# امنیت شبکه

## جلسه نهم: امنیت IP

تهیه و تنظیم: دکتر آرش حبیبی لشکری

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

اولین نسخه: دی 1393
بروزرسانی: دی 1393

## فهرست:

- امنیت IP
- مثالهایی از موارد کاربرد IPsec
- ویژگیهای Ipsec
- مزایای استفاده از IPsec
- سرویس‌های Ipsec
- حالتهای انتقال و تونل
- تبادل کلید اینترنتی
- روشهای رمزنگاری

# امنیت IP

با اجرای امنیت در سطح IP، یک سازمان می‌تواند از امنیت شبکه نه تنها برای برنامه‌هایی که دارای مکانیزم امنیتی هستند بلکه برای خیلی از برنامه‌های امنیتی که ناشناخته هستند، مطمئن شود.

امنیت سطح IP- سه زمینه اصلی را در بر می‌گیرد: احراز هویت، محرمانگی، و مدیریت کلید.

مکانیزم احراز هویت این اطمینان را فراهم می‌کند که یک بسته‌ای که به مقصد رسیده، درحقیقت، از طرف فرستنده‌ای که به عنوان منبع در سربار بسته معرفی شده، ارسال گردیده است.

امکانات محرمانه نگه‌داشتن اطلاعات امکان برقراری ارتباط کامپیوترها برای جلوگیری از استراق سمع توسط سوم شخص را می‌دهد.

امکانات مدیریت کلید برای مبادلات امن کلیدها در نظر گرفته می‌شود.

# مثالهایی از موارد کاربرد Ipsec

IPsec توانایی ارتباط امن از طریق شبکه محلی و شبکه‌های گسترده خصوصی و عمومی، و همچنین از طریق اینترنت رافراهم نموده است. مثالهایی از موارد کاربرد آن عبارتست از:

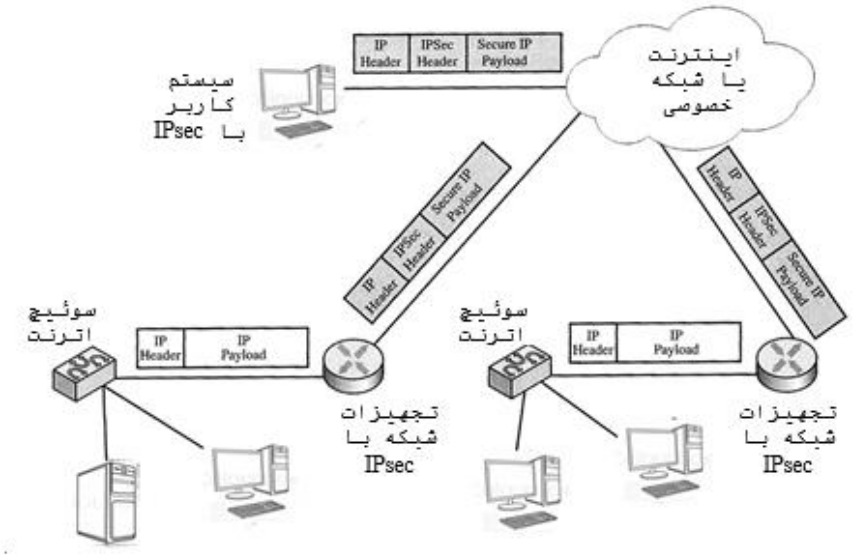
* **اتصال امن شعبه دفتر کار از طریق اینترنت:** یک شرکت می‌تواند یک شبکه خصوصی مجازی امن را از طرریق اینترنت یا شبگه گسترده عمومی برای خود ایجاد نماید. این امر یک شرکت را قادر می‌سازد تا بتواند به شکل جدی به اینترنت تکیه نموده و نیازش را به شبکه‌های گسترده خصوصی کاهش دهد، که خود باعث کاهش هزینه‌ها و سربار مدیریت شبکه خواهد شد.

