عنوان مقاله : پروتکل امنیت در لایه شبکه IPSec

گروه مطالعاتی : امنیت

گروه کاری : امنیت

ارائه دهنده:سید محمدحسینی

تاریخ ارائه: ۸۳/۱۱/۱۳

سرپرست گروه کاری: طیبه میرزائی

تاریخ اصلاح: ۸۳/۱۲/۱۵

اصلاح کننده : سید محمدحسینی

مرجع: ۱-Cryptography and Public Key Infrastructure on the Internet
by:Klaus Schmeh
press:wiley 2001

۲-اسلایدهای آموزشی مرکز امنیت شبکه شریف

۳- اینترنت

بخش اول:پروتكل امنيت در لايه شبكه IPSec

مقدمه

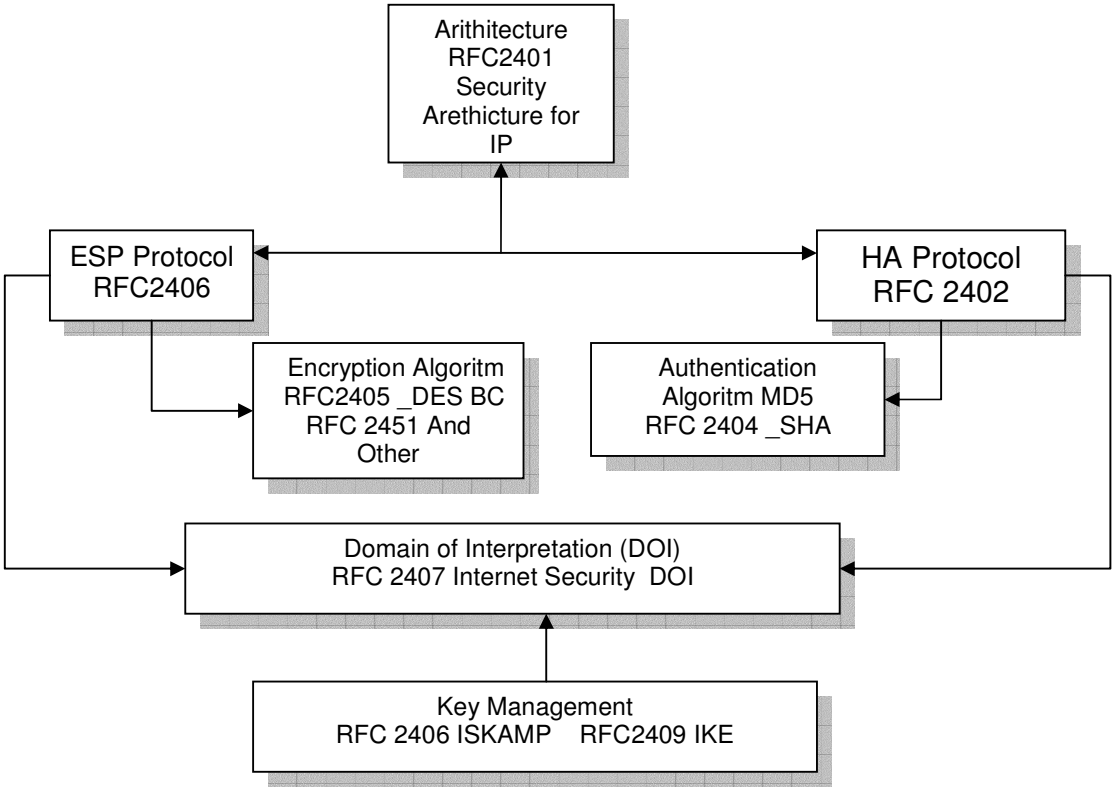
در پشته پروتكل TCP/IP هر لايه داراي يک يا چند پروتكل مي با شد كه هر پروتكل وظيفه خاصي را در آن لايه انجام مي دهد, بر همين اساس جهت ايجاد امنيت هر لايه بنا به اصول طراحي زير پروتكلها ، يک يا چند پروتكل امنيتي تعبيه شده است.مطابق اصول طراحي زير لايه هر لايه وظيفه اي را بر عهده دارد كه منحصر بفرد مي باشد و در هر لايه نيز هر پروتكل مي تواند بنا به قرارداد عمليات خاصي را برعهده بگيرد .بر همين اساس امنيت در لايه شبكه بر عهده IPSec مي باشد. از اين پروتكل بطور وسيعي درشبكه هاي مجازي خصوصي[1] VPN براي دفاتر مربوط به يک شركت يا سازمان و اساساً ايجاد ارتباط امن بين دو يا چند سازمان بكار ميرود . امنيت شبكه هاي مجازي خصوصي(VPN) از چندروش امكان پذير مي باشد كه عبارت اند از استفاده از ديواره آتش ، AAA Server ,IPsec و كپسوله سازي. اما روش IPsec به علت امن بودن ، پايداري بالا ،ارزان بودن ،انعطاف پذير بودن و مديريت بالا، مورد توجه قرار گرفته است. اين پروتكل شامل مباحث :

