آموزش راه اندازی RADIUS سرور در ویندوز سرور ۲۰۰۸ - قسمت اول (نسخه PDF)

پروتکل RADIUS برگرفتـه شـده از (Remote Authentication Dial-In User Service) ، اسـتانداردی برای طراحی و پیـاده سـازی سـرویس دهندگانی است که مسـئولیت تائید و مدیریت کاربران را برعهده خواهند گرفت.مشخصات و نحوه عملکرد پروتکل RADIUS در RFC ۲۸۶۵ و RFC ۲۸۶۶ تعریف شده است. پروتکل RADIUS از یک معماری سـرویس گیرنده - سرویس دهنده برای تائید و accounting استفاده می نمایـد . پروتکـل فوق اطلاعات accounting ، پیکربنـدی ، تائیـد و مجوزها را بین یک سـرویس گیرنـده RADIUS و یک سـرویس دهنده RADIUS حمل می نمایـد . سـرویس گیرنده RADIUS می توانـد یک سـرویس دهنده دستیابی شـبکه (NAS ، برگرفته شـده از network access server) و یا هر نوع دستگاه مشابه دیگری باشد که نیازمند تائید و accounting است.

همانگونه که اشاره گردید NAS به عنوان یک سرویس گیرنده RADIUS عمل می نماید . سرویس گیرنده مسئول ارسال اطلاعات کاربر برای سرویس دهنده RADIUS است تا بر اساس نتایج برگردانده شده توسط سـرویس دهنده ، در خصوص کاربر تعیین تکلیف گردد . سرویس دهندگان RADIUS مسـئول دریافت درخواست ارتباط کاربر ، تائید وی و ارسال اطلاعات پیکربندی مورد نیاز برای سرویس گیرنده به منظور عرضه سـرویس به کاربر می باشـند . یک سـرویس دهنده RADIUS می تواند به عنوان یک سـرویس گیرنده پراکسـی به سایر سـرویس دهندگانRADIUS و یا سایر سـرویس دهندگان تائید نیز عمل نماید. سرویس گیرندگان RADIUS از طریق پورت های ۱۸۱۲ و ۱۸۱۳ پروتکل حمل UDP برگرفته شده از (User Datagram Protocol) با یک سرویس دهنده RADIUS ارتباط برقرار می نمایند . در نسـخه های اولیه پروتکل RADIUS از پورت هـای ۱۶۴۶ و ۱۶۴۵ پروتکل UDP اسـتفاده می گردید . پروتکل RADIUS از پروتکـل حمل TCP برگرفته شده از (Transmission Control Protocol) حمـایت نمی نمایـد. پس از اینکه یـک کاربر اعتبار لازم جهت ایجاد یک ارتباط دسترسـی از راه دور را فراهم نمود، این ارتباط باید توسط یک سـرور، ویندوز سـرور ۲۰۰۸ که اجرا کننده سـرویس NPS (Network Policy Server) باشد تصویب شود، و یا توسط یک سرویس احراز هویت و تصدیق هویت دیگری مثل RADIUS) Remote Authentication Dial-In User Service) تصویب شود. مجوز دسترسی از راه دور شامل دو مرحله می باشد:

۱. ارزیابی مشخصات شماره گیری مرتبط با کاربر
۲. ارزیابی هر گونه NPS که در مقابل RRAS اعمال می شود.

پیاده سازی یک سرور RADIUS یک NPS می باشد . از یک سرور RADIUS به منظور متمرکز سازی عملیات احراز هویت (authentication) ، تصدیق هویت (authorization) و ورود کاربر اسـتفاده نمایید. زمانی که شـما یک سرورRADIUS را پیاده سازی می کنیـد ، چندین کامپیوتر اجرا کننده سرویس RRAS می توانند درخواستهای در دسترس خود را به سرور RADIUS ارسال نمایند. و سپس سرور RADIUS برای انجام فرایند تصدیق و اعمال NPS به درخواستهای ارتباط با دامین کنترلر تماس گرفته و برای آن درخواست ارسال می کند.مفاهیم احراز هویت و تصدیق هویت اغلب مورد اشـتباه قرار می گیرند. احراز هویت فرآیندی است که ارزیابی می کند موجودیت یا شـیء خاصی نسبت به آنچه ادعـا می کنـد چیست و یـا کیست .مثـال ها شامل تطابق منبع اطلاعات و تمامیت و درستی اطلاعات می باشـد مثل ارزیابی یک امضای دیجیتالی یا ارزیابی شـناسه یک کاربر یا یک کامپیوتر ، تصـدیق هویت فرآیندی است که مشـخص می کند یک کاربر بر روی شـبکه یا یک سیسـتم کامپیوتری چه کاری را اجازه دارد انجام دهـد. بطور طبیعی ، فرآینـد تصدیق هویت پس از انجام موفقیت آمیزفرایند احراز هویت رخ می دهد. به علاوه اغلب سیسـتم های دسترسـی از راه دور شامل یک بخش بررسی نیز می باشد که دسترسی به منابع را Log می کند. به طور خلاصه :