* **دسترسی از راه دور از طریق اینترنت:** یک کاربر پایانی که سیستمش توسط پروتکلهای امنیت IP تجهیز شده است می‌تواند یک تماس با تهیه کننده خدمات اینترنتی یا همانISP برقرار نموده و یک دسترسی امن به شبکه یک شرکت را بدست آورد. این امر هزینه کلی تدارکات برای کارمندان در حال ماموریت و کارمندان متصل از راه دور را کاهش می‌دهد.

* **ارتقا امنیت تجارت الکترونیکی:** اگرچه بعضی از برنامه‌های وب و تجارت الکترونیکی دارای پروتکلهای امنیتی هستند که جزئی از خود برنامه محسوب می‌شود، ولی استفاده از IPsec امنیت را ارتقا می‌بخشد. در اصل IPsec همه ترافیکی را که توسط مدیران شبکه برای هر دو مورد رمزشده و احراز هویت شده تخصیص داده‌اند، را با افزودن یک لایه امنیتی اضافی به هرچیزی که در لایه کاربردی تهیه شده باشد، تضمین می‌کند.

# ویژگیهای IPsec

ویژگی عمده IPsec که آنرا قادر می‌سازد تا از انواع مختلف برنامه‌ها حمایت کند این است که می-تواند همه ترافیک در سطح لایه IP را به رمز درآورد و یا احراز هویت نماید. بنابراین، همه نرم افزارهای توزیع شده (شامل ورود به سیستم از راه دور، مشتری/سرویس‌دهنده، پست الکترونیکی، انتقال فایل، دسترسی به وب، و غیره) می‌توانند امن شوند. تصویر زیر یک سناریوی معمول از کاربرد IPsecرا نمایش می‌دهد. یک سازمان شبکه‌های محلی خود را در محلهای مختلف توزیع و پراکنده می‌نماید. ترافیک IP غیر امن بر روی هر شبکه هدایت می‌شود. برای ترافیکی که بر روی محل خاصی واقع نشده است، از طریق نوعی از شبکه‌های گسترده خصوصی و عمومی، پروتکلهای Ipsec استفاده می‌شوند.




این پروتکلها بر روی تجهیزات شبکه همانند یک مسیریاب یا دیوار آتش، که هر شبکه محلی را به دنیای خارج متصل می‌کند، اجرا می‌شوند. تجهیزات شبکه IPsec معمولا همه ترافیک ورودی به شبکه‌های گسترده را رمز و فشرده نموده و سپس ترافیک بصورت غیررمز و غیرفشرده از شبکه گسترده خارج می‌شود.

# مزایای استفاده از IPsec

* هنگامی که IPsec در یک دیوارآتش یا مسیریاب پیاده‌سازی می‌شود، امنیت بسیار قوی فراهم می‌کند که می‌تواند بر روی همه ترافیکهایی که از محیط اطراف عبور می‌کنند، اعمال شود. ترافیک درون شرکت یا گروه کاری موجب سربار در پردازشهای مربوط به امنیت نخواهد شد.

* IPsec در دیوارآتش در برابر عبور ترافیک مقاوم است . اگر همه ترافیک‌هایی که از خارج وارد می-شوند باید از IP استفاده نمایند و دیوارآتش تنها راه ورود از اینترنت به سازمان باشد.

* IPsec در پایین لایه انتقال است (TCP, UDP) و بنابراین برنامه‌های کاربردی از وجود و عملکرد آن مطلع نبوده و وجودش برای برنامه‌های کاربردی شفاف نیست. در اینجا ضرورتی برای تغییر نرم‌افزار بر روی سیستم کاربر یا سرویس‌دهنده هنگامی که IPsec در یک دیوارآتش یا مسیریاب اجرا نشده است، وجود ندارد.

* IPsec می‌تواند برای کاربران پایانی شفاف باشد. در اینجا احتیاجی برای آموزش کاربران در مورد مکانیزمهای امنیتی، تولید موارد کلیدی مطرح شده برای هر کاربر، یا ابطال موارد کلیدی زمانی که کاربر سازمان را ترک می‌کند، وجود ندارد.