- سرآيند احراز هويت[2]:كه بحث پيرامون فرمت بسته ها و مسائل عمومي مربوط به استفاده از AH براي احراز هويت بسته مي پردازد.
- الگوريتم رمزنگاري[3] :كه به نحوي رمزنگاري هاي مختلف در ESP مي پردازد.
- الگوريتم احراز هويت كه نحوه استفاده از الگوريتمهاي احراز هويت مختلف در ESP , AH (اختياري) را بيان مي دارد.
- مديريت كليد [4] :كه به مسائل مربوط به مديريت كليد مي پردازد.
- ارتباط بين دامنه اي [5]: يا مطالب مربوط به ارتباط بين قسمت هاي مختلف مانند شناسه هاي استفاده شده براي الگوريتم ها و پارامترهايي از قبيل طول عمر كليد.

پروتكل IPSec خود شامل اجزاء تشكيل دهنده قراردادها و نحوي تامل بين آنهاست. در شكل ۱ ارتباط بخشهاي مختلف اين قرارداد نمايش داده شده است.

---

[1] - Virtal Private Network
[2] – Authentication Header(AH)
[3] – Encryption Algorithm
[4] - Key Management
[5] - Domain of Inter Predation



شكل ١.معماري پروتكل IPSec و نحوي تامل اجزاء آن

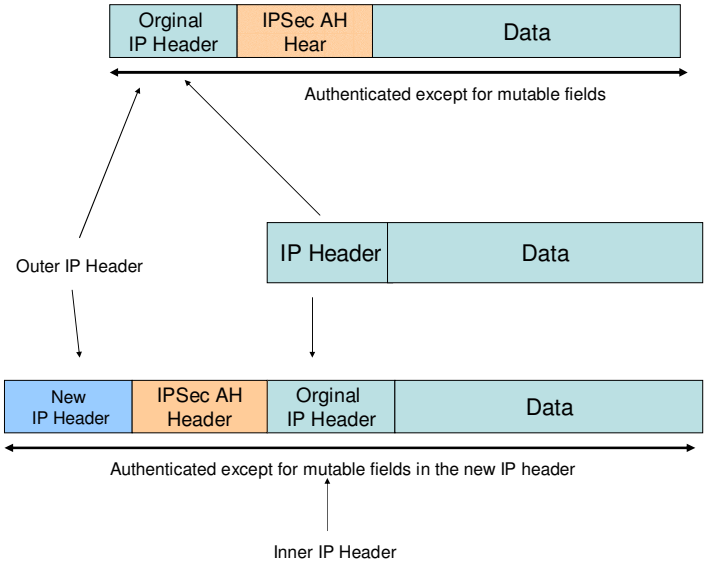
در پروتكل IPSec سرويسهاي امنيتي در دو قرارداد AH , ESP تدارک ديده شده اند .اين سرويسهاي امنيتي شامل_ :كنترل دسترسي[٦] ،تماميت[٧] ، احراز هويت مبدا داده[٨] (Data Drigin) ، رد بسته هاي دوباره ارسال شده[٩] ، محرمانگي[١٠] ، محرمانگي جريان ترافيك بصورت محدود خواهند بود.
اين سرويسها در سه نوع تركيب IPSec ارتباط فراهم آمده اند:
پروتكلهاي AH , ESP فقط بصورت رمزنگاري (Encryption) و ESP بصورت Encryption و احراز هويت (Authentication).

