نشریه پژوهش‌های نوین در مدیریت کارآفرینی و توسعه کسب و کار
جلد۲، شماره۳، پاییز ۱۴۰۰، صفحه: از ۲۴۰ تا ۲۵۷
ISSN 2717-2570
https://science-journals.ir
https://pnmktk.science-journals.ir

نحوه راه‌اندازی VPN Server در ویندوز 2008

رهبر زارعی[۱]

۱- دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش معماری کامپیوتر، دانشگاه غیر انتفاعی کارون

چکیده

در این پژوهش به بررسی نحوه راه‌اندازی VPN Server در ویندوز 2008 اشاره شده و در ویندوز ۲۰۰۸ به‌طور پیش‌فرض، به کاربران اجازه دسترسی به سرور از راه VPN داده نشده است. شما باید به‌صورت تک‌به‌تک، برای هر یک از کاربرانی که می‌خواهید از راه اینترنت به سرور شما وصل شوند این اجازه را بدهید. برای این کار مراحل زیر را انجام دهید:اگر در سرور Domain Controller تعریف کرده باشید (نصب و راه‌اندازی کامل Domain Controller در بخش اول و دوم به‌طور مفصل توضیح داده شده است)، پنجره Active Directory Users and Computers را از مسیر زیر باز کنید.

Start > All Programs > Administrative Tools > Active Directory Users ... در غیر این صورت و اگر سرور شما در هیچ Domain ای تعریف نشده باشد (و به‌صورت سرور Standalone باشد)، پنجره Computer Management را از مسیر زیر:

Computer Management < Administrative Tools < All Programs < Start

باز کنید و صفحه properties مربوط به کاربری که می‌خواهید اجازه اتصال به VPN سرور خود را به آن بدهید، را باز کنید به قسمت Dial-In بروید و گزینه "Allow access" را انتخاب نمایید.

نتیجه گیری : با توجه به نتایج این پژوهش میتوان گفت میزان مشکلات روانشناختی افراد در دوران شیوع کرونا توسط ویژگی های روان رنجور خویی، وظیفه شناسی و توافق پذیری انها قابل پیش بینی است. با توجه به نقش قوی تر روان رنجور خویی دراین زمینه ضروری به نظر میرسد برای افراد با این مشخصه خدمات روان درمانی بیشتری در سازمانها در نظر گرفته شود .

واژگان کلیدی: راه‌اندازی VPN Server، ویندوز 2008، امنیت شبکه

۱- مقدمه

در این بخش به نحوه راه‌اندازی vpn server در ویندوز ۲۰۰۸ به همراه شکل و ساختار کلی آن در دو بخش می‌پردازیم و چگونگی آن را بیان می‌نماییم.
روش تحقیق به صورت کاملا توصیفی و با اقتباس از کتاب چاپ شده زیر نظر وزارت ارشاد توسط نویسنده ی مذکور می باشد.

راه‌اندازی VPN Server در ویندوز ۲۰۰۸ (بخش اول)

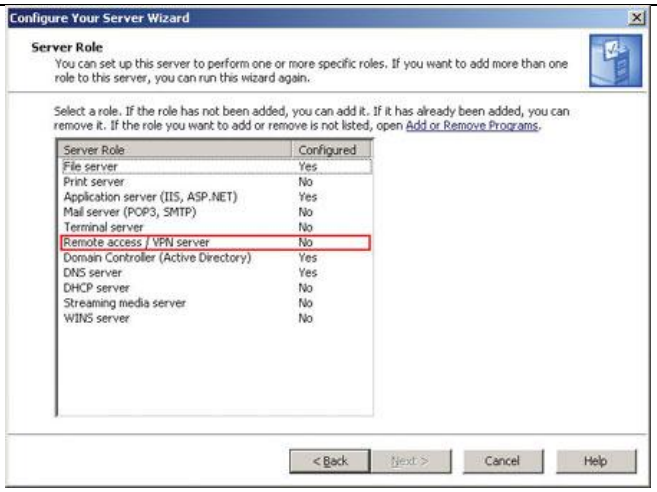
در این قسمت مرحله‌به‌مرحله و به‌صورت ساده و مختصر، مراحل نصب و راه‌اندازی VPN در ویندوز Windows Server 2008 شرح داده می‌شود...

تنظیم نقش Remote Access / VPN Server در ویندوز Server 2008

برای اعطای نقش Remote Access/VPN Server به ویندوز سرور ۲۰۰۸ یا به‌عبارت دیگر برای نصب و راه‌اندازی VPN Server باید ویزارد Configure Your Server Wizard را از مسیر زیر احضار کنیم:
Start >All Programs >Administrative Tools > Configure Your ServerWizard
اولین پنجره‌ای که ظاهر می‌شود، اطلاعات اولیه‌ای در مورد این ویزارد را نشان می‌دهد. دکمه Next را بزنید.
پنجره Preliminary Steps مواردی که لازم است قبل از شروع ویزارد انجام دهید را بازگو می‌کند مثلاً:

- اطمینان از نصب مودم‌ها و کارت‌های شبکه
- اگر ویزارد را برای اتصال به اینترنت می‌خواهید، از اتصال خود به اینترنت اطمینان حاصل کنید.
- و یا اینکه CD نصب ویندوز را آماده داشته باشید و غیره ...