* IPsec می‌تواند در صورت نیاز برای کاربران شخصی نیز امنیت فراهم نماید. این امر برای کاربرانی که خارج از شرکت کار می‌کنند برای راه‌اندازی یک زیر شبکه مجازی امن با سازمان برای نرم‌افزارهای حساس مفید خواهد بود.

# سرویس‌های IPsec

IPsec امنیت سرویس‌ها در لایه IP را از طریق فعالسازی یک سیستم برای انتخاب پروتکلهای امنیتی مورد نیاز فراهم می‌کند، که الگوریتمها را برای استفاده در سرویسها تعریف کرده، و هر نوع کلید موردنیاز برای تهیه سرویسهای مورد نیاز را در محل قرار می‌دهد.

دو پروتکل برای تامین امنیت استفاده می‌شود که عبارتند از یک پروتکل احراز هویت که توسط سربار پروتکل طراحی شده است، سربار احراز هویت یا همانAH؛ و دیگری ترکیبی از پروتکل رمزنگاری/احرازهویت که طبق فرمت خاصی برای آن پروتکل طراحی شده، که همان کپسوله‌کردن بار امنیتی یا ESP خواهد بود.

سرویسهای مهم عبارتند از (RFC4301):

* کنترل دسترسی
* درستی ارتباطات
* شناسایی و تایید منشا داده‌ها
* رد کردن بسته های پاسخ داده شده ( یک نوع یکپارچگی)
* قابلیت اعتماد (رمزنگاری)
* قابلیت اعتماد جریان ترافیک محدود

# حالتهای انتقال و تونل

هر دو مورد AH و ESP از دو حالت انتقال و تونل پشتیبانی می‌نمایند.

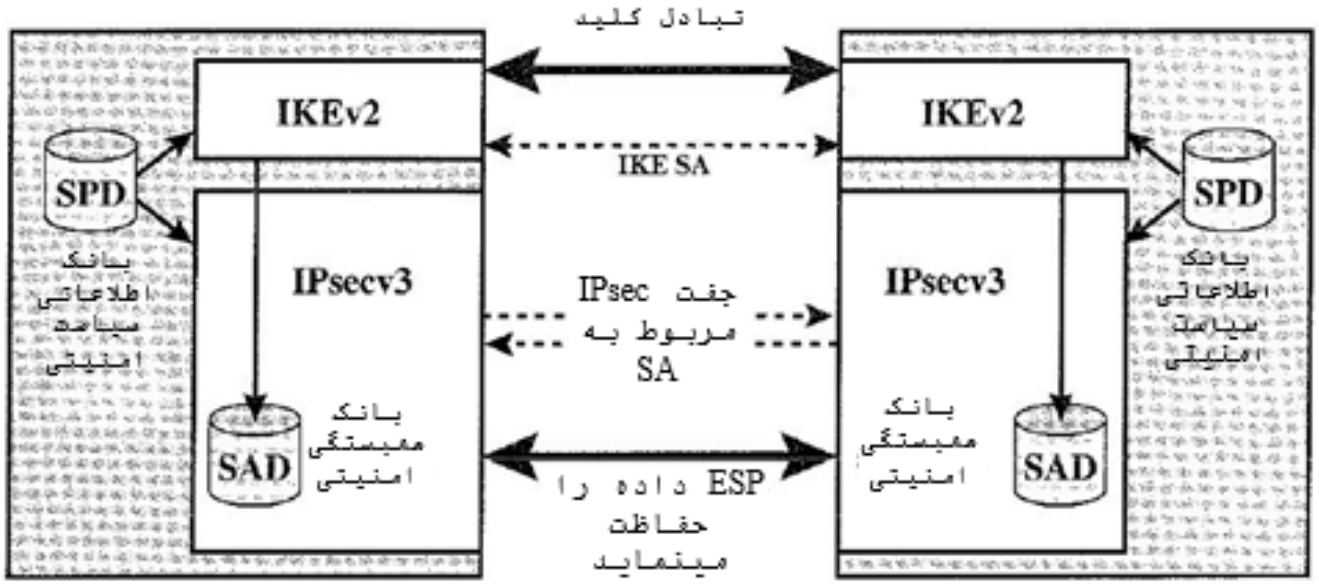
حالت انتقال حمایت اولیه‌ای برای لایه‌های بالاتر پروتکلها فراهم می‌کند. این حالت در اصل همان عملیات حفاظتی حالت انتقال است که به بار مفید یک بسته IP توسعه یافته است. یعنی در اینجا بار مفید بسته یا همان دادههای بسته که بدنبال سربار بسته قرار دارند، رمز گذاری خواهند شد.