IPSec يك پروتكل توسعه يافته روي پروتكل IP است كه جهت امنيت IP تهيه شده است. اين پروتكل از دو پروتكل AH و ESP براي اطمينان بيشتر روي احراز هويت،تماميت داده ها(سلامت داده) و محرمانگي استفاده مي كند. اين پروتكل مي تواند،هم امنيت درلايه شبكه و هم امنيت در پروتكلهاي لايه بالاتر در حالت Transport Mode را برقرار سازد. اين پروتكل از دو حالت Tunnel و Transport جهت **اعمال سرويسهاي امنيتي استفاده مي كنند، يعني براي امنيت لايه شبكه از حالت** mode

---

[٦] – Access Control
[٧] - Integrity
[٨] – Data Driving Authentication
[٩] – Anti Replay
[١٠] - confidentially

Tunnel استفاده مي كند و براي امنيت لايه هاي بالاتر از حالت انتقال يا mode Transport استفاده مي نمايد.
درحالت Tunnelling ؛ديتاگرام IP بطور كامل توسط ديتاگرامIP جديدي كپسوله شده و آنرا براي پروتكل IPSec بكار مي برد. ولي در حالت Transport فقط payload ديتاگرام بوسيله پروتكل IPSec فيلد سرآيند IPSec و سرآيندIP و فيلدهاي لايه هاي بالايي درج (inserting) مي شود.مطابق شكل١ اين دو حالت به نمايش در آمده است.



شكل٢. حالت انتقال و تونل

مزاياي حالت Tunnel اين است كه آدرسها معمولاً آدرس Gateway هاست كه پس از بازگشايي آدرس واقعي بدست مي آيد و اين موضوع از حملات شبكه جلوگيري مي كند و مزيت دوم آن است كه بسته بيروني، يك بسته IP همانند بقيه بسته هاست و قابليت مسيريابي دارد.
اما در حالت Transport احراز هويت بصورت مستقيم بين Server و سرويس گيرنده (Client)توسط كليد متقارن مشترك انجام ميگيرد وبسته بيروني هم كپسوله شده و امن مي گردد. در اين حالت كه الزاماً دو كامپيوتر در يك LAN قرار ندارند. اما در حالت Tunnel، سرويس گيرنده هويت خود را به Gateway اثبات مي كند. در هر دو روش هر يك حالت خودشان (Transport mode Munnel mode) را از طريق SA استخراج كرده و مورد استفاده قرار مي دهند.

حالت های انتقال و تونل در AH

قرارداد AH در بسته IP براي حفاظت ازتماميت داده هاي تبادلي ديتاگرام IP ، IPSec از كدهاي هَش احراز هويت پيام hash[١١] (HMAC) استفاده مي كند. براي استفاده از HMAC،پروتكلهاي IPSec از الگوريتم هاي hash ؛SHA براي محاسبات

[١١]- Hash Message Authentication Code

يك hash مبنا روي يك كليد سري(secret key) و محتويات ديتاگرام IP استفاده مي كند.بنابراين اين كدهاي هش احراز هويت پيام hash هم در سرآيند پروتكل IPSec و هم در پكت هاي دريافتي كه بتواند اين كدها را چك نمايد كه در واقع مي تواند به كليد سري دسترسي داشته باشد،قرار مي گيرد. براي ارائه سرويس محرمانگي ديتاگرام IP ،پروتكلهاي IPSec از استانداردهاي الگوريتم رمزنگاري متقارن[۱۲] استفاده مي كنند. IPSec از استانداردهاي NULL ، DESاستفاده خواهد كرد. امروزه معمولاً يكي از الگوريتم هاي قوي مثل Blowrfish AES,3DES , را بكار مي برد.

IPSec براي دفاع وحفاظت از تهاجمات داده هاي تبادلي(Deinal of services) ،از روش پنجرة اسلايدي sliding windows استفاده مي كند. در اين روش هر پكت يك شمارة توالي[۱۳] را به خود اختصاص مي دهد و اگر عدد آن پكت به همراه يك windowsيا newer درست شده باشد، در اين صورت پكت قديمي بلافاصله دور انداخته (dispatched) مي شود(اين روش همچنين براي حفاظت از تهاجمات ميانه راه پاسخ[۱۴] نيز دوباره بكار مي آيد يعني حفاظت از مهاجماني كه پكت هاي اصلي را ثبت كرده و بعد از چند لحظه تأخير و احتمالاً تغيير دادن آن، ارسال مي دارند.