دکمه Next را بزنید.
پنجره Server Role سومین پنجره‌ای است که ظاهراً می‌شود. همان‌طور که در شکل ۱ مشاهده می‌کنید لیستی از نقش‌هایی که روی سیستم می‌توانید اعمال کنید نشان داده شده است که در ستون مقابل هرکدام، وضعیت آن Role را از لحاظ اینکه این نقش اعطا شده است یا نه نشان داده شده است.



شکل ۱

برای اعطای نقش Remote Access / VPN به ویندوز، این مورد را از لیست انتخاب کرده و دکمه Next را بزنید. پنجره بعدی ویزارد توضیح مختصری درباره این نقش می‌دهد. (در صورت نیاز) پس از مطالعه آن دکمه Next را بزنید. ویزاردی با نام Routing and Remote Access Wizard ظاهر می‌شود (ویزارد RRAS) که در ادامه به آن اشاره می‌شود.

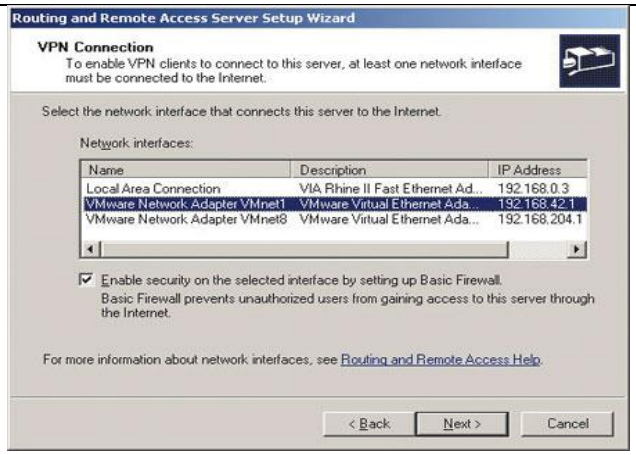
تنظیمات Routing and Remote Access (ویزارد RRAS)

مانند تمام ویزاردها، اولین پنجره این ویزارد، توضیح و نکات مختصری راجع به آن می‌باشد که ما با مطالعه آن و زدن دکمه Next از آن می‌گذریم.

در پنجره بعدی یعنی پنجره Configuration، گزینه‌های مختلفی وجود دارد که با توجه به نوع اتصال از راه دور (remote access connection) یکی از گزینه‌ها را انتخاب می‌کنیم؛ و چون قصد ما در اینجا راه‌اندازی VPN بر اساس PPTP می‌باشد ما گزینه Virtual Private Network VPN and NAT را انتخاب کرده و Next می‌زنیم.

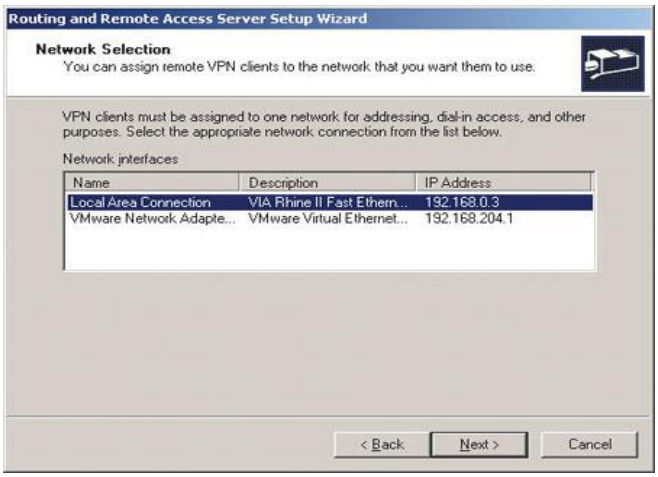
مطابق شکل ۲ و در پنجره VPN Connection باید آداپتور یا device ای که با آن به اینترنت وصل می‌شوید را تعیین کنید. نکته‌ای که در اینجا قابل‌توجه می‌باشد این است که برای برقراری امنیت بیشتر و در واقع برای کنترل دقیق‌تر، بهتر است که کارت شبکه مستقلی را برای server VPN در نظر بگیرید؛ که در اینجا ما کارتی غیر از کارت شبکه‌ای که برای اتصال کاربران محلی، انتخاب می‌کنیم.

گزینه Enable security on the selected interface by setting up Basic Firewall را تیک بزنید. این گزینه به‌عنوان یک Firewall نرم‌افزاری فعال شده و سرور شما از نفوذ خرابکاران و حملات مخرب آن‌ها از راه اینترنت در امان نگه می‌دارد. هر چند، نصب فایروال‌های پیشرفته و مستقل و یا یک فایروال سخت‌افزاری برای شبکه‌های محرمانه ضروری می‌باشد. (و این بستگی به درجه اهمیت شبکه و اطلاعات موجود در آن دارد)



شکل۲

مطابق شکل ۳ باید تنظیم نمایید که از کدام کارت شبکه برای کاربران محلی شبکه استفاده می‌کنید.