- احراز هویت اثبات می کند که کاربر کیست یا چیست ؟
- تصدیق هویت کنترل می کند که کاربر تصویب شده به چه منابعی حق دسترسی دارد و به چه منابعی ندارد.
- Accounting پیگیری می کند که کاربر به چه منابعی دسترسی پیدا کرده یا تلاش کرده تا دسترسی پیدا کند.

مشـخصات شماره گیری (dial-in) ، که به طـور مسـتقیم به هر ارتبـاط VPN و dial-up اعمـال می شـود. از طریـق برگه dial-in مربوط به properties حساب کاربری قابل تنظیم است . اگر کاربری اقدام به برقراری تماس با دامنه ای نماید،نام کاربری ارسال شده برای ارتباط -dial up باید در دامنه موجود باشد و با آن مطابقت داشـته باشد. مسـخصات شـماره گیری مربوط به این حساب کاربری همچنین می تواند در کنسول Active Directory Users and Computers نیز تنظیم شوند. اگر کاربر اقدام به شماره گیری به یک سرور stand-alone نماید ،باید یک حسـاب کـاربری درون پایگاه داده SAM) Security Accounts manager) مربوط به سـرور پاسـخگو وجود داشـته باشد. SAM یک سرویس ویندوز است که در مدت فرآیند ورود مورد اسـتفاده قرار مـی گیرد. SAM اطلاعات مربوط به حساب کاربری را نگهـداری مـی کنـد که حتـی

شامـل گروهی که کاربر عضو آن است نیز می شود. مشـخصات مربوط به شـماره گیری این حساب کاربری نیز می توانـد در کنسول Local Users And Groups در Computer Management تنظیم شود . درویندوز ۲۰۰۸ گزینه Control access through NPS Network Policy به صورت پیش فرض فعال شده است .شما می توانید اجازه دسترسی از راه دور را برای حسابهای کاربری در یکی از سه سطح زیر تنظیم نمایید:

- **Control access through NPS Network Policy** : این گزینه خاص نه اجازه دسترسی dial-up به کاربر را می دهـد و نه مانع از دسترسی کاربر می شود. در عوض ،آن مشخص می کند که کاربر مجوزهای دسترسی تعیین شده توسط اولین ماشین سیاست شبکه NPS اعمال شده برای اتصال را داشته باشد (به صورت پیش فرض،ساست شبکه NPS مانع از دسترسی تمامی ارتباطات دسترسی از راه دور می شود).
- **Deny access** : اگر شـما این گزینه را انتخـاب نماییـد، دسترسـی dial-up برای حسـاب کـاربری بلـوکه می شـود: علی رغم دیگر تنظیمات یا سیاست هایی که به حساب کاربری اعمال می شود.
- **Allow access** : زمانی که شـما این گزینه را انتخاب کنید دسترسی از راه دور dial-up برای حساب کاربری اجازه داده می شود که در نتیجه تنظیمات دسترسـی از راه دور در سـیاست شـبکه NPS نیز لغو می شود. دقت داشـته باشـید که تنظیمـات Allow access همیشه از سیاست شبکه NPS که مانع دسترسـی از راه دور شود جلوگیری نمی کند. یک سیاست شبکه ای NPS همچنان می تواند دسترسـی از راه دور حساب ها را از طریق پروفایل ساست شبکه NPS محدود کند. برای مثال ، ساعات اتصال مشـخص شده در یک پروفایل سیاست شبکه NPS از دسترسـی کاربر برای ارتباط در ساعات عصـر جلوگیری می کند، حتی در صورتیکه گزینه Allow access برای حساب کاربری درون مشـخصات شماره گیری تنظیم شده باشد. به هر حال ،گزینه Allow access مشخص می کند که تنظیمات مربوط به Deny Remote Access Permission درون سیاست شبکه ای NPS نادیده گرفته می شوند.

