà àwọn èdìdì, kìí ṣé ìpàrokò, bẹ́ẹ̀ ni kìí ṣé ìdáàbòbò àwọn èdìdì.

Src IP address àdírẹ́ẹ̀sì alátagbà tí agbàsọfúnni máa lò fi fèsì èdìdì náà, àmọ́ ó ṣeé ṣe kó máa jẹ́ àdírẹ́ẹ̀sì òtítọ́, tí àwọn èèyàn ti yípadà.

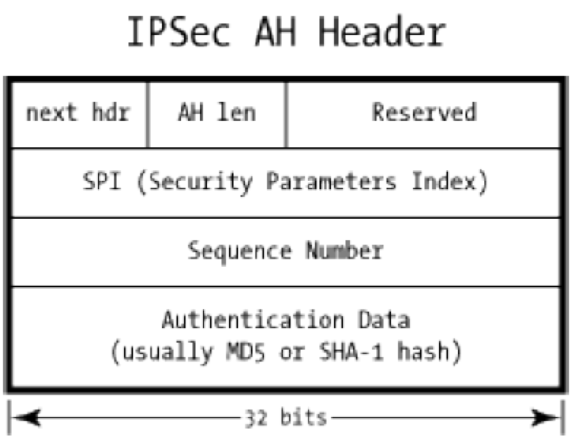
Dest IP address àdírẹ́ẹ̀sí IP ibi ti édìdì náà lè lọ.

IP Options Ààyè àkọsórí IP tí kìí ṣé dandan, ní ààyè yìí a máa rí àwọn ìsọfúnni ètò nínú ẹ, àmọ́ a kìí sàbá lò ó.
Nígbà tí a bá fẹ́ mọ̀ pé ẹ̀yàn wà nínú àkọsórí ààyè hlen máa jẹ́ iye tó jù 5, a máa fi ìsọfúnni tó jẹ́mọ ẹ̀yàn náà sínú ààyè Header cksum àkọsórí.

Payload : Ìsọfúnni tó wúlò, ìfẹnukò kọ̀ọ̀kan, ní ìgúnrégé ti rẹ̀ tó sì tẹ̀lé ìfẹnukò IP, àwọn ìfẹnukò náà ni TCP, ICMP...



Ọ̀nà Ìfàṣẹsí nìkan



A ń lò AH fún ìfàṣẹsí, a ò lè lò ó fún ìpàrokò. Èrò wa ni kó dá wa lójú pé a ń sọ̀rọ̀ fún ẹni tí a dámọ̀, kí a sì ríran rí àwọn èdìdì tí kò pé látara ìṣípòpadà wọn, kí a sì rí dájú pé àwọn ajalélókun tí ń ṣàgélọgán àwọn ìsọfúnni tí ń kọjá, wọ́n ò tún lè dá wọn padà ni àkókò mì ín sínú àwọn ìsọfúnni tí ń tẹ̀lé àwọn èyí tó ti kọjá sí wájú

Next hdr : Inú ààyè yìí ni a máa ri ìfẹ́nukò àtẹ̀lé, èdìdì orísun tí a súnkì, pẹ̀lú àwọn àkọsórí .

AH len : Ààyè yìí ń ṣàlàyé gígùn gbogbo àkọsórí AH lọ́nà ọ̀rọ̀ bíìtì 32 pẹ̀lú ìyọkúrò ọ̀rọ̀ méjì.

Reserved : Ó wà nípamọ fún ìwúlò ọjọ́ wájú.

SPI (Security Parameters Index : Ìtọ́kasí Ààtò Ààbò): àfidámọ̀ kan oní bíìtì 32 tí ń ṣèrànlọ́wọ́ fún olùgbà alátagbà láti yàn àwọn oríṣiríṣi ìtàkúrọ̀sọ tó wà lórí èdìdì náà. Àsopọ̀ kọ̀ọ̀kan tí AH dáàbòbò máa ń lò alúgórídíìmù ààké (MD5, SHA-1, ...etc); ó dàbí ọpọ̀ ìsọfúnni àṣírí àti àwọn ààtò mìíràn. A lè rí SPI bíi ìtọ́kasí inú àtẹ àwọn ààtò tí ń jẹ́ kí ìsopọ̀ èdìdì pẹ̀lú àwọn ààtò rọrùn.

Nọ́mbà ìtòléra : Ìtọ́kasí nọ́mbà tí ń lọ sókè láláìṣeéyípadà tó sì fún wa ni àǹfààní láti má jẹ́ kí ìtúnlò èdìdì wáyé, a máa ń fi nọ́mbà yìí bọnu àwọn ìsọfúnni ìfàṣẹsítí tí ń jẹ́ kí a máa ṣàkíyèsí àwọn ìyípadà tó fẹ́ máa ṣẹ̀lẹ̀.

Ìfàṣẹsí ìsọfúnni : àgbéjáde ìṣírò pípé ìsọfúnni tí a ṣé lórí èdìdì kan pẹ̀lú àwọn àkọsórí rẹ̀, alátagbà máa tún ìsírò náà sé pẹ̀lú ààké tí a sì máa rí wí pé àwọn ìṣírò wọ̀nyìí dọ́gbà bí kò jẹ́ bẹ́ẹ̀, a máa gbé èdìdì yìí sọnu.

Ìṣírò àmì iṣẹ́ẹ̀jẹ́ ti a ṣé pẹ̀lú iṣẹ́ ààké ìpàrokò sórí gbogbo àwọn ààyè èdìdì àfi àwọn ààyè tí ń yípadà ni á fún wa láǹfààní láti ṣefàṣẹsí orí àwọn èdìdì tí a sì kó gbogbo wọn sínú AH ti a sẹ̀dá kí a tó firánsẹ́ sí èbúté kèjì.

Ọ̀nà-abẹ́lẹ̀ sí ọ̀nà ìṣípòpadà

Ọ̀nà ìsípòpadà máa ń ṣàsopọ̀ láàrin èbúté ojú-àmì ìsopọ̀ méjì, ó máa fún wa ni àǹfààní láti ṣèsúnkì ìsọfúnni IP, àmọ́ ọ̀nà–abẹ́lẹ̀ máa ṣèsúnkì èdìdì lódídí fi fún fífò ààbò àfinuwò láàrin ojú-àkànpò méjì. Èyí ni a máa ń lò fún VPN tí yóò ṣẹ̀dá ọ̀nà-abẹ́lẹ̀ pẹ̀lú ààbò gbanu ayélujara ti kò níí ààbò.