شکل ۳

همان‌طور که یک کاربر محلی برای برقراری اتصال با سرور و سایر کلاینت‌های موجود در شبکه نیاز به داشتن یک IP Address در همان Range دارد، VPN کلاینت‌ها نیز در هنگام برقراری اتصال به VPN سرور، نیاز به یک IP Address دارند که بتوانند به منابع مجاز در سرور دسترسی داشته باشند. در اینجا شما به‌عنوان مدیر شبکه با انتخاب یک روش از دو راه موجود، نحوه واگذاری آی‌پی آدرس را به کلاینت‌های VPN تعریف می‌کنید.

۱- با نصب و تعریف DHCP (که در شماره ۱۳ ماهنامه به‌طور کامل توضیح داده شده است) و اعمال تنظیمات لازم، سرور خود را به‌عنوان DHCP server تعریف می‌کنید طوری که کاربران در هنگام برقراری اتصال به

سرور شما از محدوده IP هایی که در سرور تعریف کرده‌اید، یکی را به خود اختصاص می‌دهند. با انتخاب گزینه Automatically روند واگذاری IP آدرس از روی تنظیمات DHCP server انجام می‌گیرد.

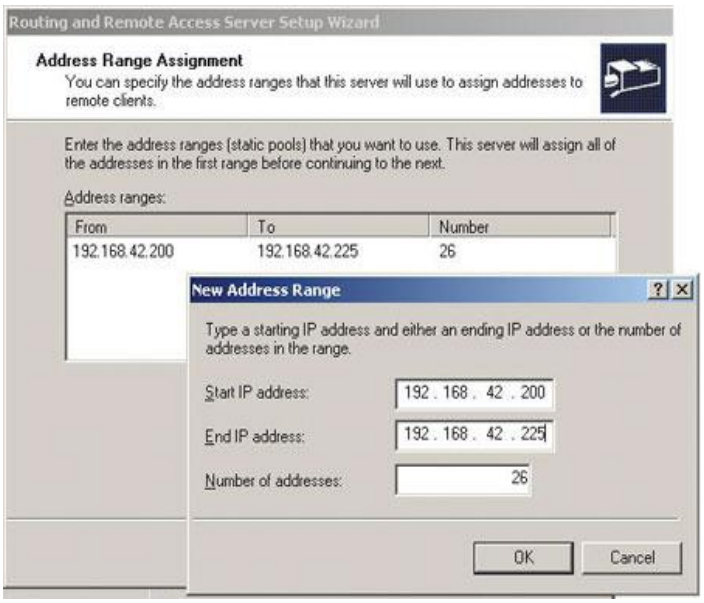
۲- تعیین محدوده خاصی از IP آدرس‌هایی که به کاربران واگذار شود.

ما در اینجا گزینه دوم را انتخاب می‌کنیم. به این دلیل که می‌خواهیم با استفاده از محدوده خاصی از IP آدرس‌ها که انتخاب می‌کنیم، کاربران شبکه محلی که به سرور وصل می‌شوند را از کاربرانی که از اینترنت (VPN Client) وصل می‌شوند تشخیص دهیم.

پس از انتخاب گزینه دوم (یعنی From a specified range of addresses)، دقیقاً تعریف می‌کنید که چه آی‌پی آدرس‌هایی را به Server VPN اختصاص می‌دهید که به VPN client ها واگذار نماید.

برای این کار دکمه New را در پنجره Address Range Assignment را بزنید و محدوده اولین و آخرین آی‌پی آدرس را تعیین کنید.

فیلد Number of addresses به‌صورت اتوماتیک با توجه به محدوده انتخابی شما تعیین می‌شود. می‌توانید فقط اولین آی پی آدرس را بنویسید و تعداد آی‌پی آدرس‌ها را مشخص کنید و ویزارد محاسبات را انجام داده و آی‌پی آدرس پایانی را وارد می‌کند. دکمه OK را بزنید تا تنظیمات شما ثبت شود. (به شکل ۴ توجه نمایید)



شکل ٤

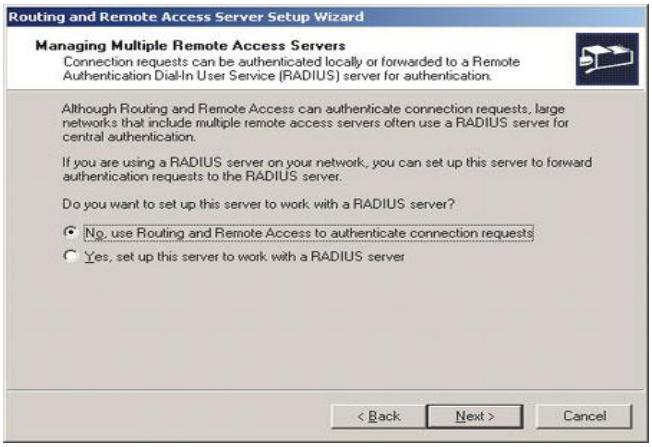
در پنجره بعدی (که دقیقاً مانند شکل ۳) کارت شبکه‌ای که برای اتصال سرور شما به اینترنت از آن استفاده می‌کنید را مشخص کنید (همان کارت شبکه‌ای که در شکل ۳ معرفی کرده بودید).