اگر گزینه Verify Caller- ID انتخاب شده باشد، سـرور شما هر تلفن تماس گیرنده را ارزیابی می کند. اگر شماره تلفن با شماره تلفن تنظیم شده مطابقت نداشـته باشد،تلاش برای برقراری ارتباط با شـکست روبرو می شود. توجه داشته باشید که تماس گیرنده ،سیستم تلفنی بین تماس گیرنده و سـرور و نیز سرور دسترسی از راه دور باید از تکنولوژی callrr ID پشتیبانی نمایند. بر روی یک کامپیوتر اجرا کننده سرویس RRAS ، پشتیبانی از caller ID شامل تجهیزات call answering (پاسخگوی تماس) می باشد، که اطلاعات مربوط به شناسه تماس گیرنده و نیز درایور ویندوز متناسب جهت گذر اطلاعات به سـمت سرویس RRAS را فراهم می کند. اگر شـما شماره تلفن یک تماس گیرنده را برای یک کاربر تنظیم می کنید ولی شما از گذر اطلاعات caller ID از تماس گیرنده به سمت سرویس RRAS پشتیبانی نکنید،تلاش برای برقراری ارتبـاط با شـکست روبرو می شود.به صورت پیش فرض، Callback Options به صورت No Callback تنظیم شـده است ، اگر گزینه Set by Caller انتخاب شده باشد،سـرور یا تماس گیرنده با شـماره مشخص شده توسط تماس گیرنده تماس می گیرد. اگر گزینه Always Callback to : انتخاب شده باشد، مدیر شبکه باید شماره ای را مشخص کند که سرور در مدت فرآیند Callback همیشه از آن استفاده نماید. به علاوه ، شـما می توانیـد برای این کار یک و یا چند آدرس IP ثابت را پیکربنـدی کنید برای هر زمانی که کاربر به یک سـرور دسترسـی از راه دور متصل می شود.

اعمال سیاستهای شبکه ای NPS

یک سیاست شبکه NPS مجموعه ای از مجوزها و محـدودیت ها است که توسط یک سـرور تصدیق دسترسـی از راه دور خوانده شده و به اطلاعات دسترسـی از راه دور اعمال می شود. مجوزهای دسترسی از راه دور به آسانی قابل درک می باشند و در ویندور NT۴.۰ و ویندوز NT ۳.۵۱ پیـاده سـازی شـده انـد. مجوزهـای دسترسـی از راه دور به صورت مسـتقیم به حسابهای مربوط به کاربران و از طریق ابزارهای User Manager و یا Remote Access Administration اعطـا می شود، که این امری سـاده و آسـان می باشـد و البته در صورتی که هر چه تعـداد کاربران نیازمند اعطای کمتر باشد، ایده آل تر کار خواهد کرد. در ویندوز سرور ۲۰۰۸ ، ویندوز سرور ۲۰۰۳ و ویندوز ۲۰۰۰ سرور تصدیق هویت از راه دور پیچیـده تر می باشـد و در نتیجه تلاش بیشتری را برای درک آن نیازمنـد است . به هر حال ، قدرتمند تر بوده و نیازهای امنیتی بیشتری را برای سازمان های کوچک و بزرگ فراهم می کند.

- **نکته امنیتی** : پیکربندی سیاستهای شبکه ای NPS در پیـاده سازی کنترل های تصـدیق هویت کاربر برای اتصالات بیرونی، کنترل اتصال به شـبکه ، خروج زمانی از لایه ارتباطی و محدود سازی زمان اتصال ،محاسـبه و ارتباطات سیار در استاندارد سیستم مدیریت امنیت اطلاعات تأثیرگذار می باشد.
- **نکته** : سیاسـتهای شبکه ای NPS در ویندوز سرور ۲۰۰۸ با سیاسـتهای دسترسـی از راه دور درون ویندوز سرور ۲۰۰۳ و ویندوز ۲۰۰۰ سرور قابل مقایسه است.

سرور قابل شناسه است.

همانطور که پیش از این ذکر شد، تصدیق هویت توسط ترکیب مشـخصات شماره گیری مربوط به حساب کاربری و نیز گروه ها، زمان ،نوع ارتباط درخواست شده و دیگر متغیرها ، تصویب می شود و یا با شـکست مواجه می شود. با استفاده از NPST ، یک کامپیوتر ویندوز سرور ۲۰۰۸ می تواند به عنوان یک سرور RADIUS عمل کند و عملیات احراز هویت ، تصدیق هویت و accounting را برای دستیابی به منابع شبکه ای انجام دهد.