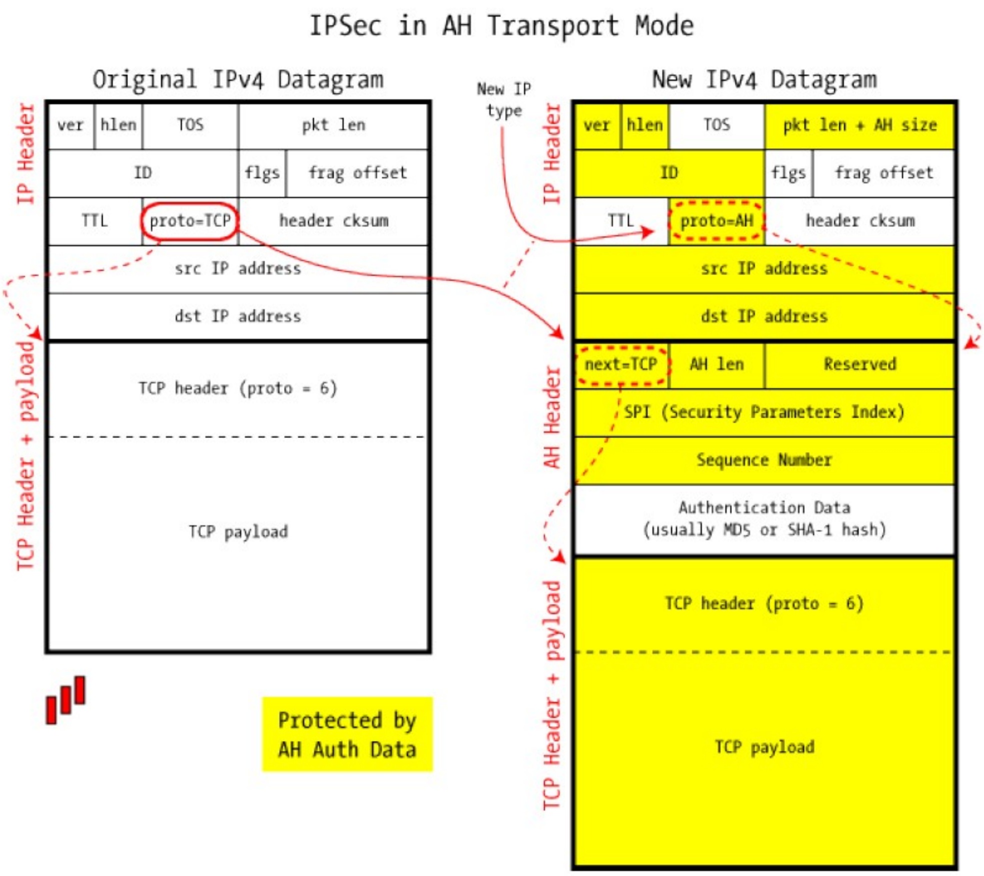
IPsec Ọ̀nà ìṣípopadà

Ọ̀nà tó rọrùn ni ọ̀nà ìṣípopadà, ó lè tètè yé ẹni. Ọ̀nà ìsípoppadà ni a máa ń lò fi dáàbòbò ìbáẹraẹnisọ̀rọ̀ kúró ni èbúté kan lọ sí omií. Ìdáàbòbò lè jẹ́ ìfàṣẹsí, ìpàrokò, tàbí àwọn méjèjì, àmọ́ kìí ṣe ìṣípòpadà ọ̀nà-abẹ́lẹ̀, kìí ṣe VPN, àsopọ̀ IP pẹ̀lú ààbò ni.

Ní ọ́nà ìsípòpadà AH, a máa ṣàtúntò èdìdì IP díẹ̀, a máa fi àkọsórí AH túntún sí ààrin àkọsórí IP àti àwọn ìsọfúnni tó wà lẹ́yìn ti àwọn ìfẹ́nukọ̀ wọn jẹ́ (TCP, UDP....etc) òfin ìdàpọ̀ kan so àwọn àkọsórí pọ̀.

Àwọn àsopọ̀ ìfẹnukọ̀ ṣe pàtàkì fi ṣàtúntò èdìdì IP, kí a sì tún padà rí IP orísun ní èbúté ìpari.
Nígbà tí a bá ti ṣèfọwọ́síwé àkọsórí IPsec , olùmúlò alátagbà máa yọ àwọn àfikún kúró, tí á wá kù irú ìfẹnukò orísun (TCP, ICMP, ...) tí a máa kó padà sínú àkọsórí IP.

Nígbà tí èdìdì bá dé èbúté tó sì gbà àyẹ̀wó ìfàṣẹsí kọjá a máa ṣèparẹ́ àkọsórí AH nínú àkọsórí IP , a máa ṣèrọpò ìfẹnukò AH pẹ̀lú ìfẹnukò tó tẹ̀lé ìsọfúnni IP máa padà sórísun, a lè gbé fún ìṣiṣẹ́ tó tẹ̀lé.