اعتبار سنجی (Authentication) یا بازرسی کاربران VPN ای که به سرور شما وصل می‌شوند بسیار مهم است. برای این اعتبار سنجی و برقراری امنیت دو گزینه را می‌توانید انتخاب نمایید:

۱- اگر در شبکه سرویس‌دهنده RADIUS داشته باشید، می‌توانید تنظیم کنید که VPN سرور شما، برای اعتبار سنجی کاربران خود از RADIUS استفاده کند. بدین معنی که اگر یک RADIUS سرور مرکزی در شبکه‌تان داشته باشید، اعتبار سنجی تمام کاربران شبکه برای بررسی به این سرور فرستاده تا برای ورود به VPN Server، تائید صلاحیت و یا رد صلاحیت شوند. با این روش کاربران در بین تمام سرورهای VPN به اشتراک گذاشته‌شده و نیازی به تعریف کاربران در تمامی سرورها نمی‌باشد.

- اما گزینه دوم، تمام تقاضاها برای اتصال به VPN Server، از طریق خود سرور و تنظیماتی که در آن نظر گرفته است، موردبررسی قرار گیرند.

که مطابق شکل ۵، ما اولین گزینه را انتخاب کرده و دکمه Next را می‌زنیم.

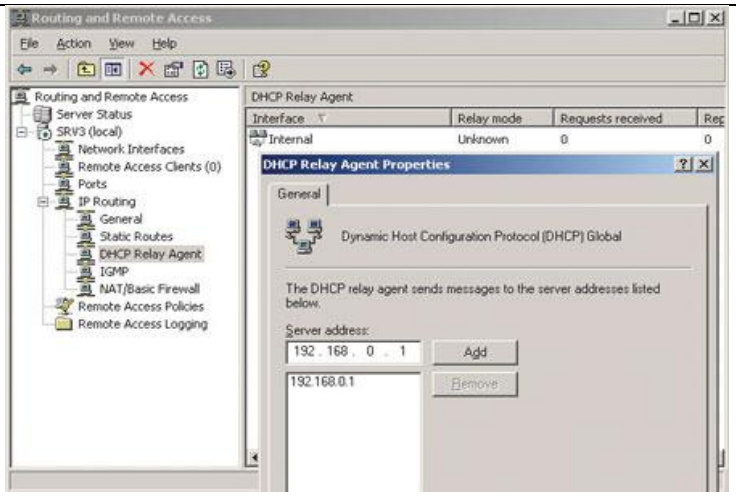


شکل ۵

در انتها ممکن است که پنجره‌ای ظاهر گردد که فقط کافی است دکمه OK را بزنید.

تا این مرحله تنظیمات مربوط به ویزارد نصب RRAS به پایان رسیده و نقش Remote Access /VPN Server به ویندوز ۲۰۰۸ اعطا شده است؛ اما برای دیدن نتیجه کار پنجره Routing and Remote Access را از مسیر زیر باز کنید و آدرس سرور را مطابق شکل ۶ اضافه کنید. انجام این تنظیم بسیار مهم می‌باشد.

Start > All Programs > Administrative Tools > Routing and Remote Access



شکل ٦

تنظیمات کاربران در ویندوز ۲۰۰۸

در ویندوز ۲۰۰۸ به‌طور پیش‌فرض، به کاربران اجازه دسترسی به سرور از راه VPN داده نشده است. شما باید به‌صورت تک‌به‌تک، برای هر یک از کاربرانی که می‌خواهید از راه اینترنت به سرور شما وصل شوند این اجازه را بدهید. برای این کار مراحل زیر را انجام دهید:

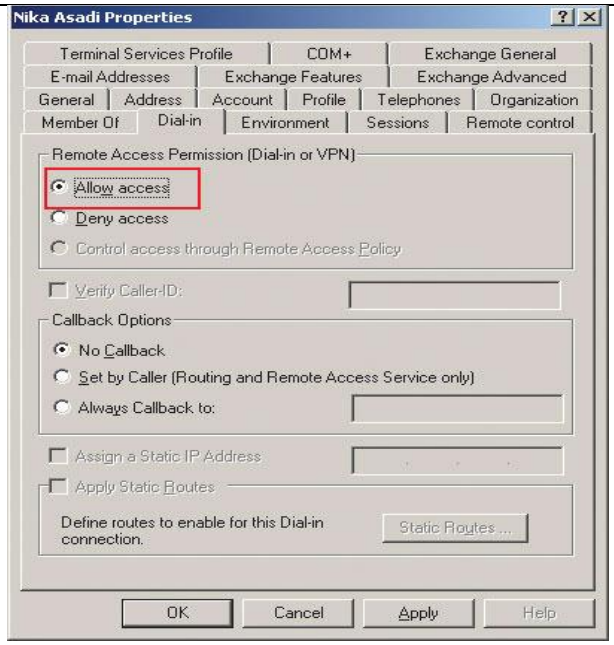
اگر در سرور Domain Controller تعریف کرده باشید (نصب و راه‌اندازی کامل Domain Controller در قسمت راه‌اندازی VPN Server در ویندوز ۲۰۰۸ (بخش دوم) مفصل توضیح داده شده است)، پنجره Active Directory Users and Computers را از مسیر زیر باز کنید.

