

تفاوت IKE v1 با IKE v2 در چیست؟ مقایسه پروتکل IKEv1 و IKEv2 (نسخه PDF)

پروتکل IKE مخفف کلمات Internet Key Exchange میباشد که این پروتکل یکی از مجموعه پروتکل های IPsec است. یکی از مسئولیت های این مجموعه پروتکل این است که هر دو طرف فرستنده و گیرنده بصورت امن پکت های خود را در شبکه ارسال کنند. پروتکل IKE در سال ۱۹۹۸ معرفی شد و حدود ۷ سال بعد از معرفی نسخه اولیه آن نسخه دوم آن یا IKEv2 معرفی شد. IKEv1 با IKEv2 دارای تفاوت هایی است یکی از آن تفاوت ها این است که IKEv2 پهنای باند کمتری را نسبت به نسخه قدیمی خود یعنی IKEv1 مصرف میکند. آزاد بودن پهنای باند برای انتقال بهینه تر داده ها در شبکه نقش موثری دارد.

تفاوت دیگری که میان IKEv1 با IKEv2 وجود دارد پشتیبانی نکردن پروتکل احراز هویت EAP در IKEv1 است که در IKEv2 به طور کامل پشتیبانی میشود. IKEv1 از EAP پشتیبانی نکرده و از pre-shared key و یک گواهی احراز هویت که در IKEv2 هم پشتیبانی میشود استفاده میکند. استفاده از پروتکل احراز هویت EAP در ارتباط با سیستم های احراز هویت سازمانی ضروری است. با به میان آمدن IKEv2 قابلیت MOBIKE هم کنار آن مطرح شد که در IKEv1 وجود ندارد. MOBIKE همان IKEv2 است که در گوشی های موبایل (MOBILE) استفاده میشود.

تفاوت دیگر میان IKEv1 با IKEv2 در این است که بر خلاف IKEv1 پروتکل IKEv2 در ارتباطاتش از NAT پشتیبانی میکند که در اصطلاح به آن NAT Traversal نیز میگویند. این قابلیت به شما امکان میدهد تا مثلا زمانی که شما یک سرور در جایی دور از شبکه داخلی تان دارید و میخواهید با پروتکل IKEv2 به آن VPN بزیند این قابلیت به شما کمک میکند که با استفاده از NAT عملیات ارتباط از راه دور را با سرور خود انجام دهید. کمی فنی تر به قضیه نگاه کنیم: در عملیات NAT traversal زمانیکه روتر پکت ارسالی را دریافت کرد پکت را باز کرده و آدرس Destination یا مقصد را تغییر میدهد که به این فرآیند در اصطلاح Static NAT یا SNAT میگوییم. به طور معمول زمانی که چندین کاربر از یک آدرس IP استفاده میکنند و میخواهند که با اینترنت ارتباط برقرار کنند از عملیات NAT استفاده میشود.

در آخر IKEv2 بهبود داده شد تا جاییکه میتواند تشخیص دهد که ارتباطش با Tunnel هنوز برقرار است یا خیر، که به این فرآیند در اصطلاح فنی liveness check میگویند. اگر نتیجه فرآیند liveness check با موفقیت انجام نشد یا عبارتی Fail بود نتیجه این است که ارتباط با Tunnel قطع شده است. IKEv2 قادر به re-establish یا re-connect کردن ارتباطش با تانل به صورت اتوماتیک نیز هست. IKEv1 از قابلیت re-connect کردن ارتباط برخوردار نیست و فرض را بر این میگیرد که ارتباط همیشه برقرار خواهد بود. گر چه چندین راه حل برای حل این مشکل وجود دارد اما آنها بر طبق استاندارد نیستند. پس در کل نتیجه میگیریم که اطمینان پذیری IKEv2 از IKEv1 بیشتر است.

خلاصه :

- IKEv2 به اندازه IKEv1 پهنای باند شبکه را مصرف نمیکند
- IKEv2 از پروتکل EAP پشتیبانی میکند در حالیکه IKEv1 از این پروتکل پشتیبانی نمیکند
- IKEv2 از قابلیت MOBIKE پشتیبانی میکند در حالیکه IKEv1 از این قابلیت برخوردار نیست
- IKEv2 قابلیت NAT traversal را به طور درون ساخت در خودش دارد در صورتیکه IKEv1 از این قابلیت پشتیبانی نمیکند
- IKEv2 توانایی تشخیص برقرار بودن ارتباط با tunnel را دارد در حالیکه IKEv1 این توانایی را ندارد

نویسنده : امیرحسین کریم پور

منبع : ITPRO

هرگونه نشر و کپی برداری بدون ذکر منبع و نام نویسنده دارای اشکال اخلاقی میباشد

مطلب اصلی