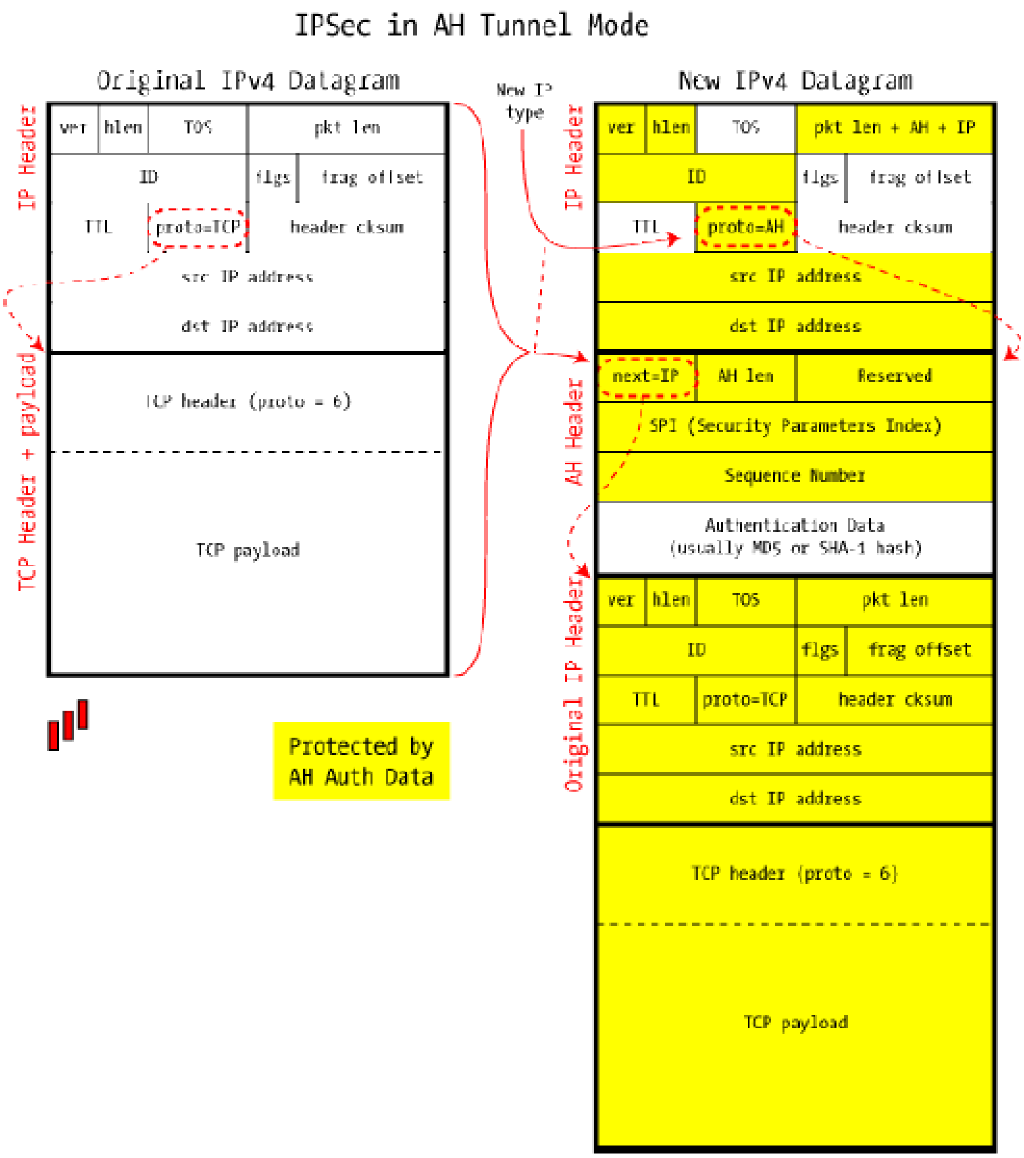
IPsec Ọ̀nà ìṣípòpadà

Ọ̀nà tó rọrùn ni ọ̀nà ìṣípopadà, ó lè tètè yé ẹni. Ọ̀nà ìsípoppadà ni a máa ń lò fi dáàbòbò ìbáẹraẹnisọ̀rọ̀ kúró ni èbúté kan lọ sí omìí. Ìdáàbòbò lè jẹ́ ìfàṣẹsí àbíìpàrokò, tàbí àwọn méjèjì, àmọ́ kìí ṣe ìṣípòpadà ọ̀nà-abẹ́lẹ̀, kìí ṣe VPN, àsopọ̀ IP pẹ̀lú ààbò ni.
Ní ọ́nà ìsípòpadà AH a máa ṣàtúntò èdìdì IP díẹ̀ fi fi àkọsórí AH sí ààrin àkọsórí

IP àti àwọn ìsọfúnni tó wà lẹ́yìn ti àwọn ìfẹ́nukọ̀ (TCP, UDP....etc) òfin ìdàpọ̀ kan so àwọn àkọsórí pọ̀.

Àwọn àsopọ̀ ìfẹnukọ̀ ṣe pàtàkì fi ṣàtúntò èdìdì IP orísun ní èbúté ìpari.
Nígbà tí a bá ti ṣèfọwọ́sí àkọsórí IPsec , olùmúlò aàgbà máa yọ àwọn àfikún kúró tí á wá kù irú IP orísun tí a máa fipamọ sínú àkọsórí IP.

Nígbà tí èdìdì bá dé èbúté tó sì gbà àyẹ̀wó ìfàṣẹsí kọjá a máa ṣèparẹ́ àkọsórí AH nínú àkọsórí IP , a máa ṣèrọpò ìfẹnukò AH pẹ̀lú ìfẹnukò tó tẹ̀lé ìsọfúnni IP máa padà sórísun, a lè gbé fún ìṣiṣẹ́ tó tẹ̀lé.



Ọ̀nà-abẹ́lẹ̀

Ọ̀nà abẹ́lẹ̀ ni a máa ń lò fún VPN, níbi ti á ṣèsúnkì gbogbo èdìdì sínú omìí títí dé èbúté. Bíi ọ̀nà ìṣípòpadà a máa dé èdìdì pẹ̀lú àbájáde ìṣíró ìdarí fún pípé ìsọfúnni láti fi ṣé ìfàṣẹsí àti ìṣàtúntò nígbà ti èdìdì bá ń ṣèṣípòpadà.
Èyí ti ọ̀nà-abẹ́lẹ̀ ṣe yàtọ sí ọ̀nà ìṣípòpadà ni ọ̀nà-abẹ́lẹ̀ máa ń ṣé ìsúnkì àkọsórí èdìdì àti gbogbo àwọn ìsọfúnni àdírẹ́ẹ̀sì alátagbà àti agbásọfúnni máa yàtọ.
Nígbà tí èdìdì ọ̀nà-abẹ́lẹ̀ bá dé èbúté, wọ́n máa gbà àyẹ̀wò ìfàṣẹsí kannáà pẹ̀lú àwọn èdìdì àlákọsórí AH. Àwọn èyí tó bá ráyè kọjá àkọsórí AH àti IP máa jẹ́ píparẹ, èdìdì IP máa padà sórísùn tí yóò sì máa gbà inú àfisọ̀nà mì ín lọ.
èdìdì orísùn ni a máa firánṣẹ́ sí kọ̀ńpútà agbègbè tàbí tí a máa firánṣẹ́ síbòmíràn pẹ̀lú àdírẹ̀sì èdìdì tí a ṣé ìsúnkì, nígbà tí kò ti sí ní ààbò IPsec, ó ti di èdìdì IP lásan.
A máa ń lò ọ̀nà ìsípòpadà fi dáàbòbò bó àsopọ̀ kọ̀ńpútà méjì, àmọ́ a máa lò ọ̀nà –abẹ́lẹ̀ láàrin àwọn ojúàkànpọ̀ (alànà, ògiriná, VPN aládàáṣé.), àsopọ̀ àdáni aláfojúnúdá.

