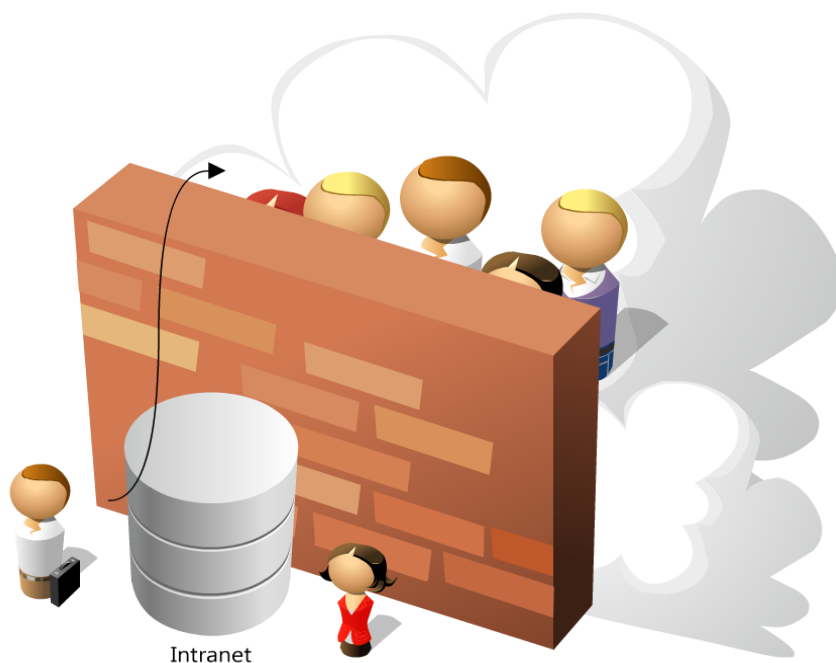




خانه سیتریکس ایران
گروه پال نت

طرح جداسازی اینترنت از شبکه محلی سازمان با استفاده از تکنولوژی مجازی سازی



www.citrixhome.ir ۰۲۱ - ۸۸۱۷۳۳۱۷

info@palnetgroup.ir
www.palnetgroup.ir

مقدمه:

دنیای امروز دنیای اطلاعات است و امروزه زندگی بشر به گونه‌ای شکل گرفته است که در تمامی عرصه‌های حیات، چه در محیط‌های زندگی شخصی و چه در محیط‌های کاری، به شدت در حال دریافت حجم بالای اطلاعات می‌باشد. مدیریت و راهبری سازمانها اعم از دولتی و تجاری و تولیدی در جهان امروز بدون در دسترس بودن آخرین اطلاعات امری بسیار مشکل و بعضا غیر ممکن است. از طرفی استفاده از این شبکه‌ها نیز چندان امن نیست و هر از گاهی اخبار گوناگونی مبنی بر سرقت اطلاعات و داده‌های سازمان‌ها توسط افرادی مختلف از اینترنت شنیده می‌شود. مهمترین چالش پیش روی استفاده از اینترنت می‌توان به مبحث امنیت داده‌های سازمان و کاربران آن اشاره نمود که در این مستند قصد داریم جنبه‌های مختلف از راهکاری را معرفی کنیم که به کمک تکنولوژی‌های نوین و جدید، امنیت صد درصدی را برای داده‌ها و اطلاعات مجموعه‌ها و سازمان‌های مختلف را فراهم می‌نماید.

ضرورت جداسازی اینترنت از شبکه داخلی:

یکی از اصولی ترین مبانی امنیت اطلاعات محافظت از محیط سرویس دهی در فضای سایبر می باشد. از همین رو یکی از مهم ترین دغدغه‌های سازمان‌ها، شرکتها و مراکز دولتی در حال حاضر جداسازی اینترنت از شبکه LAN سازمانی می باشد. مسلما به واسطه این جداسازی به میزان قابل توجهی، از تهدیدات امنیتی کاسته شده و از وقوع مشکلات بسیاری جلوگیری به عمل خواهد آمد. از سوی دیگر استفاده از اینترنت به عنوان یک منبع اطلاعاتی و ارتباطی بسیار ضروری بوده و غیرقابل چشم پوشی است. بنابراین حفظ و پایداری شبکه‌های داخلی و امنیت آن از اهمیت بسیار بالایی برخوردار است.

برای حل این معضل چه باید کرد ???