براي كپسوله كردن و بازگشائي اين يک پكت كپسوله شده ، با استفاده ازروشهاي ذخيرة سازي، كليدهاي سري،الگوريتم هاIP و آدرسها درگير در تبادلات اينترنتي را ذخيره نمايند و بكار ميگيرد. همة اين پارامترهاي مورد نياز جهت حفاظت ديتاگرامIP درجايي بنام مجمع امنيتي يا SA ها ذخيره مي شوند. اين مجمع امنيتي به نوبت در پايگاه دادة مجمع امنيتي[۱۵] يا (SAD) ذخيره مي شوند.

مجمع امنيتي (SA) داراي سه پارامتر يگانه (يكتا-يكه) است كه شامل :

۱- شاخص پارامتر امنيت (Security Parameter Index): اين پارامتر ۳۲ بيتي ارزش محلي داشته. اين پارامتربهمراه ESP , HA حمل مي شود تا سيستم دريافت كننده بتواند SA مربوط به آن را انتخاب نمايد.

۲- مشخصه پارامتر امنيت[۱۶] (security Parameter Identifier) :اين پارامتر نوع پروتكل امنيتي SA را تعيين مي كند، AH يا ESP طبيعتاً اين مشخصه بطور همزمان هر دو پروتكل را بهمراه ندارد.

۳- آدرس مقصد IP : ، اين آدرس اساساً آدرس يك نقطه انتهايي يا يك شبكه (روتر، حفاظ) خواهد بود.

با اين تفاصيل، بطور كاملترو ريزتر مجمع امنيتي يا SA شامل اطلاعات و پارامترهاي زير است:

۱- آدرس مبداءو مقصد مربوط به سرآيند IPSec.اينها IP آدرسهاي پكت هاي نظير به نظير مبداء و مقصد حفاظت شده توسط IPSec مي باشند.

۲- الگوريتم و كليد سري بكار برده شده در IPSec (ESP Information و AH. (Informantion

---

[۱۲] – Symmetric Encryption Algorithm

[۱۳] - sequance number

[۱۴] – The– of- middle Response Attach–

[۱۵] – security association database

[۱۶] - security Parameter Identifier

برخي پايگاه ذخيره سازي SA ها،اطلاعات بيشتري را نيز ذخيره مي كنند كه شامل:
۳- حالت هاي اصلي انتقال بستهIPSec(TransportياTunnel)
٤- اندازه Sliding windows جهت حفاظت از تهاجمات بازگشتي (replay attach)
٥- زمان حيات[۱۷] SA ها .فاصله زماني است كه پس از آن SA بايد پايان يابد يا باSA جديدي عوض شود.
٦- حالت ويژه پروتكل IPSec كه در اين پارامتر علاوه بر حالتهاي Transport , Tunnel ، حالت wildcard نيز مشخص مي شود.
9-Sequence Number counter كه يك پارامتر ۳۲ بيتي كه در سرآيند ESP,AH بعنوان فيلد شمارة سريال قراردارد.
10-Sequence counter overflow يك شمارشگر كه سرريز در شماره سريال را ثبت مي كند و تعيين اينكه بسته هاي بعدي SA ارسال شود يا خير؟
۱۱-Path Maximum Transportion limit يا ماكزيمم بسته اي كه در مسير قابل انتقال است.