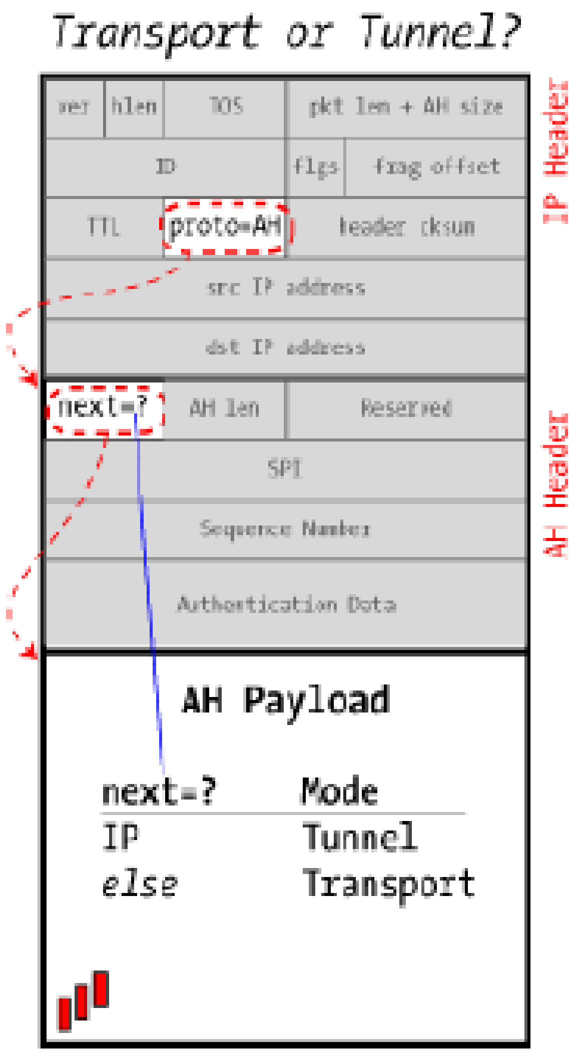
Ìṣípòpadà tàbí Ọ̀nà-abẹ́lẹ̀

Nínú IPsec nǹkan tí ń mú ìyàtọ wa láàrin ọ̀nà ìṣípòpadà àti ọ̀nà-abẹ́lẹ̀ ni ààyè “àtẹ̀lé” ti àkọsórí AH.
Nígbà tí IP bá wà ni ààyè “àtẹ̀lé” nínú àkọsórí AH, èyí á túmọ̀ sí wí pé ọ̀nà-abẹ́lẹ̀ ni, tí a sì ṣé ìsúnkì gbogbo èdìdì, tí àwọn àdírẹ́ẹ̀sì èbúté orísun yàtọ sí àdírẹ́ẹ̀sì ti IPsec ń lò.

Nígbà tí kìí ṣe IP ló wà ni ààyè “àtẹ̀lé” àkọsórí AH tó jẹ́ nǹka mì-ín bíi (TCP, UDP, ICMP,..), èyí á túmọ̀ sí pé ọ̀nà ìṣípòpadà tí ń dáàbòbò bó ìsopọ̀ ojú-́mì méjì.

Yálà tó jẹ́ ọ̀nà ìṣípòpadà tàbí ọ̀nà-abẹ́lẹ̀, orí àwọn èdìdì jẹ́ nǹkan kannáà, èyí tó túmọ̀ sí pé bákan náà ni ìfisọ̀nà àwọn èdìdì ṣe ń lọ gbà, làì jẹ́ pé a ń tú kòkò ọbẹ̀ dé ìsàlẹ̀.
A mọ̀ wí pé a ní láti lò kọ̀ńpútà fún ìṣípòpadà àwọn èdìdì ní ọ̀nà ìṣípopadà tàbí ọ̀nà-abẹ́lẹ̀, àmọ́ fún ìsopọ̀ kọ̀ńpútà méjì a ò lè lo ọ̀nà-abẹ́lẹ̀.

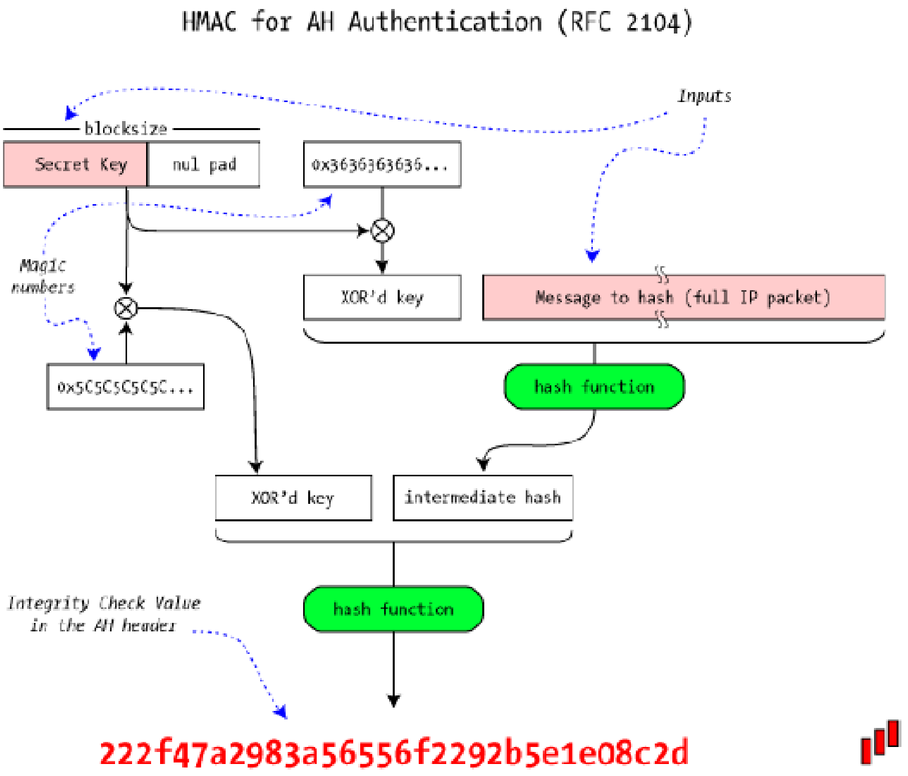
Ojú-àkànpọ̀ (Alànà, ògiri-iná) nìkan ni a máa ń lò fún ìṣípòpadà àwọn èdìdì ni ọ̀nà-abẹ́lẹ̀, àmọ́ a tún lè ṣàsopọ̀ kọ́pútà pẹ̀lú ojú-àkànpọ̀ nígbà ti a bá fẹ́ máa ṣàkósó àwọn àsopọ̀.