حالت تونل حمایت از کل بسته IP را فراهم می‌کند. برای دست یافتن به این هدف، بعد از AH یا ESP فیلدهایی به بسته IP اضافه می‌شوند، کل بسته بعلاوه فیلدهای امنیتی بعنوان بارمفید بسته خروجی IP با یک سربار جدید خروجی IP در نظر گرفته می‌شود. کل، ورودی، بسته از طریق یک تونل از یک نقطه از یک شبکه IP به نقطه دیگر حرکت می‌کند، هیچ مسیریابی در طول مسیر قادر به بررسی سربار IP ورودی نیست.

مثالی برای حالت تونل چنین خواهد بود. میزبان A در شبکه یک بسته IP با آدرس مقصد میزبان B بر روی شبکه دیگر تولید می‌نماید. این بسته‌ها از میزبان منبع به دیوارآتش یا یک مسیریاب امن در محدوده شبکه A هدایت می‌شوند. دیوارآتش همه بسته‌های خروجی را برای مشخص‌کردن نیاز به فرایند IPsec فیلتر می‌کند. اگر این بسته از A به Bنیاز به IPsecداشته باشد، دیوارآتش پردازش IPsec و کپسوله کردن بسته را با یک سربار IP خروجی انجام می‌دهد. آدرس IP منبع در این بسته IPخروجی همان دیوارآتش بوده و آدرس مقصدش نیز ممکن است دیوارآتشی باشد که محدوده B در شبکه محلی وجود داشته باشد. این بسته اکنون از طریق مسیریابهای میانی که فقط سربار IPخروجی را بررسی می‌کنند به دیوارآتش B، منتقل می‌شود. در دیوارآتش B، سربار IPخروجی پاک شده و بسته داخلی به B انتقال داده می‌شود.

# سیاست IPsec

اساس کار IPsec مفهوم سیاست امنیتی بکار برده شده در هر بسته IP است که از یک منبع به یک مقصد عبور می‌کند. سیاست IPsec عمدتا توسط تعامل دو پایگاه داده، پایگاه داده اجتماع امنیتی یا همان SAD و پایگاه داده سیاست امنیتی یا همان SPD تعیین می‌شود.



# سیاست IPsec

مفهوم کلیدی که در هردو مکانیزم احرازهویت و محرمانگی برای IP ظاهر می‌شود همان همبستگی امنیتی یا SA است. یک همبستگی در اصل یک ارتباط یکطرفه منطقی بین یک فرستنده و یک گیرنده است که سرویسهای امنیتی در ترافیک جاری آن اعمال شده باشند. اگر یک جفت ارتباط برای مبادله دو طرفه امن مورد نیاز باشد، آنگاه دو همبستگی امنیتی مورد نیاز خواهد بود.

یک همبستگی امنیتی به طور منحصر بفرد توسط سه پارامترها شناسایی می‌شود:

* شاخص پارامترهای امنیتی یا همان SPI: یک عدد صحیح بدون علامت 32 بیتی که به این SA اختصاص داده می‌شود و فقط اهمیت محلی دارد. در واقع SPI درون سربار AH و ESP قرار داده می-شود تا به سیستم گیرنده این امکان را بدهد که بتواند انتخاب نماید که SA تحت کدام بسته دریافت شده پردازش گردد.