Start>All Programs>Administrative Tools>Active Directory Users ...

در غیر این صورت و اگر سرور شما در هیچ Domain ای تعریف نشده باشد (و به‌صورت سرور Standalone باشد)، پنجره Computer Management را از مسیر زیر:

Computer Management < Administrative Tools < All Programs < Start

باز کنید و صفحه properties مربوط به کاربری که می‌خواهید اجازه اتصال به VPN سرور خود را به آن بدهید، را باز کنید و مطابق شکل ۷ به قسمت Dial-In بروید و گزینه "Allow access" را انتخاب نمایید.



شکل ۷

به خاطر بسپارید که پیاده‌سازی VPN بار زیادی را روی پردازنده سرور می‌گذارد و هر چقدر تعداد ارتباطات VPN بیشتر باشد بار زیادتری بر روی سرور خواهد گذاشت. می‌توانید از یک وسیله سخت‌افزاری مانند روتر جهت پیاده‌سازی VPN کمک بگیرد.

راه‌اندازی VPN Server در ویندوز ۲۰۰۸ (بخش دوم)

بعد از نصب و راه‌اندازی VPN Server در ویندوز سرور ۲۰۰۸، در این قسمت قصد داریم نحوه اتصال کاربران به شبکه VPN را شرح دهیم.

این اتصال از دو راه صورت می‌گیرد:

• اتصال به شبکه VPN از طریق راه دور، با استفاده از مودم (اتصال به اینترنت تحت پروتکل PPTP)

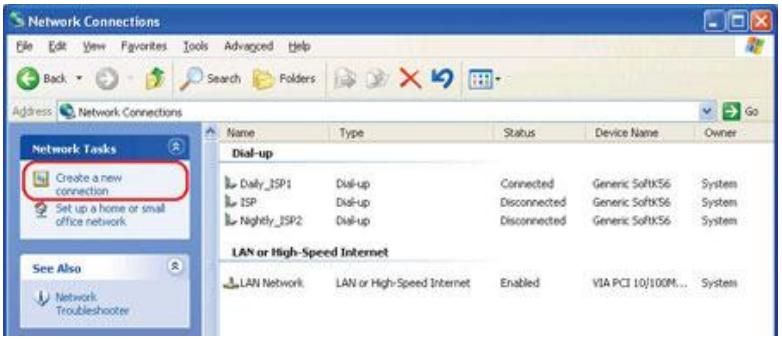
• اتصال به شبکه VPN، با استفاده از کارت شبکه (ارتباط کاربران داخل شبکه با یکدیگر) حتماً به یاد دارید که در هنگام راه‌اندازی VPN Server، در ویندوز سرور ۲۰۰۸، امکان Remote Access را به ویندوز سرور ۲۰۰۸ می‌توان داد، ضمن اینکه به کاربران موردنظر، مجوز اتصال از راه دور را اعطا کردیم. تنظیماتی که در این مقاله برای برقراری ارتباط VPN Client به VPN Server تشریح می‌شود، برای کاربران ویندوز XP Pro ارائه داده شده است. این تنظیمات با کمی اختلاف، برای کاربران ویندوز Professional Windows 2000 نیز قابل انجام است.

برقراری کانال ارتباطی

۱- برای برقراری کانال ارتباطی پنجره Network Connections را از مسیر زیر باز کنید:

Start > Control Panel > Network Connections

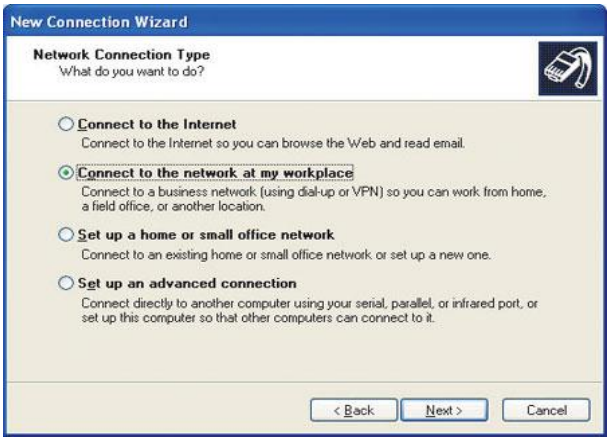
در اینجا لازم است یک آیکن اتصال جدید به شبکه مجازی بسازید برای این کار از منوی File گزینه New Connection را انتخاب کنید؛ و یا مطابق شکل ۸ گزینه Create a new connection را از پانل سمت چپ انتخاب نمایید.



شکل ۸

۲- اولین پنجره اطلاعات اولیه‌ای در مورد خود ویزارد به شما می‌دهد. فقط دکمه Next را بزنید.

۳- پنجره بعدی از شما می‌خواهد که نوع اتصال خود را مشخص کنید. در اینجا مطابق شکل ۹ گزینه "Connect to the network at my workplace" که مربوط به ایجاد اتصال به شبکه VPN می‌باشد را انتخاب کرده و دکمه Next را بزنید.



شکل ۹

همان‌طور که در شکل ۱۰ ملاحظه می‌نمایید از دو راه می‌توان به شبکه وصل شد.