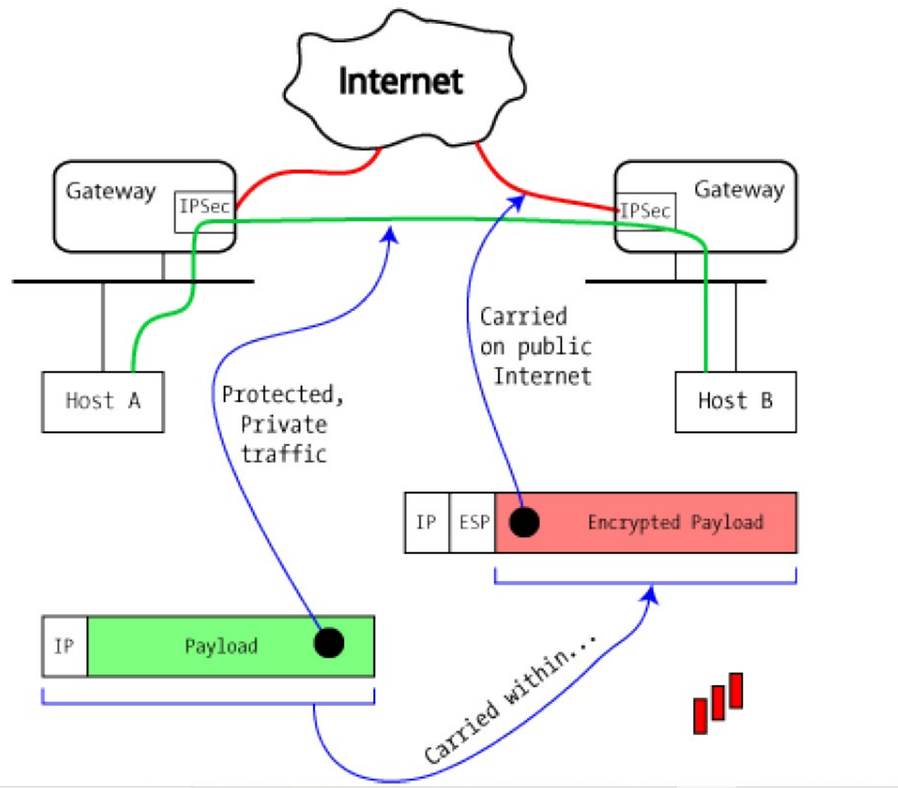


Alúgóríídíìmù ìfàṣẹsí

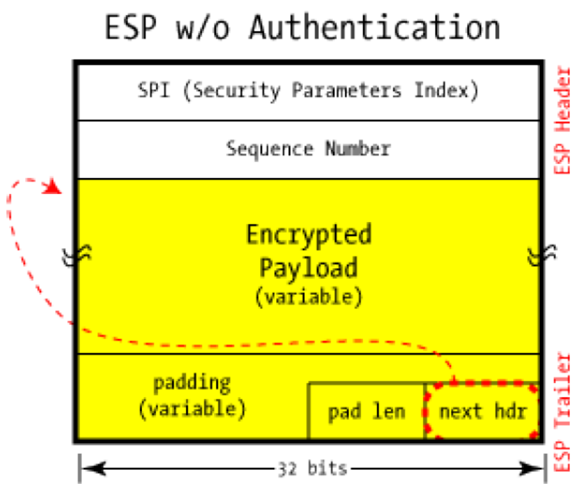
Ìfẹ́nukò AH ní nọ́mbà ìṣàyẹ̀wò ìsọfúnni pípé ní ààyè àwọn ìsọfúnni pípé àti ti ìfàṣẹsí tó wà ni àkọsórí. A máa sàbá ṣẹ̀dá nọ́mbà yìí pẹ̀lú alúgóríídíìmù ààké ìpàrokò bíi MD5 tàbí SHA-1 àmọ́ kìí ṣe ìgbà gbogbo.

Nígbà tí a bá lò àwọn àfikún àyẹ̀wò nìkan, a ò lè ní ààbò tó péye fi dójúkọ àwọn màdàrú ìmọ́mọ̀ṣe.
A máa lò àmì ìfàṣẹsí iṣẹ̀ẹ̀jẹ́ ààké (HMAC), pẹ̀lú nọ́mbà àṣírí nígbà ti a bá ṣẹ̀dá ICV. Ó ṣeé ṣe ki alátàkò ṣírò àgbéjáde ààké, àmọ́ nígbà tí kò bá ti mọ̀ nọ́mbà àṣírí,a á lè fún kó fi mọ̀ ICV (nọ́mbà àmì pípé ìsọfúnni).
Àwòrán ìṣàlẹ̀ máa ṣàlàyé bíi ti iṣẹ̀ẹ̀jẹ́ àti nọ́mbà ICV máa jẹ́ kí a dáàbòbò àwọn ìsọfúnni.


HMAC for AH Authentication (RFC 2104)
Inputs
blocksize
Secret Key
nul pad
0x3636363636...
Magic numbers
XOR'd key
Message to hash (full IP packet)
0x5C5C5C5C5C...
hash function
XOR'd key
intermediate hash
Integrity Check Value in the AH header
hash function
222f47a2983a56556f2292b5e1e08c2d



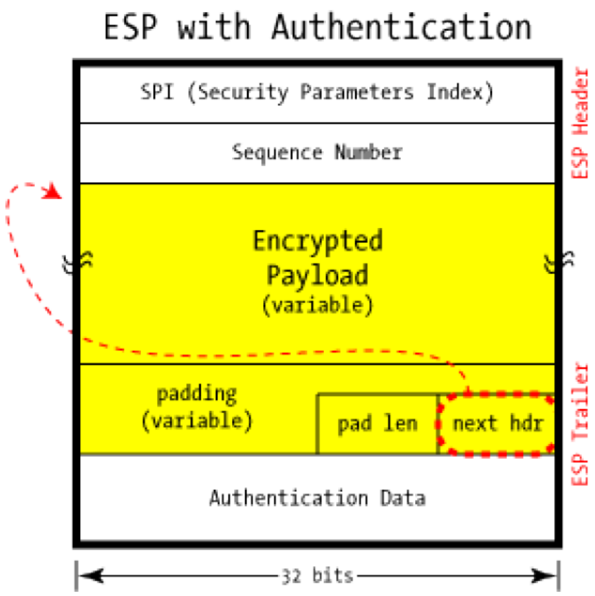
ESP Encapsulation ESP



1fikàn ìpàrokò máa jẹ́ kí ESP ní ìṣòro díẹ̀, nítorí pé ESP máa yìká àwọn ìsọ́fúnni tó wúlò, àmọ́ AH máa wà lórí.
ESP máa ní àwọn ààyè àkọsórí àtì àkọsísàlẹ̀ ti ẹ̀yàn ìfàṣẹsí àti ti ìpàrokò. A máa ń lò ESP lọ́nà ìṣípòpadà àti ọ̀nà-abẹ́lẹ̀. IPsec ò pa alúgórídíìmù kan láṣẹ, àmọ́ àwọn èyí ti a máa sàbá lò ni DES, trip-DES, AES àti Blowfish fún ìpàrokò àwọn ìwúlò ìsọfúnni.
SA (Security Association : Àsopọ̀ ààbò) nígbàkan ni jẹ́ kí a mọ̀ alúgórídíìmù tí a

lò pẹ̀lú kọkọrọ.
Ìyàtọ tó wà láàrin AH pẹ̀lú ESP ni pé ESP máa ń ṣàyíká ìwúlò ìsọfúnni pẹ̀lú ààbò.
Nígbà tí ìtọ́kasí àwọn ààtò ìdáàbòbò pẹ̀lú àwọn nọ́mbà àtòtẹ̀lé ń sisẹ́ kannáà bíi AH, àmọ́ àfikún àkọsórí àtẹ̀lé àwọn ìsọfúnni ìfàṣẹsí tí kò ṣe dandan ni àkọsísálẹ̀.