* آدرس مقصد IP: یک آدرس از مقصد نهایی SA است، که ممکن است یک سیستم کاربر پایانی یا یک سیستم شبکه مانند دیوارآتش یا مسیریاب باشد.

* شناسه پروتکل امنیتی: این فیلد از سربار IP خروجی نشان می‌دهد که آیا همبستگی یک همبستگی امنیتی AH یا ESP است یا خیر.

# سیاست IPsec

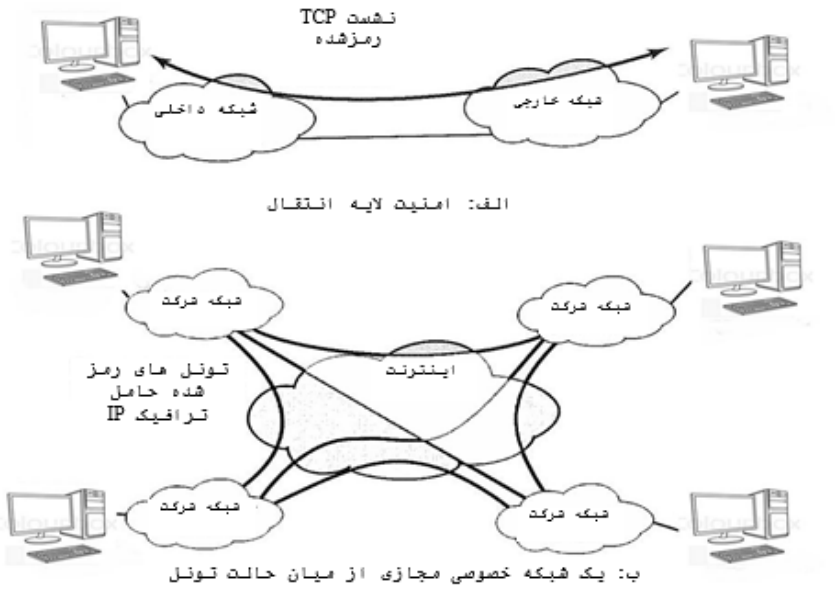
پایگاههای امنیتی SAD و SPD:

در هر پیاده سازی IPsec، یک پایگاه داده همبستگی امنیتی یا SAD وجود دارد که پارامترهای ارتباط با هر SA مانند شمارنده شماره توالی، سرریز شمارنده توالی، سول عمر، حالت پروتکل Ipsec و ... را تعریف می‌کند. در واقع می‌توان چنین گفت که IPsec مقدار قابل توجهی انعطاف پذیری برای کاربران فراهم می‌کند به طریقی که سرویسهای IPsec به ترافیک IP اعمال شوند.

مفهوم اینکه ترافیک IPبه کدام SAهای خاص (یا SA که در مورد ترافیک اجازه عبور IPsec را ندارد) ارتباط دارد یک پایگاه سیاست امنیتی یا همان SPD است. در ساده‌ترین شکل، یک SPD شامل ورودیهاست، که هر کدام از آنها یک زیرمجموعه از ترافیکهای IP را تعریف می‌کند و به یک SA مرتبط با آن ترافیک اشاره می‌کند. مواردی چون آدرسهای IP راه‌دور، آدرسهای IP محلی، پروتکل لایه بعدی، گذرگاه‌های محلی و راه‌دور و ..و ورودیهایSPD هستند.