• اتصال از طریق اینترنت

• اتصال از طریق مودم و dial-up: با انتخاب این گزینه، در پنجره‌های بعدی نام مودم، شماره تلفن تماس با سروری که به آن وصل می‌شوید را تعیین خواهید کرد. زمانی که دسترسی به اینترنت ندارید می‌توانید از این روش استفاده نمایید. توجه داشته باشید که این یک اتصال پرخرج می‌باشد مخصوصاً مواقعی که VPN Server در مسیر دوری قرار گرفته باشد.

اما همان‌طور که در شکل ۱۰ مشاهده می‌کنید گزینه دوم (Virtual Private Network) را انتخاب کرده و Next کنید. یک نام را برای این اتصال در نظر می‌گیریم. بهتر است که نام مناسبی را انتخاب کنید. مخصوصاً زمانی که به شبکه‌های مختلف متصل می‌شوید.

شکل ۱۰

۵- مطابق شکل ۱۱ در پنجره Public Network، یکی از خطوط ISP خود را برای برقراری اتصال اینترنتی به VPN Server خود انتخاب کرده و دکمه Next را بزنید. اگر در شبکه داخلی هستید، گزینه اول یعنی Do not dial ... را انتخاب نمایید (شما ازاین‌پس از طریق این کانال اینترنتی به VPN وصل خواهید شد).

شکل ۱۱

۶- مطابق شکل ۱۲ در پنجره Connection Name آی‌پی آدرس یا Host Name سرور VPN را وارد نموده و دکمه Next را بزنید. به‌عنوان‌مثال آی‌پی آدرس سرور داخلی ما 192.168.0.1 می‌باشد.

شکل ۱۲

۷- در آخرین پنجره، خلاصه تنظیمات نمایش داده می‌شود. با زدن دکمه Finish کار ساخت یک VPN Connection به پایان می‌رسد.

تنظیمات کانال ارتباطی

بعد از اتمام مراحل فوق یک پنجره مانند شکل ۱۳، برای اتصال به VPN Server، ظاهر خواهد شد؛ که از شما نام کاربری و کلمه عبور درخواست می‌کند. در واقع تا این مرحله شما فقط یک آیکن اتصال اولیه به شبکه را ساخته‌اید. قبل از اتصال، توضیحاتی در مورد این تنظیمات می‌دهیم

همان‌طور که در شکل ۱۳ می‌بینید، دکمه Properties را بزنید تا در مورد قسمت‌های مختلف توضیحاتی ارائه دهیم.

شکل ۱۳

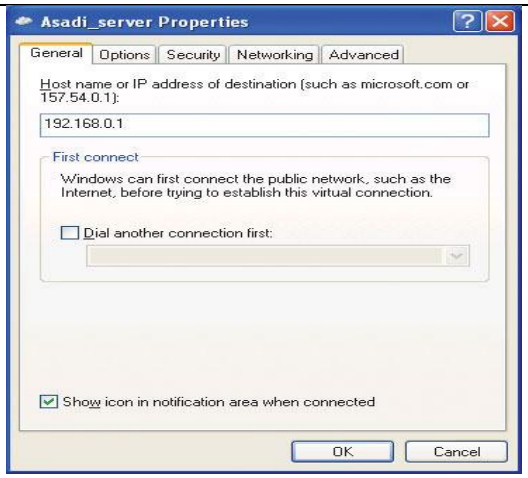
قسمت General

همان‌طور که در شکل ۱۴ ملاحظه می‌کنید این قسمت نیاز به تنظیمات و تغییرات چندانی ندارد. اگر می‌خواهید نام و یا آی‌پی آدرس سروری که می‌خواهید به آن وصل شوید را تغییر دهید، در اولین کادر می‌توانید تغییرات را وارد نمایید. توجه نمایید که ما قبلاً آی‌پی آدرس موردنظر را وارد کرده بودیم. (به شکل ۱۲ دقت کنید.)

همچنین در همین صفحه و در قسمت First Connection می‌توانید تنظیم کنید که کدام‌یک از خطوط ISP را برای برقراری اتصال اینترنتی به VPN سرور می‌خواهید استفاده نمایید. (این گزینه را نیز قبلاً با توجه به شکل ۱۱ تنظیم نموده‌ایم).

توجه: اگر بخواهید به VPN سرور داخل شبکه متصل شوید نیازی به تعریف این گزینه نیست.

در انتها نیز گزینه‌ای مربوط به فعال یا غیرفعال کردن نمایش آیکن آداپتور شبکه در system tray (بعد از برقراری اتصال به شبکه) می‌باشد.



شکل ۱۴

قسمت Options

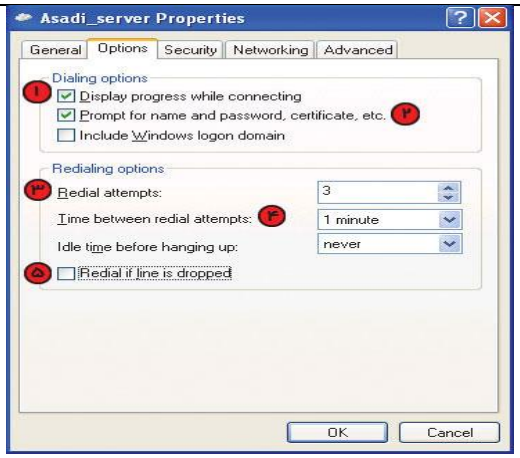
همان‌طور که در شکل ۱۵ مشاهده می‌نمایید در این قسمت عملیاتی که در هنگامی برقراری اتصال انجام می‌شود را می‌توان تنظیم نمود. برخی از این تنظیمات در قالب سؤال‌های زیر نشان داده شده است.