Ó ṣeé ṣe ká lò ESP làì ṣe ìpàrokò (fi lọ alúgórídíìmú òdo) tí á sì ní ètò kannáà pẹ̀lú èdìdì.
Àmọ́ kò wúlò, àṣà fi tí a bá so ó mọ́ ìfàṣẹsí ESP. Kò sí àǹfààní láti lò ESP làì sí ìpàrokò àti ìfàṣẹsí àfiu tí bá fẹ́ lò ó fi ṣé àwọn ìdànwó ìṣiṣẹ́ ètò.
Láti jẹ́ kí àwọn alúgóéídíìmù ìpàrokò tí lò ìṣùpọ̀, wọ́n a máa lò aṣàtopọ̀ tí gígùn ẹ wà ni ààyè len. Ààyè hdr máa fún wa ni irú ù IP, TCP, UDP...) ìwúlò ìsọfúnni tí a máa sàbá lò, bó tí lè jẹ́ pé o dári síwájú, nígbà tí ti AH dári sẹ́yìn.



Lẹ́yìn ìpàrokò, ESP lè ṣe ìfàṣẹsí bíi àyàn pẹ̀lú ìfẹnukó HMAC bíi ti AH.
Èyí tí ìfàṣẹsí ESP fi yàtọ sí ti AH ni pé ìfàṣẹsí yìí máa dúró lórí àkọsórí ESP àti àwọn ìwúlò ìsọfúnni àmọ́ kìí ṣe orí gbogbo àwọn èdìdì, síbẹ̀ síbẹ̀ ìfàṣẹsí yìí kò di agbára ìdáàbòbò kù, ó tún ní èrè tó pọ̀ ni.

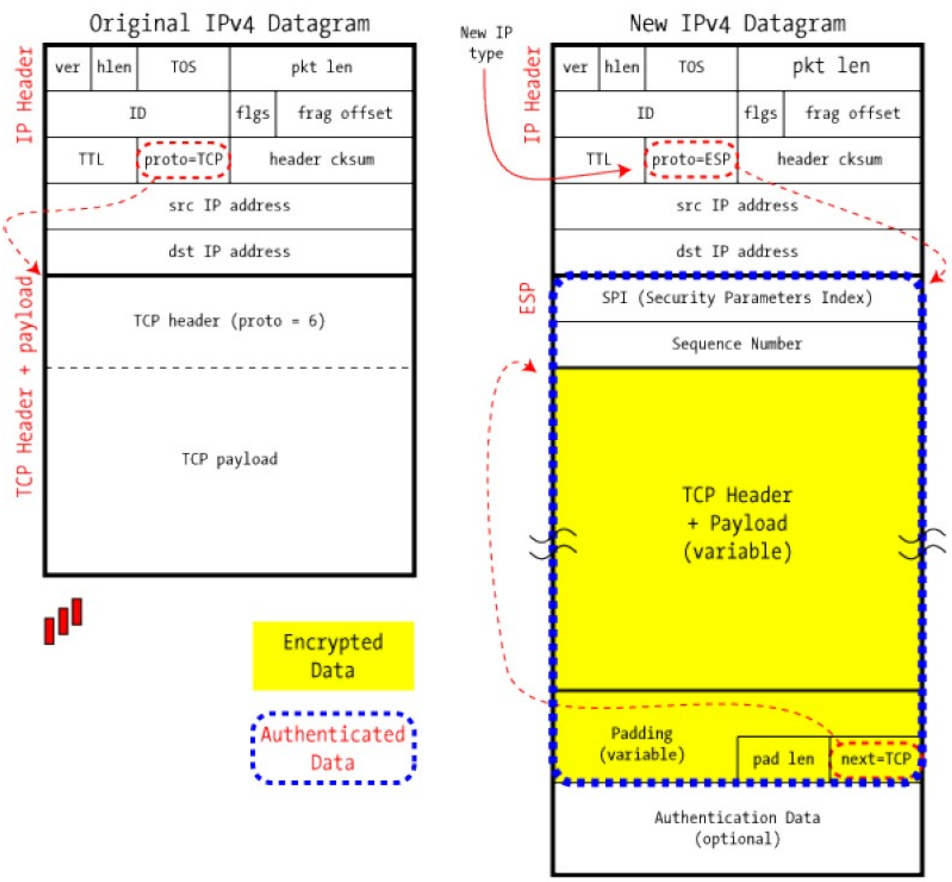
Ó máa sọ̀ro fún àjèjì tí ń ṣàyẹ̀wò èdìdì IP tó ní àwọn ìsọfúnni ESP láti fójúnu mọ́ nǹkan tó wà nínú èdìdì làì jẹ́ pé àwọn ìsọfúnni IP tó ti mọ̀ bíi (àdírẹ́ẹ̀sì orísun, àdírẹ́ẹ̀sì èbúté IP) ó máa mọ̀ pé àwọn ìsọfúnni ESP ni, nítorí pé ó wà nínú àkọsorí, àmọ́ ìwúlò ìsọfúnni ti wa ni ìpàrokò.

Nígbà tí bá ṣàyẹ̀wò èdìdì yìí, a ò lè mọ̀ tí àwọn ìsọfúnni ìfàṣẹsí bá wà tàbí tí wọ́n bá sí. A máa mọ̀ tí a bá lò àwọn ìtọ́kasí ààtò ààbò ti a pín àti alúgóridíìmù àsopọ̀.

Ó yẹ kí a ṣàkíyèsí pé àpò yìí máa tọ́ka sí àwọn nǹkan mì ín ti àwọn ìsọfúnni tó wúlò kìí ṣe. A máa fi QoS sínú àkọsórí kí a lè mọ́ àwọn ìgbì IP tó jẹ́ ti fóònù ayélújára, nítorí lóde oníì, àwọn èèyàn púpọ̀ ń fi irúfẹ́ àwọn fóònù wọ̀nyìí sínú ESP. Ó yẹ kí a mọ̀ ìgbì èdìdì tó jẹ́ Voip (ìṣíwájú IP 3) ti ìgbì RTP (ìfẹnukò tó jẹ́mọ àsìkò) (ìṣíwájú IP 5) kìí ṣé nǹkan tó dájú, àmọ́ ó lè jẹ́ ìtọ́sọ́nà nígbà mì ín.