پیکربندی یک سیاست شبکه NPS

یک سیاست شبکه ای NPS ، که در حقیقت قانونی برای ارزیابی ارتباطات راه دور می باشد دارای سه بخش می باشد: Conditions (شرایط) ، Constrains (محدودیت ها) و Settings (تنظیمات) . شما می توانید در مورد یک سیاست شبکه NPS به عنوان یک قانون برای اجازه یا عدم اجازه دسترسی از راه دور فکر کنید: ویندوز سرور ۲۰۰۸ هر گونه تلاش برای برقراری ارتباط با قوانین پیکربندی شده درون هر سیاست شبکه ای NPS را مقایسه می کنـد. اگر شـرایط و محـدودیت های تعریف شـده توسط ارتباط درخواستی با موارد تنظیم شده در سیاسـت شبکه ای مطابقت داشـته باشـد سـرور دسترسـی از راه دور به برقراری ارتباط اجازه می دهد یا اجازه نمی دهد و سـپس تنظیمات اضافی دیگری را همان گونه که توسط سـیاست تعریف شـده است نیز پیکربنـدی می کنـد. هر کـدام از سـیاست های دسترسـی از راه دور دارای تنظیمات مرتبط به مجوزهای دسترسی (Access permission) می باشـند که مشخص می کند آیا ارتباط منطبق با سیاست اجازه داده شود یا خیر.زمانی که کاربری اقدام به اتصال به یک سـرور دسترسـی از راه دور می کند، فرآیند زیر که در شکل توضیح داده شده است اتفاق می افتد:

۱. کاربر تلاش می کند تا یک ارتباط دسترسی از راه دور را آغاز نماید.
۲. سرور دسترسی از راه دور شرایط درون اولین سیاست شبکه ای NPS پیکربندی شده را چک می کند.
۳. اگر شـرایط بالا هماهنگ و مطابقت نداشـته باشد، سرور دسترسی از راه دور دیگری سیاست شبکه ای NPS باقی مانده را چک می کند تا زمانی که یک هماهنگی پیدا کند.
۴. هنگامی که سـرور دسترسـی از راه دور دریابد که تلاش وارده برای برقراری ارتباط با سیاست شبکه NPS مطابقت دارد،آنگاه سرور هر گونه محدودیت هایی را که برای این سیاست تنظیم شده است را چک می کند.
۵. اگر ارتباط درخواست شده با هیچ یک از محدودیت های تنظیم شده هماهنگی نداشته باشد- زمان در روز ، حداقل سطح رمزگذاری و غیره – آنگاه سرور دسترسی از راه دور این ارتباط را از بین می برد.
۶. اگر ارتباط درخواست شده با شـرایط و محدودیت های تنظیم شده با یکی از سـیاست هاس شبکه ای NPS خاص، هماهنگی داشته باشد، آنگاه سـرور دسترسـی از راه دور بر اساس مجوزهای دسترسـی پیکربندی شده برای آن سیاست به آن ارتباط اجازه می دهد یا اجازه نمی دهد.

سیاست شبکه ای NPS بر روی هر سرور دسترسی از راه دور تدارک دیده می شود و هر سیاست از بالا به پایین ارزیابی می شود. قرار دادن سیـاست هـا به ترتیب درست ، از اهمیت خاصـی برخوردار است ، چرا که به محض اینکه سـرور RRAS یک هماهنگی را پیـدا کند، فرآیند پردازش دیگر سـیاست ها را متوقف می سازد. برای مثال، اگر شـما یک سـیاست شبکه NPS را به این صورت داشـته باشید که << تمامی ارتباط ها بین ساعات ۸ صبح تا ۵ بعداز ظهر نادیده گرفته شوند>> و به عنوان اولین سـیاست تنظیم شده باشد، آنگاه سرور RRAS تمامی ارتباطات در مدت زمان مشـخص شده را نادیده می گیرد، حتی اگر شـما سیاست مهمتری در پایین لیست داشته باشید. به عنوان بهترین کار، سیاست های شبکه NPS بایـد طوری مرتب شوند که سـیاست های خاص تر در بالای لیست قرار بگیرند و سـیاست های غیرخاص در پایین لیست قرار بگیرد و به این ترتیب سیاست ها به صورت صحیح پردازش می شوند.

برای مثال ، شما ممکن است دو سیاست را به صورت زیر داشته باشید:

۱. اگر یک کاربر عضو گروه"Remote Consultant" باشد ، بدون توجه به زمان ، ارتباط اجازه داده شود.
۲. تمامی ارتباط های بین ساعت ۸ صبح تا ۵ بعد از ظهر از روز دوشنبه تا جمعه بدون توجه به دیگر شرایط نادیده گرفته شود.