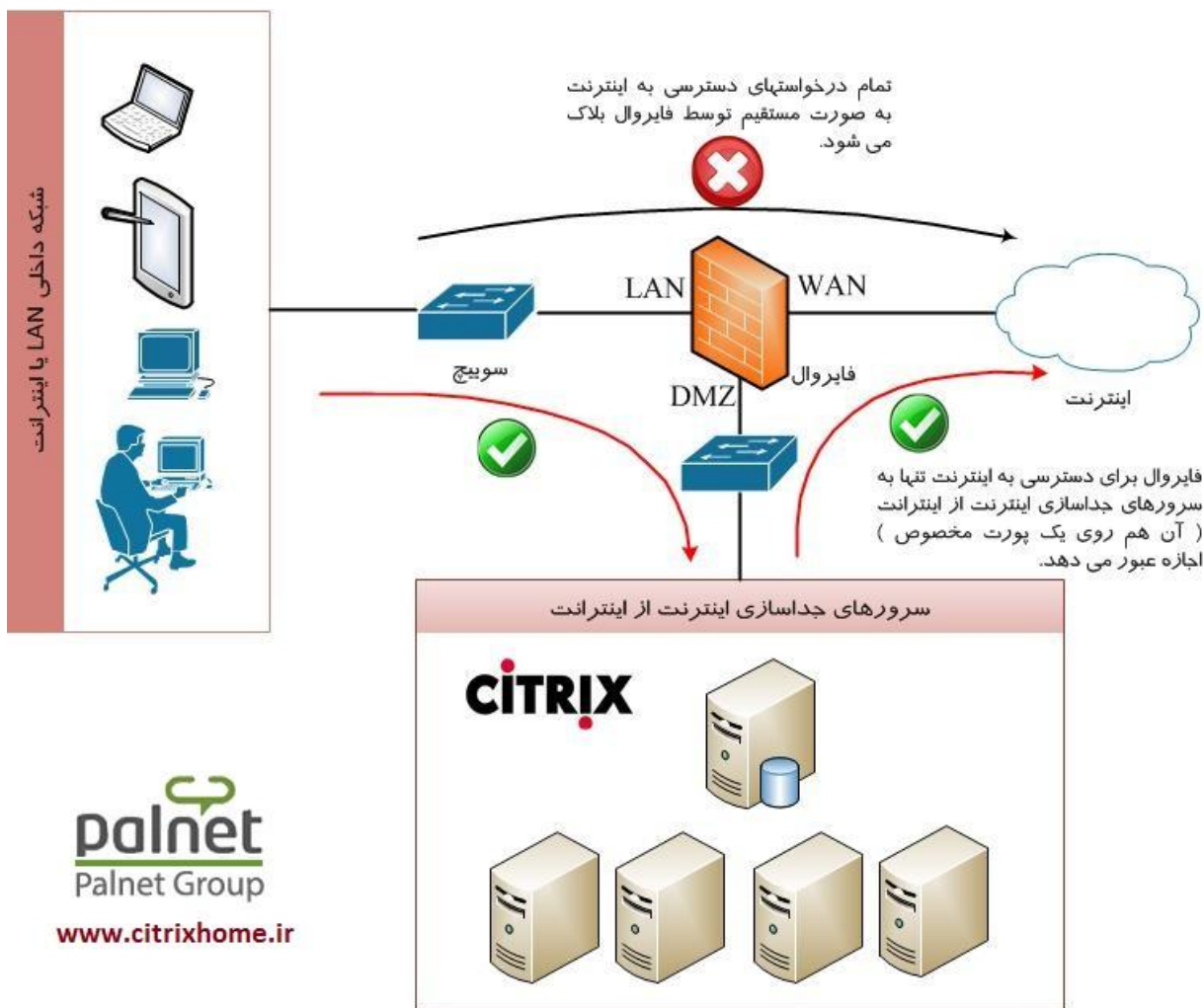
یکی از راه حل‌های انتخابی سازمانها، راه اندازی یک شبکه Passive مجزا می باشد که به هیچ وجه مقرون به صرفه نیست. در این حالت سازمانها اقدام به برپاسازی یک شبکه LAN مجزا می کنند که در این حالت سازمان می بایست هزینه‌ای برابر با آنچه پیش از این پرداخته است را پرداخت کند. و همچنین باید بودجه‌ای مضاعف برای تهیه سیستم‌های مورد نیاز جهت برقراری ارتباط با اینترنت در نظر بگیرد و در کنار تمام این هزینه‌ها باید مبلغ هنگفتی را برای نگهداری و پشتیبانی شبکه و سخت افزار جدید در نظر بگیرد.



راهکار خانه سیتریکس وابسته به گروه پال نت

شرکت سیتریکس راهکاری را ارائه می کند که بر اساس آن شبکه اینترنت از شبکه داخلی کاملاً جدا می شود اما در عین حال کاربران از پای سیستم خود می توانند همزمان از شبکه داخلی و اینترنت استفاده کنند!!! سیستم کاربر فقط به شبکه داخلی متصل است. سیستم کاربر به هیچ وجه به اینترنت متصل نبوده و هیچ ارتباط اینترنتی نیز وجود ندارد. تنها یک کامپیوتر در سازمان به اینترنت متصل است (که آن هم در یک VLAN و یا DMZ جداسازی و کاربران با آن هیچ ارتباطی نمی توانند برقرار کنند)

در این حالت با استفاده از تکنولوژی مجازی سازی سیتریکس بر روی کامپیوتری که اینترنت دارد یک Browser باز می شود و تصویر آن بصورت Image (تصویر) برای کاربر به نمایش در می آید و کاربران می توانند با استفاده از آن به اینترنت دسترسی پیدا کنند.