ESP ni Ọnà ìṣípòpadà

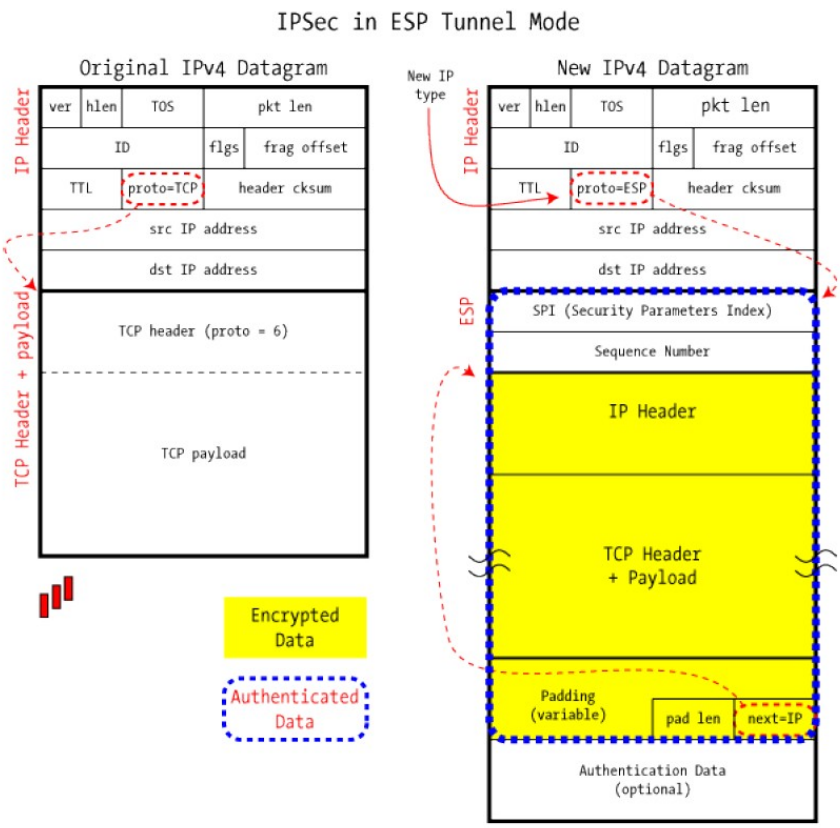
Bíi ti AH àwọn ìsọfúnni tó wúlò nìkàn ni a máa ń súnkì, nítorí ìjùmọ̀sọ̀rọ̀ láàrin kọ̀ńpútà méjì ni a fi gbékalẹ̀, a kìí fọwọ́ kan àkọsórí IP (lẹ́yìn ààyè ifẹnukò tí a máa pàrọ) èyí túmọ̀ sí pé a kìí fọ́wọkan àwọn àdírẹ́ẹ̀sì orísun àti ti èbúté.



ESP ni Ọnà-abẹ́lẹ̀

VPN ni kí a ṣe ìpàrokò àsopòkan, tí a bá ń sọ̀rọ̀ IPsec nǹkan ti a máa rò ni pé àsopọ̀ ti a pàrokò ni, àmọ́ a ní láti fi ìfàṣẹsí fi kun ún. A máa ṣàlàyé gbogbo ní wájú.
Ìyàtọ tó wà láàrin AH àti ESP ni : Tí èèyàn bá ń wò àwọn èdìdì AH ti ń kọjá, ó

máa mọ̀ tó bá jẹ́ ìgbì ọ̀nà ìṣípopadà tàbí ti abẹ́lẹ̀, ti ìgbì ESP kò jẹ́ bẹ̀ẹ̀ nítorí àkọsórí (next = IP) wà ni ìpàrokò pẹ̀lú àwọn ìsọfúnni tó kù, ẹni tí kò bá kájú ẹ ò lè mọ̀.



Àpapọ̀ : Ìgbékalẹ̀ ojúlówó VPN

A ti ṣétán láti gbé ojúlówó VPN kalẹ̀ pẹ̀lú ìbòjú pátápátá àkọsórí ìfàṣẹsí àti àwọn ìwúlò ìsọfúnni tí a ṣèsúnkì wọn. Àǹfààní àsopọ̀ méjì agbègbè tó dájú pẹ̀lú àsopọ̀ tí kò fini lọ̀kan balẹ̀, bíi èyí tó jẹ́ wí pé a so àwọn àsopọ̀ agbègbè méjèjì pẹ̀lú wáyà. A máa sàbá lò ó fún ìsọpọ̀, àwọn ẹ̀ka ibiṣẹ́ mọ́ olú ibiṣẹ́.

Ojúlówó VP

N ní láti lò ìfàṣẹsí àti ìpàrakò ESP nìkan ni a máa ṣe ìpàrokò, àmọ́ ESP àti AH máa ṣe ìfàṣẹsí : èwo ni a máa mu ?

Èyí ti a lè ṣé ni kí a ṣèsúnkì ESP sínú AH, àmọ́ agbára AH ò lè débẹ̀, bíi àpẹẹrẹ tí a bá lò AH + ESP , ọ̀nà-abẹ́lẹ̀ yìí kò lè dá kọ̀ńpútà pẹ̀lú NAT kọjá.

Nígbà tí kò sọ̀nà níbẹ̀, a máa lò ESP + Auth ni ọ̀nà abẹ́lẹ̀ fi ṣèsúnkì gbogbo ìsọfúnni fi gbanu àsopọ̀ tí kò fini lọ̀kàn balẹ̀, tí á sì ṣe ìfàṣẹsí àti ìpàrokò àwọn ìsọfúnni.

Àwọn ààbò tí a ṣègbékalẹ̀ lọ́nà yìí máa jẹ́ kí àwọn ajalélókun má rí àwọn

ìsọfúnni tí ń kojá jù kí wọ́n mọ̀ pé VPN ni. Àwọn alátàkò ò lè rí àwọn ìsọfúnni àti àwọn ìfẹnukò tí a súnkì bíi TCP, UDP, tàbí ICMP.

Nǹkan tó dára ni ọ̀nà-abẹ́lẹ̀ ni pé : Àwọn kọ̀ńpútà aṣojú, wọ́n ò mọ̀ nǹkan kan sórí VPN tàbí àwọn àbò mì-ín.