- آیا سیستم وضعیت اتصال را به شما نشان دهد یا خیر؟
- نام کاربری، کلمه عبور و نام domain را درخواست کند یا خیر؟

و با گزینه‌هایی که در قسمت Redialing Options وجود دارد، عکس‌العمل سیستم در مقابل عدم دریافت پاسخ از طرف سرور را می‌توانید تنظیم نمایید:

- در صورت عدم دریافت پاسخ از سرور، چند بار سعی برای اتصال صورت گیرد؟
- تنظیم فاصله زمانی بین هر سعی با سعی دیگر
- اگر اتصال ناخواسته قطع شد، آیا مجدداً برقرار شود یا خیر؟

در حالت عادی نیازی به تغییر در این برگه نیست.



شکل ۱۵

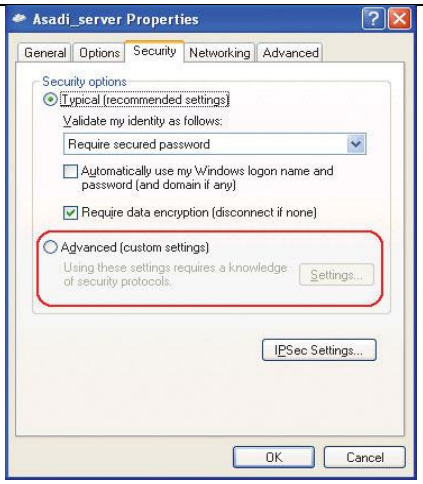
قسمت Security

همان‌طور که در شکل۱۶ می‌بینید در این قسمت می‌توانید امنیت اتصال خود را تنظیم کنید. اگر طبق دستورالعمل‌های داده شده در VPN Server تنظیمات را انجام داده باشید نیازی به تغییر در اینجا احساس نمی‌شود مگر اینکه بخواهید امنیت بیشتری را در نظر بگیرید. برای انجام این کار گزینه Advanced را انتخاب نموده و سایر تنظیمات را برحسب نیاز انجام دهید. (توضیحات تک‌تک گزینه‌های آن خارج از بحث این کتاب می‌باشد).

توجه: این گزینه زیر را فعال نکنید:

Automatically use my Windows logon name and password

اگر این گزینه در کامپیوتر فعال باشد و این کاربر به قصد استراحت، برای مدت کوتاهی کامپیوتر را رها کرده باشد. هر کسی می‌تواند از طریق این کامپیوتر به شبکه (VPN Server) وصل شود. زیرا با فعال کردن این گزینه عملاً نیاز به تایپ نام کاربری و کلمه عبور برای ورود به سرور را از بین برده‌اید.

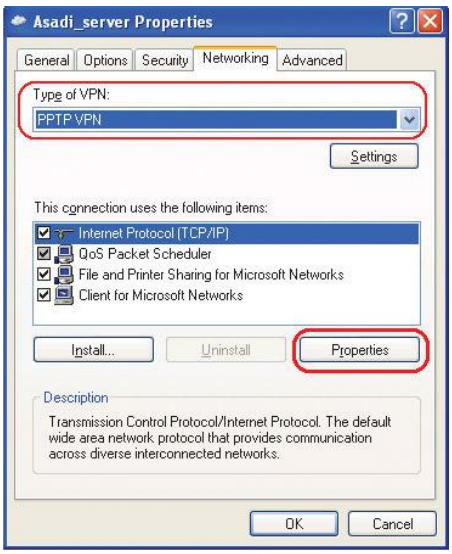


شکل ۱۶

قسمت Networking

در این برگه تنظیمات مختلفی می‌توان انجام داد. همان‌گونه که در شکل ۱۷می‌بینید اولین تنظیم مربوط به نوع اتصال VPN شما می‌باشد. به‌صورت پیش‌فرض Automatic انتخاب شده است که هر دو حالت PPTP VPN و L2TP VPN را به ترتیب بررسی می‌نماید.

PPTP برای کاربردهای عمومی و غیرحرفه‌ای مناسب‌تر می‌باشد. پروتکل L2TP که به‌وسیله شرکت CISCO ارائه شده است به لحاظ امنیتی بسیار قدرتمندتر است. پروتکل دیگری را به نام IPSec پایه‌ریزی شده است که پیچیدگی‌های خاصی دارد. ما در اینجا از پروتکل PPTP استفاده می‌کنیم که تنظیمات راحت‌تری دارد.



شکل ۱۷

یکی دیگر از تنظیمات، تعیین اینکه آیا می‌خواهید برای اتصال به شبکه VPN از Default Gateway استفاده شود یا نه؟ برای این کار می‌توانید، با توجه به شکل ۱۷ پس از انتخاب Internet Protocol (TCP/IP) و سپس زدن دکمه Properties ازآنجا دکمه Advanced را بزنید (به شکل ۱۸ دقت کنید) تا گزینه‌ای مانند آنچه در شکل ۱۹ نشان داده شده را پیدا نمایید.