از آنجائيكه IP آدرس مبدأ و مقصد توسط خود SA ها تعريف مي شوند. حفاظت از مسير دو طرفه كامل IPSec بطور مستقيم فقط براي يك طرف امكان پذير خواهد بود. براي اينكه بتوانيم حفاظت هر دو طرف را انجام دهيم نيازمند دو مجمع امنيتي غير مستقيم[۱۸]خواهيم بود. SA ها فقط چگونگي حفاظت توسط IPSec را تعريف مي كنند:
اطلاعات مقررات امنيتي راجع به هر پكت در مقررات امنيتي[۱۹](sp) تعريف شده است كه در پايگاه ذخيره كنندة مقررات امنيتي[۲۰] (SPD) ثبت ونگهداري مي شود.
SP يامقررات امنيتي شامل اطلاعات زير است:
۱- آدرس مبدأ و مقصد پكت هاي حفاظت شده. در حالت Transport اين آدرسها درست همان آدرسهاي مبدأ و مقصد SA است.
۲- پروتكل و پورت حفاظت شده . برخي IPSec ها اجاره نمي دهند يك پروتكل به خصوص حفاظت شود. در اين حالت تمام تبادلات ارسال و دريافت بين IP آدرسهاي ذكر شده حفاظت مي شوند.
۳- مجمع امنيتي(SA)[۲۱] براي حفاظت پكت ها مورد استفاده قرار مي گردد.
تنظيم دستي SA ها همواره دچار خطا و بي دقت است. از سوي ديگر كليد سري و الگوريتم هاي رمزنگاري مابين همه نقاط شبكه اختصاصي مجازي (VPN) بايد به اشتراك گذاشته شود. به خصوص براي مديران سيستم , تبادل كليد مسئله بحراني خواهد كرد. بطور مثال اينكه چطور مي توانيم تشخيص دادهيم هيچ عمليات رمزنگاري انجام نمي شود تا در آن هنگام تبادل كليد متقارن سري انجام گيرد يكي از همين مسائل است.براي حل اين مشكل پروتكل تبادل كليد اينترنت[۲۲](IKE) پياده سازي شده است . اين پروتكل احراز هويت، براي نقاط نظير

---

[۱۷] life time-
[۱۸] indirection -
[۱۹] Security Policy –
[۲۰] Security Policy Database – -
[۲۱] Security Association–
[۲۲] Internet Key Exchange -

اولين گام خواهد بود. دومين گام ايجاد SA و كليد سري متقارن جهت انتخاب و بكارگيري كلي تبادلي ديفن هيلمن[۲۳] خواهد بود.پروتكلIKE براي اطمينان از محرمانگي بطور دوره اي بدقت كليد سري را دوباره دريافت مي دارد.

پروتكلهای IPSec

خانواده پروتكل IPSec شامل دو پروتكل است. يعني سرآيند احراز هويت(۱) يا , ESP AH هر دوي اين پروتكل ها از IPSec مستقل خواهد بود.

پروتكل AH

بطور خلاصه پروتكل AH در واقع تأمين كنندة سرويسهاي امنيتي زير خواهد بود:
۱.تماميت دادهء ارسالي
۲.احراز هويت مبدا داده ارسالي
۳.رد بسته هاي دوباره ارسال شده
اين پروتكل براي تماميت داده ارسالي از HMAC استفاده ميكند و براي انجام اين كار مبناي كارش را مبتني بر كليد سري قرار مي دهد كه playload پكت و بخشهايي تغيير ناپذير سرآيند IP شبيه IP آدرس خواهد بود. بعد از اينكار اين پروتكل سرآيند خودش را به آن اضافه مي كند در شكل۳ زيرسرآيند ها و فيلدهاي AH نمايش داده شده است.

Next Heuder	Payload length	Reseved
SPI(Security Parameter Index)		
Replay Ddfense (Sequence Number)		
Hash Message Authentication code		

شكل۳.پروتكل AH در لايه شبكه

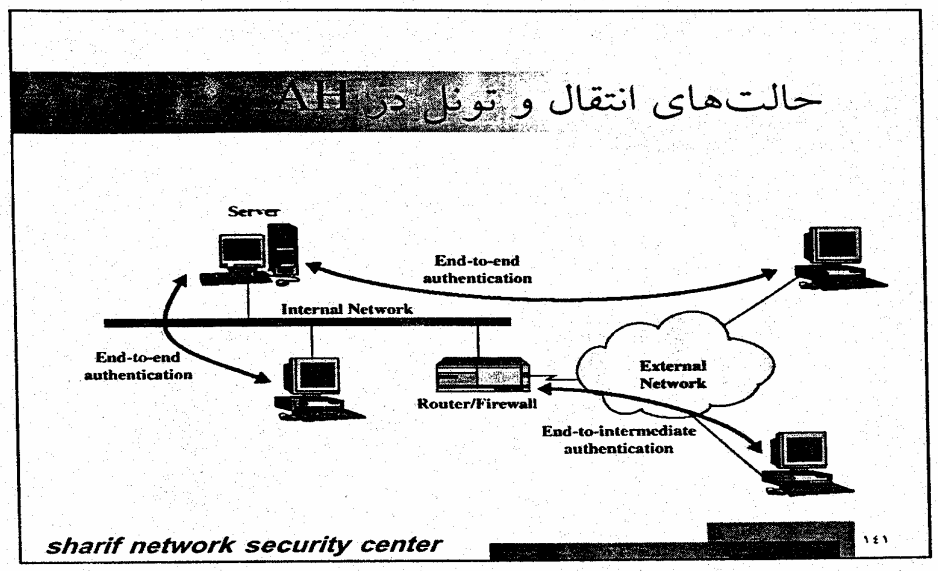
سرآيند AH،۲٤ بايت طول دارد. حال به توضيح فيلدهاي اين پروتكل مي پردازيم.
۱. اولين فيلد همان Next Header مي باشد. اين فيلدحالتهای بعدي را تعيين مي كند. در حالت Tunnel يک ديتاگرام كامل IP كپسوله مي شود