در این سناریو، یک عضو گروه Remote Consultant قادر به برقراری ارتباط در ساعت ۱۰ صبح روز شنبه خواهد بود . چرا که با سیاست شماره یک مطابقت دارد و قبل از سـیاست شـماره دو پردازش می شود. اگر کاربری عضو گروه مـذکور نباشـد ، با سـیاست شـماره یک هماهنگی نخواهد داشت و سـیاست شـماره تأثیرگذار می باشد.در ویندوز سرور ۲۰۰۸ به صورت پیش فرض دو سـیاست شبکه NPS پیکربندی شده

است. اولین سیاست پیش فرض، مربوط به ارتباطات Routing and Remote Access Server مایکروسافت می باشد، و برای هماهنگی تمامی ارتباط های دسترسی از راه دور با سرویس RRAS پیکربندی شده است . زمانی که RRAS این سیاست را مطالعه می کند، سیاست به صورت طبیعی با هرگونه ارتباط ورودی تطابق پیدا می کند. اگر یک سرور RADIUS و یا یک مکانیزم احراز هویت Third – party (سوم شخص تصدیق کننده) دیگری این سیاست را مطالعه کند دسترسی شبکه ممکن است توسط یک سازنده غیرمایکروسافتی تدارک دیده شود. در نتیجه این سیاست با آن ارتباطات مطابقت نخواهد داشت.

دومین سیاست پیش فرض مربوط به ارتباطات دیگر سرورهای دسترسی از راه دور می باشد این سیاست برای تطابق و هماهنگی هرگونه ارتباط ورودی بدون توجه به نوع سرور دسترسی به شبکه ، پیکربندی شده است به دلیل اینکه اولین سیاست با تمامی ارتباطات ارسالی به سرور RRAS هماهنگی دارد، این سیاست تنها زمانی موثر است که ارتباط ورودی توسط یک سرور RADIUS یا مکانیزم احراز هویت دیگری، تصدیق شده باشد.

پیکربندی شرایط اعمال سیاست

هر سیاست شبکه NPS براساس شرایط سیاستی می باشد که مشخص می کند چه زمانی سیاست باید اعمال شود . برای مثال ، یک سیاست ممکن است حاوی شرطی معین براین باشد که Windows Groups با WINGTIPTOYS\\Telecommuters هماهنگ باشد . این سیاست سپس ممکن است با یک ارتباط مربوط به کاربری عضو گروه امنیتی Telecommuters هماهنگی و مطابقت کند.با کلیک کردن بر روی دکمه Add درون کادر محاوره ای select Attribute از برگه conditions، شما می توانید یک گروه جدید برای یک شرط سیاست دسترسی از راه دور، اضافه نمایید.

- **نکته:** تنها عضویت در گروه های global security می تواند به عنوان یک شرط سیاست از راه دور خدمت کند. شما نمی توانید عضویت در گروه های امنیتی domain local و یا universal را به عنوان شرطی برای یک سیاست دسترسی از راه دور مشخص کنید.

پیکربندی تنظیمات اعمال سیاست

یک پروفایل سیاست شبکه NPS حاوی مجموعه ای از تنظیمات و مشخصات است که می توانند به یک ارتباط اعمال شوند. شما می توانید یک پروفایل NPS را از طریق کلیک کردن بر روی برگه Settings در صفحه Properties سیاست ، پیکربندی نمایید. نمونه ای از تنظیمات سیاست NPS حاوی مشخصات IP است که رفتار تخصیص آدرس IP را مشخص می کند. شما دارای گزینه های زیر می باشید:

- سرور باید یک آدرس IP را تدارک ببیند.
- کاربر ممکن است یک آدرس IP را درخواست نماید.
- تنظیمات سرور تخصیص آدرس IP را مشخص می کند. (تنظیمات پیش فرض)
- یک آدرس IP ثابت را تخصیص دهید. آدرس IP تخصیص داده شده به طور نمونه برای تطابق با ویژگی های مشخص شده توسط تولید کننده (سازنده) برای آدرس های IP، استفاده می شود.

به علاوه شما می توانید مشخصات مربوط به multilink را نیز تنظیم کنید که یک ارتباط دسترسی از راه دور را قادر می سازد تا از چندین مودم برای تنها یک ارتباط استفاده کند و حداکثر تعداد پورت هایی(مودم) را که یک ارتباط multilink می تواند استفاده کند را مشخص می کند،همچنین می توانید سیاستهای مربوط به Bandwidth Allocation Protocol(BAP) را نیز تنظیم کنید که کاربرد و استفاده از BAP و اینکه چه زمانی خطوط BAP اضافه یا حذف شوند را مشخص می کند. تمامی مشخصات مرتبط با multilink و BAP در سرویس RRAS مشخص شده است. به صورت پیش فرض BAP وmultilink به صورت غیرفعال می باشند. سرویس RRAS به منظور اجرای ویژگیهای مربوط به پروفایل multilink باید این دو کاربرد را فعال کند.در نهایت چهار روش رمزنگاری در برگه Encryption در دسترس می باشد:

- **Basic Encryption (MPPE ۴۰-Bit)** : برای ارتباطات dial-up و VPN مبتنی بر PPTP می باشد و این روش با یک کلید ۴۰ بیتی مورد استفاده قرار می گیرد. در ارتباطات VPN مبتنی بر L۲TP/IPSec روش DEC با ۵۶ بیت مورد استفاده قرار می گیرد.
- **Strong Encryption (MPPE ۵۶-bit)** : برای ارتباطات dial-up و VPN مبتنی بر PPTP می باشد که با یک کلید ۶۶ بیتی مورد استفاده قرار می گیرد. و برای ارتباطات VPN مبتنی بر L۲TP/IPSec مانند DEC با ۵۶ بیت استفاده می شود.
- **Strong Encryption (MPPE ۱۲۸-bit)** : برای ارتباطات dial-up و VPN مبتنی بر PPTP مانند MPPE با کلید ۱۲۸ بیتی مورد استفاده قرار می گیرد. برای ارتباطات VPN مبتنی بر L۲TP/IPSec ، روش Triple DES با ۱۶۸ بیت استفاده می شود.
- **NC Encryption** : این گزینه به ارتباط های رمزگذاری نشده ای اجازه می دهد که با شرایط مربوط به سیاست دسترسی از راه دور هماهنگی دارند. برای استفاده از رمز گذاری علامت این گزینه را بردارید.

انتخاب پروتکل احراز هویت

برای احراز هویت یا تصدیق کردن اعتبار ارائه شده توسط ارتباطات dial-up ابتدا سرور دسترسی از راه دور باید با کاربران طبق یک پروتکل احراز هویت رایـج مـذاکراتی را انجام دهـد. اغلب پروتکل های احراز هویت برخی معیارهای امنیتی را در نظر می گیرند که اعتبارات کاربر می تواند در آنها نفوذ کند. پروتکل های احراز هویت به کاربران در سـرورهای تحت سیسـتم عامل ویندوز اولویتی بر اساس سـطح امنیتی تخصیص می دهند.در زیر لیست کاملی از تمامی پروتکل های احراز هویت (به ترتیب از امن ترین تا کم ترین امنیت لیست شده اند)، که توسط سرویس RRAS در ویندوز سرور ۲۰۰۸ پشتیبانی می شوند آمده است :

- **EAP -TLS :** یک روش احراز هویت مبتنی بر گواهینامه است که براساس EAP بوده و دارای یک چارچوب توسعه پذیر است که در روش های جدید احراز هویت پشتیبانی می شود. EAP-TLS برای ترکیب با کارت های هوشمند استفاده می شود. این روش هم از رمز نگاری داده های احراز هویت و هم از داده های مربوط به برقراری ارتباط پشتیبانی می کنـد، دقت داشـته باشـید که سـرورهای stand-alone روش EAp-TLS را پشتیبانی نمی کنند و سرور دسترسی از راه دور که ویندوز سرور ۲۰۰۸ را اجرا می کند باید عضوی از یک دامنه باشد.
- **MS-CHAP v۲ :**یـک روش احراز هویت دو جانبه است که رمز نگاری هم داده های مربوط به مکانیزم احراز هویت و هم داده های مربوط به برقراری ارتباط را ارائه می کند. یک کلید رمز گزاری جدید برای هر ارتباط و هر مسـیر انتقال ، مورد استفاده قرار می گیرد. این روش به صورت پیش فرض در ویندوز ۲۰۰۰ ، ویندوز XP ، ویندوز سرور ۲۰۰۳، ویندوز سرور ۲۰۰۸ فعال شده است.
- **MS-CHAP v۱ :** یـک روش احراز هویت یـک جـانبه است که رمزنگـاری داده های مربوط به مکانیزم احراز هویت و هم داده های مربوط به ارتباط را ارائه می دهد. یک کلید رمزنگاری مشابه نیز در تمامی ارتباطات مورد استفاده قرارا می گیرد. روش MS-CHAP v۱ از کاربرهای قدیمی تر مثل ویندوز ۹۵ و ویندوز ۹۸ نیز پشتیبانی می کند.
- **Extensible Authentication Protocol =Message Digest ۵ Challenge Handshake Authentication Protocol (EAP-MD۵ CHAP :** یک نسـخه از روش CHAP (به گزینه های بعـدی توجه کنیـد.) است که به چارچوب EAP راه پیـدا می کند. EAP-MD۵ CHAP رمزنگـاری داده هـای احراز هـویت را از طریق اسـتاندارد hash کردن MD۵ پشتیبـانی می کنـد و سازگـاری با کاربران غیرمایکروسافتی ماننـد کاربران اجرا کننده Mac OSX را فراهم می کنـد. این روش از رمزنگـاری داده هـای مربوط به برقراری ارتباط پشتیبانی نمی کند.
- **Challenge Handshake Authentication Protocol (CHAP) :** یـک روش احراز هویت عمومی است که امکـان رمزنگاری داده های احراز هویت را به وسیله hash کردن مربوط به MD۵ ارائه می کند.
- **CHAP** همچنین سازگـاری با کاربر غیر مایکروسافتی را فراهم می کنـد. Group Policy که بـا اسـتفاده از این احراز هویت به حساب های کاربری اعمال می شود بایـد طوری پیکربندی شود که کلمه های عبور را با اسـتفاده از رمزنگاری برگشت پذیر، ذخیره کند (کلمه های عبور پس از اعمال سـیاست جدیـد مجـددا تنظیم شوند). این روش از رمزنگاری داده های مربوط به برقراری ارتباط پشتیبانی نمی کند.
- **Shiva Password Authentication Protocol (SPAP) :** یک روش احراز هویت رمزنگاری ضعیف می باشد که قابلیت همکاری با محصولات Shiva در شبکه های از راه دور را ارائه می دهد. SPAP از رمزنگاری داده های مربوط به ارتباط پشتیبانی نمی کند.
- **Password Authentication Protocol (PAP) :** یـک روش احراز هـویت عمومی است که از رمزنگـاری داده هـای احراز هویت پشتیبانی نمی کند. اعتبارات کاربر در بسته شبکه به صورت متن معمولی ارسال می شوند، PAP نیز از رمزنگاری داده های مربوط به برقراری ارتباط پشتیبانی نمی کند.
- **Unauthenticated access :** این پروتکـل احراز هویت نمی باشـد، بلکه یک گزینه پیکربنـدی است –زمانی که بر روی NAS تنظیم شود و سیاست دسترسی از راه دور به ارتباط اعمال شود- به ارتباطات دسترسی از راه دور اجازه می دهد تا بدون ارائه مجوز و اعتبار متصل شوند. این گزینه برای اشـکال زدایی یا امتحان برقراری اتصال دسترسـی از راه دور کاربرد دارد. این نوع دسترسی از رمزنگاری داده های برقراری ارتباط پشتیبانی نمی کند.