Láti ìgbà ti ẹ̀rọ ojú-akànpọ̀ tí ń lọ VPN bíi ojú-akànpọ̀, àwọn alátagbà tí ń lọ sí èbúté kèjì máa lọ dáadáa.
Èdìdì kan nínú èdìdì omiì máa wáyé ni ìpele tó pọ̀. Aṣojú A àti aṣojú B l ṣàgbékalẹ̀ àsopọ̀ wọn pẹ̀lú ìfàṣẹsí AH ti wọ́n sì gbélọ pẹ̀lú VPN. A máa gbé èdìdì AH sínú èdìdì ESP + Auth tí a sì bó gbogbo ẹ.
Ó di dandan kí a lò ìfàṣẹsí tí a bá ti lò ìpàrokò, ìlò ìpàrokò nìkan, kìí dá alátàkò dúró, bíi àkọsílẹ̀ lórí ìpàrokò.

Àwọn onírúurú nǹkan
IPsec jẹ́ àwọn ìfẹnukò tó ní àwọn nǹkan ìṣòro púpọ̀, àmọ́ díẹ̀ ni a máa múlò. Nínú ẹ̀kọ́ yìí a máa lò àwọn mélòó kan.

Àsopọ̀ ààbò àti SPI
Nígbà tí a bá ṣàsopọ̀ ojú-àmì méjì tàbí ojú-àkànpọ̀ lọ́nà ààbò o di dandan kí a pín àṣíẹ́ fi béèrè ìfàṣẹsí tàbí kí a lò alúgóridíìmù ìpàrokò. Ọ̀nà wo ni a máa gbà fi pín àṣírí ? a máa ri níwájú.
Nígbà tí èdìdì IPsec (AH tàbí ESP) bá dé ojú-àkànpọ̀ , báwo ni ó máa mọ̀ àwọn ààtò tó somọ́ (kọkọrọ, alúgóridíìmù, àti ètò) aṣojú kan lè ní ìtákurọ̀sọ púpọ̀ pẹ̀lú àwọn ìṣàkósó kọkọrọ àti alúgóridíìmù, báwo ni ó ṣeé ṣe.

SADB máa lò irú ìfẹnukò àti SPI fi yàn ìwọlé kan, àmọ́ kìí ṣe àdírẹ́ẹ̀sì IP.
yí máa jẹ́mọ ọ̀nà ti a fi ṣàgbékalẹ̀ ìsopọ̀ pẹ̀lú olórí tàbí ọ̀nà agbára.
Àsopọ̀ ààbò (SA) ni ó máa ṣàlàyé pẹ̀lú àwọn ààtò ìsopọ̀ tó jẹmọ ìsopọ̀ náà, ẹ́yà kan lè ní (SA) mélòó kan.
Nígbà tí èdìdì kan bá dé, àwọn ohun mẹ́ta ni a máa lò fi mọ̀ SA tó somọ́ nínú àkójọpọ̀ àwọn SA (SADB) :

- Àdírẹ́ẹ̀sì IP èyà náà
- Ìfẹnukò IPsec (ESP tàbí AH)
- Àwọn ààtò atọ́kasí ààbò

A lè fi àwọn nǹkan mẹ́tẹ̀ta wọ̀nyìí wé ìdìmú òkèrè, tó somọ́ àdírẹ́ẹ̀sì IP, ìfẹnukò àti nọ́mbà ojú-àkànpọ̀. Àsopọ̀ ààbò máa ń wà lórí ìdarí kan, àsopọ̀ ẹ̀yà máa ní ìdarí méjì, àwọn ìfẹnukò (AH + ESP) ni SA kọ̀ọ̀kan ní gbogbo ètí túmọ̀ sí pé VPN ní SA mẹ́rin tíì lápàpọ̀ tí a kó pamọ sínú ìkójọpọ̀ àwọn SA (DBSA).

Àwọn ìsọfúnni pọ̀ nínú SADB, àmọ́ díẹ̀ kan ni a lè múlò.

- Alúgórídíìmù ìfàṣẹsí AH
- Àsírí ìfàṣẹ́sí AH
- Alúgórídíìmù ìpàrokò
- Kọkọrọ àṣírí ESP
- Ìfàṣẹsí tó ṣeé ṣe pẹ̀lú ESP bẹ́ẹ̀ ni / bẹ́ẹ̀ kọ
- Àwọn ààtò pàṣipàárọ kọkọrọ
- Ìdíwọ̀n ìfisọ́nnà
- Ètò aṣẹ́ àwọn IP

Àwọn àgbékalẹ̀ kan máa fún wa ni àǹfààní láti ṣàtúntò àwọn àkójọpọ̀ ètò.

Àkóso kọkọrọ

A máa rí ní ṣókí ẹ̀kọ́ àkóso kọkọrọ , ẹ̀kọ́ yìí ní ìṣòro, ìfẹnukò àti ẹ̀yàn tó pọ̀. A máa ṣàlàyé wọn nínú àwọn àkọ́ọ́lẹ̀ niwájú, àmọ́ bẹ́ẹ̀ ni a ò lè kọ́ gbogbo ẹ níbi.

IPsec ò lè wúlò jù bẹ́ẹ̀ lọ tí kò bá sí àgbékalẹ̀-ètò ìpàrokò àti ti ìfàṣẹsí. Èyí túmọ̀ sí pé a á lò kọkọrọ tí àwọn olùmúlò nìkan mọ̀ tí kò jẹ́ mímọ́ fún ẹlòmìí.
Àmọ́ ilànà yìí ò tẹ̀ síwájú kò sí ṣe gbọ́kan lè.
Nígbà tí a ti lè gbé kọkọrọ àṣírí gbanu àsopọ̀, èwu ti wà. Nínú àwọn àsopọ̀ pẹ̀lú àwọn ẹ́rọ kọ́ǹpútà tó pọ̀, tí a ń fi àwọn kọkọrọ tó jọra ránṣẹ́, àwọn kọkọrọ wọ̀nyìí lè bàjẹ, èyí máa fún wa ni iṣẹ́ fikun tí ò sí máa di wa lọ́wọ́.

IKE (Inteẹnet key Exchange : Pàṣipàárọ kọkọrọ ínténẹ́ẹ̀tì) máa ń fún àwọn ẹ̀rọ kọ́ǹpútà méjì láǹfààní láti se ìgbékalẹ̀ àsopọ̀ ààbòwọn pẹ̀lú àwọn àṣírí ti wọ́n fẹ lò.
IKE máa lò ìfẹnukò ISAKMP (Internet Security Key Management Protocol : Ìfẹnukò àkóṣo kọkọrọ Àsopọ̀ ààbò íntẹ́nẹ́ẹ̀tì) fún ìgbékalẹ̀ àsopọ̀ ààbò tó dọ́gba pẹ̀lú àwọn ẹ̀yà méjèjì.
IPsec máa ń lò àwọn ìfẹnukò pàsipààrọ̀ kkọkọrọ púpọ̀, Oakley ni a ń lò gan an, ojú-àkànpọ̀ 500/udp ni ń lò.