در این شکل تمامی کاربران شبکه داخلی (LAN یا اینترنت) به هیچ عنوان مستقیماً به اینترنت دسترسی نخواهند داشت. چرا که تمامی درخواستها به اینترنت به صورت مستقیم توسط فایروال بلاک می شود. برای استفاده از اینترنت کاربران شبکه داخلی از سرورهای موجود در DMZ بهره می برند. سرورهای جداسازی اینترنت از اینترنت (که در DMZ واقع شده اند) تنها روی پورت های خاصی به اینترنت دسترسی دارند و کاربران از طریق آنها به اینترنت متصل می شوند.

نکته مهمی که در این بین وجود دارد این است که کاربران تصویر مرورگر اینترنتی را از طریق سرورهای جداسازی خواهند دید و این بدان معنی است که گرچه کاربران به اطلاعات مورد نیازشان روی اینترنت دسترسی پیدا خواهند کرد اما رایانه های آنها از محیط نا امن اینترنت مصون مانده، هرگز ویروسی نخواهد شد، امکان خروج اطلاعات از رایانه ها از طریق اینترنت وجود نخواهد داشت، امکان پیوست کردن فایل های مهم سازمان از روی رایانه ها وجود نخواهد داشت، هم چنین امکان دانلود هم از کاربران گرفته خواهد شد. البته می توان امکانات فوق را در اختیار برخی کاربران با اهمیت مانند مدیران ارشد سازمان قرار داد تا به درایوهای خود دسترسی داشته باشند و بتوانند از روی آن فایل آپلود کرده یا دانلود نمایند.

در طراحی توپولوژی شبکه این امکان وجود دارد که از VLANNING برای جداسازی بیشتر شبکه داخلی از اینترنت و به تبع آن امنیت بالاتر استفاده کرد.

برخی از مزایای استفاده از این راهکار :

- راه اندازی فوق العاده ساده این راهکار
- مدیریت آسان این راهکار
- هزینه پایین این راهکار
- کاهش هزینه سخت افزاری کاربران بدون نیاز به ارتقاء
- real time و آنلاین بودن سیستم و مشاهده تمامی اطلاعات برای تمامی کاربران
- قابلیت اعمال سیاست های امنیتی به کاربران با کمترین هزینه و زمان
- قابلیت کنترل کاربران در حال استفاده از سرویس و تنظیم سطوح دسترسی
- اضافه کردن لایه های امنیتی و load balancing به سرویس های ارائه شده
- متمرکز کردن اطلاعات و بالا بردن ضریب امنیتی شبکه و داده های آن
- افزایش توانایی سرویس دهی در حجم بالا

مدت زمان استفاده این راهکار

مدت زمان استفاده این راهکار نامحدود می باشد و از لحاظ مدت زمان استفاده از این راهکار هیچ گونه محدودیتی وجود ندارد.

مشخصات سرور مورد نیاز:

براساس تعداد کاربر استفاده کننده از این راهکار، سرور برنامه باید مشخصات زیر را دارا باشد:

مقدار حافظه (RAM)	پردازنده (CPU)	نوع سرور	تعداد کاربر	بسته
5GB	Pentium4 Corei3 2.5GHz or higher	PC	۵۰	۱
8GB	Pentium4 Corei5 2.6GHz or higher	PC	۱۰۰	۲
10GB	Intel Xeon 5506 or higher	HP ML150G6	۲۰۰	۳
20GB	Intel Xeon 5550 or higher	HPDL370G6	۵۰۰	۴
30GB	Intel Xeon 5220 or higher	HP DL380G6	۱۰۰۰	۵
45GB	Intel Xeon 5760 or higher	HP DL380G7	۱۵۰۰	۶
60GB	Intel Xeon 5550 or higher	HP DL380G8	۲۰۰۰	۷

مدت زمان اجرای طرح جداسازی شبکه اینترنت از شبکه داخلی

با توجه به فراهم بودن سخت افزار مورد نیاز برای سرور برنامه، مدت زمان انجام پروژه طبق جدول ذیل به طول خواهد انجامید.

مدت زمان اجرای طرح	بسته پیشنهادی
حداکثر ظرف ۳ روز	۱ و ۲ و ۳
حداکثر ظرف ۴ روز	۴ و ۵
حداکثر ظرف ۶ روز	۶ و ۷