به صورت پیش فرض ،تمامی تلاش های دسترسـی از راه دور درون یک فایل متنی در مسیر C:\\Windows\\system۳۲\\LogFiles ذخیره می شود، اما شـما می توانید برای گزارش دهی و همبسـتگی رخـدادها به صورت بهینه تر و بهتر آنهـا را درون یک پایگاه داده SQL ذخیره و ثبت نماید.

پیکربندی دسترسی بی سیم

علاوه بر چالش های دسترسی از راه دور به شبکه سازمانی شما، پیشرفت های اخیر در تکنولوژی های سیار نیاز جدیدی را مبتنی بر تأمین امنیت دیگر انواع دسترسی ها به شبکه ایجاد نموده است .موضوع نگران کننده تأمین امنیت دسترسی های بی سیم از استفاده های غیرمجاز و یا جلوگیری از اتصال بازدید کننده ها و مشاورین به یک شبکه غیر ایمن در یک اتاق کنفرانس برای استفاده از منابع حساس می باشد ، که نیاز به داشتن دسترسی ایمن به شبکه سازمان حتی با وجود نام کاربری و کلمه عبور و فرآیندهای محافظتی احراز هویت که در قبل کافی بوده است، احساس می شود.

برای کمک به تأمین امنیت دسترسی های شبکه چه در ارتباطات سیمی و چه در ارتباطات بی سیم انجمن IEEE اقدام به ایجاد استاندارد ۸۰۲.۱X برای کنترل دسترسی به شبکه نموده است. ۸۰۲.۱X مبتنی بر پورت می باشد، یعنی اینکه می توان دسترسی را براساس یک پورت فیزیکی اجازه داد یا نادیده گرفت ، مثل اینکه شخصی فقط به یک پایه wall jack با استفاده از یک کابل اترنت متصل شود و یا براساس یک پورت منطقی مثل اینکه شخصی به یک Access Point بی سیم با استفاده از کارت های WIFI در یک یا چندین کامپیوتر همراه یا وسیله دستی متصل شود.۸۰۲.۱X امنیت مبتنی بر پورت را با استفاده از سه بخش زیر برقرار می کند:

- **Supplicant :** این در حقیقت دستگاهی است که با آن به شبکه دسترسی پیدا می کنید مثل یک کامپیوتر همراه .
- **Authenticator:** این بخش اعبارات و مجوزهای مربوط به احراز هویت را برای supplicant درخواست می کند ، که اغلب یک پورت سوئیچ برای ارتباطات سیمی و یا یک نقطه دسترسی بی سیم می باشد. البته برخلاف آن به طور طبیعی اقدام به انجام فرآیند احراز هویت نمی کند بلکه به جای آن اعتبارات Supplicant را برای سرور احراز هویت ارسال می کند.
- **Authentication Server(AS) :** همانطور که ذکر شد، این همان سروری است که اعتبارات Supplicant را ارزیابی می کند و چگونگی دسترسی یا عدم دسترسی به پورت شبکه ایمن شده ، ۸۰۲.۱X را به authenticator (تایید کننده اعتبار) اعلام می کند. این سرور در یک زیر ساخت ۸۰۲.۱X می تواند توسط یک کامپیوتر ویندوز سرور ۲۰۰۸ نقش NPS یا هر گونه سرور RADIUS دیگری را اجرا کند.