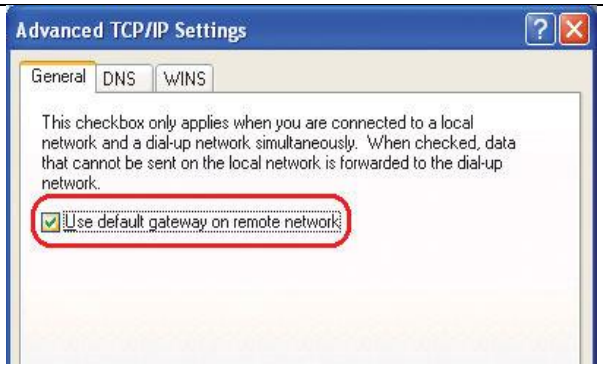
در این گزینه به‌صورت پیش‌فرض تیک خورده و فعال است. ممکن است که برایتان این سؤال پیش بیاید که چه زمانی این گزینه فعال و چه زمانی غیرفعال کنیم؟

بعضی از کاربران در خانه و یا بعضی‌ها در کافی‌نت‌ها و یا هتل و غیره... و از راه اینترنت به VPN وصل می‌شوند. این‌گونه افراد برای اتصال به شبکه VPN، در واقع از راه دور (Remote) به VPN Server وصل می‌شوند؛ بنابراین با فعال کردن این گزینه یک مسیری برای آن‌ها ایجاد کرده‌اید که بتوانند بدون مشکل وصل شوند.

توجه:

برای کاربران داخلی (کاربران داخل شبکه) که از یک محدوده خاصی از IP آدرس استفاده می‌کنند، گزینه "Use default gateway on remote network" را غیرفعال کنید.

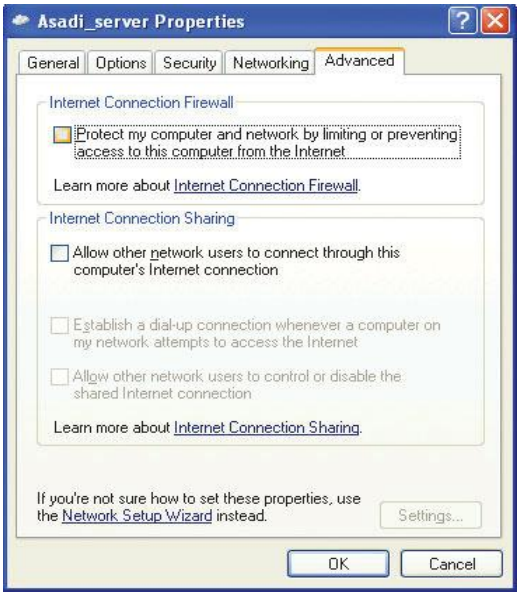
شکل ۱۸



شکل ۱۹

قسمت Advanced

در اتصال معمولی و ساده به شبکه VPN، این قسمت نیاز به تنظیمات خاصی ندارد.



شکل ۲۰

بعد از انجام تنظیمات لازم نوبت به برقراری ارتباط می‌رسد. دکمه Connect در پنجره اصلی را بزنید (به شکل ۱۳ دقت نمایید). چنانچه تنظیمات VPN Server و VPN Client را به‌درستی انجام داده باشید. اتصال با موفقیت انجام می‌شود و آیکنی مشابه آیکن اتصال به اینترنت در System Tray ظاهر می‌شود؛ که می‌توانید خصوصیات اتصال خود را با زدن دکمه Properties مشاهده کنید. با این اتصال مانند آن است که خود در سرور قرار گرفته باشید؛ و از امکانات آن استفاده نمایید.

نتیجه گری

مفید باشند، به‌طوری‌که دیگر به داشتن یک شبکه خصوصی کامل که منابع زیادی را برای پیاده‌سازی استفاده می‌کند، نیازی نباشد. از طرفی وقتی یک شبکه‌ای خصوصی مجازی برای داشتن ارتباط با همدیگر، مسأله اشتراک IPاینترنت سوار می‌شود و بسته‌های آن آدرس backbone دنیای شبکه‌های خصوصی مجازی با داشتن معماری مدیریتی مناسب و پیاده‌سازی صحیح، می‌توانند برای سازمان‌ها اینترنت بر روی منابع پیش می‌آید و ممکن است، در اختیار قرار دادن منابع برای درخواست‌ها در همه زمان‌ها امکان‌پذیر نباشد. بنابراین باید توابعی را برای تضمین کیفیت سرویس در این شبکه‌ها به کار ببریم. بنابراین ضرورت مدیریت این شبکه‌ها در مقایسه با شبکه‌هایی که برای کیفیت سرویس تضمین پایین‌تری دارند، بسیار محسوس است.

منابع

تمامی این مقاله صرفا از کتاب رهبر زارعی با عنوان کتاب شبکه‌های خصوصی مجازی VPN که در سال چاپ ۱۳۹۷ چاپ گردیده تخلیص شده است.