[۲۳]- Diffle – Hellman key exchange

۲. بنابراين مقدار اين فيلد برابر ٤ است. وقتي كه كپسوله كردن يك ديتا گرام TCP در حالت انتقال(Transport mode) باشد، مقدار اين فيلد برابر ٦ خواهد شد
۳. . فيلدpayload langht همانطوريكه از نامش پيداست طول payload را تعيين مي كند.
٤. فيلد Reserved از دو بايت تشكيل شده است.براي آينده در نظر گرفته شده است.
۴.فيلد Index security parameter يا SPI از ۳۲ بيت تشكيل شده است. اين فيلد از SA تشكيل شده كه جهت باز كردن پكت هاي كپسوله شده بكار مي رود. نهايتاً ٩٦ بيت نيز جهت نگهداري احراز هويت پيام Hash يا (HMAC) بكار مي رود.
۵ HMAC حفاظت تماميت دادهء ارسالي را برعهده دارد. زيرا فقط نقاط نظير به نظير از كليد سري اطلاع دارند كه توسط HMAC بوجود آمده و توسط همان چك ميشود.

چون پروتكل HA حفاظت ديتاگرام IP شامل بخشهاي تغيير ناپذيري مثل IP آدرسها نيز هست، پروتكل HA اجازه ترجمه آدرس شبكه را نمي دهد. NAT يا ترجمه آدرس شبكه در فيلد IP آدرس ديگري (كه معمولاً IP آدرس بعدا مي باشد) قرار مي گيرد. وبه اين جهت تغيير بعدي HMAC معتبر نخواهد بود.

در شكل ۴ حالتهاي انتقال و تونل در پروتكل AHبه نمايش در آمده است.همان طور كه مي بينيد اين پروتكل در اين دو حالت ارتباط امن بين دو نقطه انتهائي كه در دو شبكه مجزا قرار دارند را فراهم مي آورد ،همچنين ارتباط امن بين دو نقطه در يک شبكه داخلي و يک نقطه انتهائي و يک مسير ياب يا حفاظ ديواره آتش(FireWall) را ممكن مي سازد.



شكل ۴ حالتهاي انتقال و تونل در پروتكل AH

پروتكل ESP (Encaprolation Security Payload)

پروتكل ESP سرويسهاي امنيتي زير را ارائه مي كند:
١.محرمانگي
٢.احراز هويت مبدا داده ارسالي
٣.رد بسته هاي دوباره ارسال شده
در واقع پروتكل ESP هم امنيت تماميت داده (سلامت داده هاي ارسالي) پكت هايي كه از HMAC استفاده مي كنند را تامين كنيد و هم محرمانگي از طريق اصول رمزنگاري[٢٤] بكار گرفته شده .بعد از رمزنگاري پكت و محاسبات مربوط به HMAC ، سرآيند ESP محاسبه و به پكت اضافه مي شود. سرآيند ESP شامل دو بخش است كه مطابق شكل ٥ نمايش داده شده است.