# حالتهای انتقال و تونل

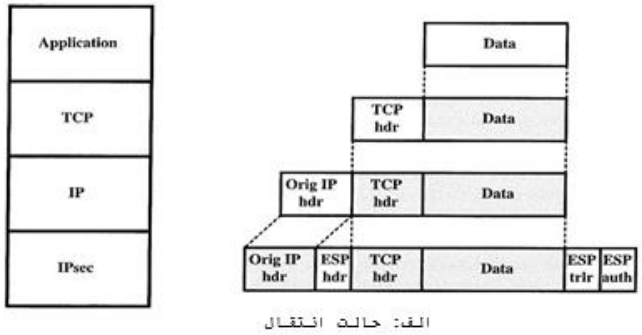
تصویر زیر دو روش که در سرویس ESP IPsec قابل استفاده است را نشان می‌دهد. در قسمت بالای تصویر، رمزنگاری (و به طور انتخابی احراز هویت) مستقیم و بدون واسطه بین هر دو میزبان فراهم شده است. تصویر پایین نشان می‌دهد که چگونه می‌توان از عملیات حالت تونل استفاده کرد تا یک شبکه مجازی خصوصی را راه‌اندازی کرد.



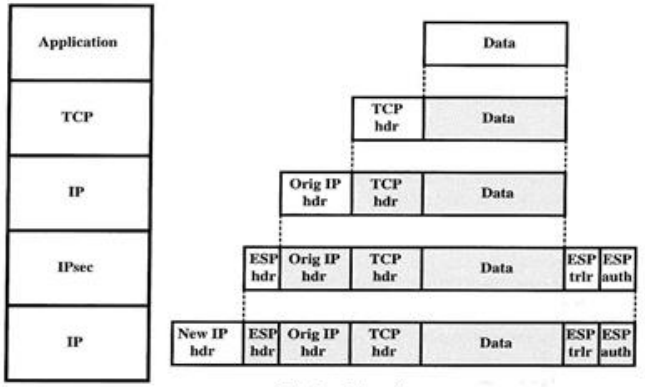

در این مثال، یک سازمان 4 شبکه خصوصی متصل به اینترنت دارد. میزبانها بر روی شبکه‌های داخلی از اینترنت برای انتقال داده‌ها استفاده می‌کنند اما با سایر میزبانهای متصل به اینترنت تعاملی ندارند. با خاتمه دادن به تونلهای مربوط به دروازه‌های امنیتی در هر شبکه داخلی، تنظیمات اجازه می‌دهند تا میزبانها از پیاده‌سازی تواناییهای امنیتی دوری گزینند. تکنیکهای پیشین توسط حالت انتقال SA حمایت شده است، در حالی که اخیرا تکنیکها از حالت تونل SAاستفاده می-کنند.

# امنیت IPsec

**حالت انتقال ESP:** حالت انتقال ESP برای رمزنگاری و به طور بالقوه احراز هویت داده که توسط IP منتقل می‌شود استفاده خواهد شد. در این حالت سربار ESP در بسته IP بلافاصله بعد از سربار لایه انتقال (به عنوان مثال، TCP، UDP، ICMP) استفاده می‌شود، و یک دنباله ESP(لایه‌گذاری، طول لایه، و فیلدهای سربار بعدی) نیز بعد از بسته IPقرار می‌گیرد.




الف: حالت انتقال




ب: حالت تونل

اگر احراز هویت انتخاب شود، فیلد داده احراز هویت ESP بعد از دنباله ESPاضافه می‌شود. تمام بخش لایه انتقال به علاوه دنباله ESPرمز خواهد شد. (این روش معمول در IPV4 است، برای IPV6 چگونه خواهد بود؟)

**حالت تونل ESP:** حالت تونل ESPبرای رمزنگاری همه بسته IP( تصویر 9. 8پ) استفاده می‌شود. برای این حالت، سربار ESPپیشوند بسته بوده و سپس بسته بهمراه دنباله ESPرمز خواهد شد.

از آنجایی که حالت انتقال برای حمایت ارتباط بین میزبانهایی که از ویژگیهای ESP حمایت می‌کنند، مناسب است لذا حالت تونل برای پیکربندی که شامل یک دیوارآتش یا انواع دیگری از دروازه‌های امنیتی که یک شبکه قابل اعتماد را از شبکه های خارجی محافظت می‌نمایند، مفید خواهد بود.