زمانی که یک پورت سیمی یا بی سیم با وجود۸۰۲.۱X امنیت لازم را داشته باشد، قبل از هر گونه اعطای مجوز دسترسی به شبکه ، فرآیند زیر صورت می گیرد:

۱- **authenticator** (پورت سوئیچ یا WAP) یک تلاش برای دسترسی را از سمت یک Supplicant جدید شناسایی می کند(یک کاربر بی سیم یا یک کاربر متصل شده به یک پورت فیزیکی).

۲- authenticator سپس پورت را (خواه فیزیکی یا منطقی)به عنوان unauthorized (غیرمجاز) تنظیم می کند که تنها ترافیک ۸۰۲.۱X قادر به عبور از آن می باشد.

۱. authenticator سپس یک بسته درخواست EAP را به سمت Supplicant ارسال می کند و اطلاعاتEAP آن را درخواست می کند.Supplicant با یک پاسخ EAP به درخواست authenticator پاسخ می دهد، که authenticator آن را به سمت سرور احراز هویت (AS) هدایت می کند.
۲. اگر AS بسته پاسخ را بپذیرد، به authenticator ابلاغ می کند تا پورت را به عنوان authorized(مجاز) تنظیم نماید که در این صورت ترافیک به صورت نرمال از آن عبور خواهد کرد.
۳. در پایان زمانی که Supplicant دیگر از پورت ایمن استفاده نکند، یک پیغام EAP-Logoff را برای authenticator ارسال می کند و پورت به حالت unauthorized(غیرمجاز) بازگردانده می شود.

برای پیکربندی یک ویندوز سرور ۲۰۰۸ برای داشتن دسترسی های بی سیم شما نیازمند انجام موارد زیر می باشید:

۱. کلاینت RADIUS را نصب و پیکربندی نمایید. در این موارد، کلاینت RADIUS یک کامپیوتر با سیستم عاملهای ویندوز ویستا یا XP نمی باشند، بلکه به جای آن کلاینت RADIUS حاوی سرورهای دسترسی به شبکه مثل سوئیچ های منطبق بر ۸۰۲.۱X و Access Point های بی سیم می باشد.
۲. یک یا چند روش احراز هویت را انتخاب نمایید، برای ارتباطات سیمی و بی سیم مبتنی بر ۸۰۲.۱X شما باید یک یا چند روش احراز هویت زیر را انتخاب نمایید:

- الف) EAP با TLS (که معمولاً EAP-TLS نامیده می شوند)
- ب) Protected EAP (PEAP) با MS-CHAP V۲ یا PEAP-MS-CHAP V۲

- ج) PEAP با EAP-TLS (که معمولاً PEAP-TLS نامیده می شوند)

۳. یک سرور NPS ویندوز سرور ۲۰۰۸ را بعنوان یک سرور RADIUS پیکربندی کنید که این شامل سه مرحله زیر میشود:

- الف) از این طریق NPS MMC Scap In ، هر سوئیچ یا نقطه دسترسی بی سیم به بعنوان کلاینت RADIUS را اضافه نمایید.
- ب) سیاست شبکه ای NPS را همان طور که پیش از این ذکر شـد پیکربنـدی کنید تا تعریف کنید. شـرایطی که تحت آنها شـما می توانید دسترسی های شبکه ای را اجازه دهید یا رد کنید.
- ج) Accounting را بروی سرور NPS پیکربندی کنید، چه بروی یک فایل متنی و چه بروی یک پایگاه داده SQL.

نویسنده :

منبع:جزیره سرویس های شبکه مایکروسافت وب سایت توسینسو

حامد اعظمی

آیا امکان راه اندازی radius client در ویندوز های غیر سروری مثل ۷ هست؟

پوریا

سلام

من که در حدی نیستم جواب بدم ولی جواب سوال شما رو فکر کنم بلدم :)

بله هست :) توی تمام ویندوز ها فکر کنم بشه

melika.a

سلام

دوست عزیز

این مقاله ادامه نداره ؟

مطلب اصلی