<table>
<tr><td colspan="4">Security Parameter Index (SPI)</td></tr>
<tr><td colspan="4">Sequence Number (Ready Defense)</td></tr>
<tr><td colspan="4">Initialization Vector (IV)</td></tr>
<tr><td colspan="4">Data</td></tr>
<tr><td></td><td>Padding</td><td>Padding Length</td><td>Next header</td></tr>
<tr><td colspan="4">Hash Massage Authentication Code (HMAC)</td></tr>
</table>

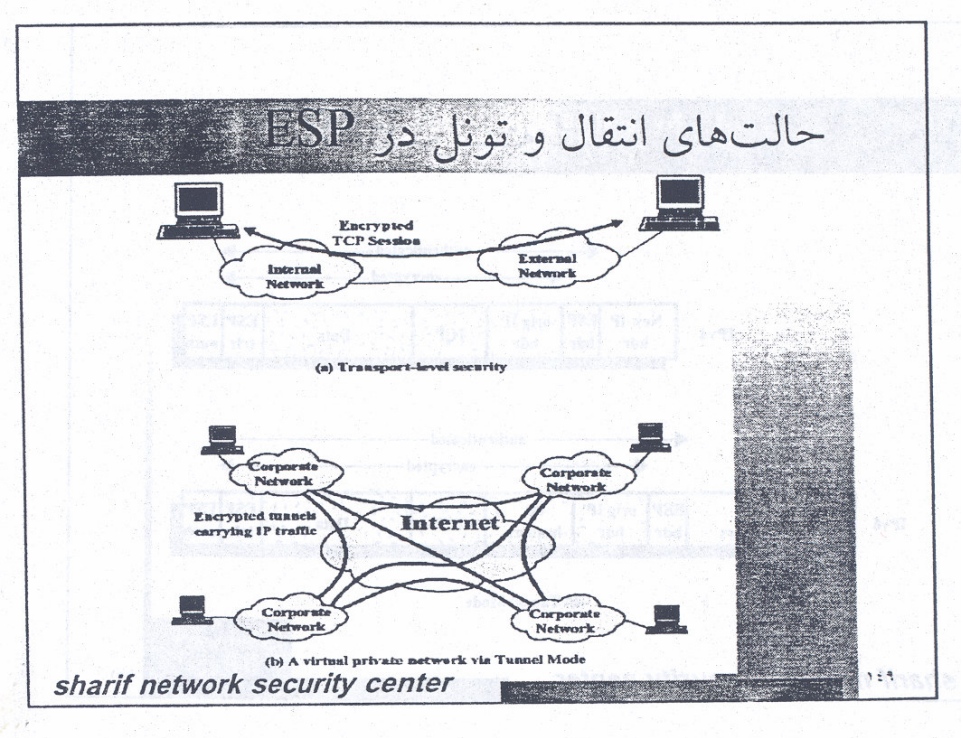
شكل ٥ . پروتكل ESP درلايه شبكه

١. اولين ٣٢ بيت سرآيند ESP همان SPI است كه درSA بكار گرفته شده و جهت بازگشايي پكت كپسوله شده ESP بكار مي رود.
٢. دومين فيلد همان شماره توالي يا Sequence Number مي‌باشد كه به جهت حفاظت از تهاجمات داده هاي بازگشتي استفاده مي شود.
٣. سومين فيلد همان بردار مقدار اوليه يا(IV) Initialization Vector مي باشد. اين فيلد نيز براي پردازش رمزنگاري بكار مي رود. الگوريتمهاي رمزنگاري متقارن اگر از IV استفاده نكنند، مورد تهاجم متوالي روي پكت قرار ميگيرد. IV اين اطمينان را ميدهد تا دو مشخصه Payload روي دو Payload رمز شده مختلف قرار گيرد.
پردازش رمزنگاري در IPSec در دو بلوك رمز (Chiper) بكار مي رود. بنابراين اگر طول Payload ها تك تك باشند. IPSec , Payload ها را به شكل لايه لايه قرار ميدهد. و از اينرو طول اين لايه ها همواره در حال اضافه شدن است. طول لايه (Pad length) ٢ بايت است.

[٢٤] – Encryption principle

۵. فيلد بعدي كه همان Next header مي باشد، سرآيند بعدي را مشخص مي كند.
۵. اين پروتكل HMAC است كه مانند پروتكل HA از تماميت و سلامت داده هاي ارسالي حفاظت ميكند. فقط اين سرآيند است كه مي تواند به Payload اعتبار دهد. سرآيند IP شامل پروسه محاسبه نمي باشد.
NAT هيچ دخلي به كار ESP ندارد و اين بخش هنوز هم ممكن است بخشي از IPSec باشد و با آن تركيب گردد. NAT پيمايشي[۲۵] راه حلي است در كپسوله كردن پكت‌هاي ESP به همراه پكت هاي UDP.