# تبادل کلید اینترنتی

بخش مدیریت کلید IPsec شامل تعریف و پخش کلیدهای مخفی است. یک درخواست معمولا شامل چهار کلید برای ارتباط بین دو برنامه خواهد بود: جفت دریافت و ارسال بمنظور مدیریت هر دو عملیات یکپارچگی و محرمانگی پیام است.

اسناد موجود برای شرح ساختار IPsec حمایت از دو نوع مدیریت کلید را الزامی دانسته اند:

* **دستي (راهبر):** یک راهبر سیستم بصورت دستی هر سیستمی را بوسیله کلیدهای خودش و کلیدهای سیستم‌های ارتباطی دیگر تنظیم می‌کند. این مورد برای فضاهای کوچک و محیطهای به نسبت پایدار کاربرد دارد.

* **اتوماتیک (سیستم):** یک سیستم اتوماتیک تولید کلیدها برحسب تقاضا را برای SAها فعال نموده و امکان استفاده از کلیدها را در یک سیستم توزیع شده بزرگ با یکسری تنظیمات امکان پذیر می-سازد.

پروتکل پیش‌فرض مدیریت تولید اتوماتیک کلید برایIPsec با عنوان ISAKMP/Oakley شناخته می‌شود.

# مجموعه روشهای رمزنگاری

پروتکلهای IPsecv3 و IKEv3 بر انواع مختلفی از الگوریتم‌های رمزنگاری تکیه می‌کنند. برای ارتقاء این همکاری، دو RFC سعی در تعریف مجموعه‌های پیشنهادی از الگوریتم‌های رمزنگاری و پارامترهای برنامه‌های مختلف دارند.

اول RFC4308 که مجموعه رمزنگاری برای بنا نهادن شبکه‌های خصوصی مجازی را تعریف می‌کند. در اینجا مجموعه VPN-Aکه باید با امنیت VPN سازمانهایی که به طور معمول استفاده شده اند، انطباق داشته باشد و در پیاده‌سازی IKEv1های قدیمی‌تر در زمان انتشار IKEv2 در 2005 استفاده شده است. مجموعه VPN-B امنیت قویتری را فراهم می‌کند و برای VPNهای جدید پیشنهاد می‌شود که IPsecv3 و IKEv2 را پیاده‌سازی می‌کنند.

| | VPN-A | VPN-B |
|---|---|---|
| رمزنگاری ESP | 3DES_CBC | AES-CBC (کلید 128بیتی) |
| یکپارچگی ESP | HMAC-SHA1-96 | AES-XCBC-MAC-96 |
| رمزنگاری IKE | 3DES-CBC | AES-CBC (کلید 128بیتی) |
| IKE PRF | HMAC-SHA1 | AES-XCBC-PRF-128 |
| یکپارچگی IKE | HMAC-SHA1-96 | AES-XCBC-MAC-96 |
| گروه IKE DH | MODP با 1024 بیت | MODP با 2048 بیت |

# سوالات مرتبط

1. چند مثال از کاربردهای IPSec بیان نمایید؟
2. چه سرویسهایی توسط IPSec پشتیبانی می‌شوند؟
3. چه پارامترهایی یک SA را شناسایی می‌نمایند و چه پارامترهایی برای تعریف یک SA خاص بکار می‌روند؟
4. تفاوت بین حالت انتقال و حالت تونل چیست؟
5. منظور از حمله بازپخش چیست؟
6. نقش پروتکل تعریف کلید Oakley و ISAKMP در IPSec چیست؟

**خلاصه:** امنیت IP، مثالهایی از موارد کاربرد Ipsec، ویژگیهای Ipsec، مزایای استفاده از Ipsec، سرویس‌های Ipsec، حالتهای انتقال و تونل، تبادل کلید اینترنتی، روشهای رمزنگاری

## جلسه بعدی: بدافزارها

منبع: کتاب اصول و مبانی امنیت شبکه (استانداردها و کاربردها)

ترجمه: دکتر آرش حبیبی لشکری، مهندس نسرین بدیع، مهندس فرنار توحیدی

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.