در شكل شماره ۶ حالتهاي انتقال و تونل در پروتكل ESP به نمايش در آمده است.



شكل ۶ حالتهاي انتقال و تونل در پروتكل ESP

همان طور كه مي بينيد اين پروتكل در اين دو حالت ارتباط امن بين دو نقطه انتهائي كه در دو شبكه مجزا قرار دارند را فراهم مي آورد ،همچنين ارتباط امن بين دو نقطه در يک شبكه داخلي و يک نقطه انتهائي و يک مسير ياب يا حفاظ ديواره آتش(FireWall) را ممكن مي سازد.

پروتكل IKE

[۲۵] NAT-Traversal-

IKE پروتكلي است كه چندين مسئله مهم در ارتباط امن را تنظيم مي كند. احراز هويت نقاط نظير و كليد تبادلي متقارن. اين پروتكل مجمع امنيت (SA) را ايجاد كرده و درSAD يا پايگاه مجمع امنيت[۲۶]
قرار ميدهد. IKE پروتكلي است كه عموماً نيازمند فضاي كاربر فوق العاده اي[۲۷] است و روي سيستم هاي عامل پياده سازي نمي شود. پروتكل IKE، از پورت شماره UDP/500 استفاده مي كنند.
IKE از دو مرحله تشكيل شده است. اولين مرحله همان تشكيل مجمع امنيت مديريت كليد SA[۲۸] يا (ISAKMP SA) مي باشد. در مرحله دوم ISAKMPSA ، براي مذاكره [۲۹] و تنظيم IPSec , SA بكار مي رود.
احراز هويت مرحله اول نقاط نظير معمولاً بر مبناي كليدهاي پيش اشتراك شده[۳۰] يا(PSK) (Per Shared Keys)، كليدهاي RSA و گواهينامه X509 بوجود مي آيد.
مرحله اول از دوحالت پشتيباني مينمايد. حالت اصلي (main mode) و حالت تهاجمي (aggressire mode) اين دو حالت نقاط نظير را احراز هويت كرده و ISAKMP SA را تنظيم مي نمايند. در حالت تهاجمي تنها نصف تعداد پيامها در اين مورد تحت پوشش قرار ميگيرد. به هر حال اين خود يك اشكال محسوب مي شود، زيرا اين حالت نمي تواند از هويت نقاط نظير پشتيباني حفاظت نمايد و از اين جهت است كه اين حالت با داشتن كليد پيش اشتراكي (PSK) مستعد حملات ميان راهي (man-in-the-middle) خواهد بود. از طرف ديگر تنها منظور از حالت تهاجمي همين است.
در حالت اصلي نه تنهااز كليد پيش شرط مختلف نمي تواند پشتيباني نمايدبلكه نقاط نظير به نظير را نيز نمي شناسد. در حالت تهاجمي كه از حفاظت هويت افراد / نقاط حمايت نمي كند و هويت كاربران انتهايي را چنين شفاف انتقال ميدهد. بنابراين نقاط نظير هر چيز را خواهد دانست پيش از آنكه احراز هويتي در مورد جا و كليدهاي پيش شرط بتواند بكار برد.
در مرحله دوم پروتكل IKE كه SA هاي پيشنهادي تبادل مي شوند و توافقاتي بر پايه ISAKMP SA براي SA انجام خواهد شد. ISAKMP SA احراز هويت براي حفاظت از تهاجمات ميان راهي را تهيه مي بيند. دومين مرحله از حالت سريع[۳۱] استفاده مي كند.
معمولاً دو نقطه نظير روي SAKMP SA با هم مذاكره و توافق مي كنند كه هر دو طرف معمولاً روي چندين مذاكره (حداقل ۲ تا) بطور غير مستقيم توافق كنند.

---

[۲۶] - Security Association data base
[۲۷] - a user space daemon
[۲۸] - Internet Security Association and key-negotiate
[۲۹] -
[۳۰] – Pre Shared Key
[۳۱] - quick mode