پیاده سازی DMZ[1] به صورت مجازی

همانطور که می دانید تکنولوژی مجازی سازی موجب تحولی شگرف در زیرساخت شبکه های کامپیوتری شده است و مزایای متنوع آن از لایه فیزیکی و دیتا گرفته تا لایه کاربردی قابل دسترسی می باشد.

متد امنیتی DMZ از نمونه مواردی است که قابلیت پیاده سازی به صورت مجازی دارد ولی ممکن است عده ای از کارشناسان بر این باور باشند که چنین کاری باعث کاهش امنیت خواهد شد. در صورتی که این گفته مبنا و پایه ی علمی ندارد و نه تنها از میزان امنیت سیستم نمی کاهد بلکه مزایای جدیدی به ارمغان می آورد. البته باید در نظر داشت پیاده سازی DMZ به صورت مجازی از یک جنبه دارای ریسک بالایی است و آن هم اشتباه کارشناس در پیاده سازی چنین ساختاری به دلیل پیچیدگی های فنی آن می باشد.

به طور کل متد امنیتی DMZ را به سه روش می توان پیاده سازی نمود :

۱- جداسازی نواحی فیزیکی[2]

سازمان هایی که می خواهند نواحی DMZ را به صورت فیزیکی از هم جدا داشته باشند، از این راه حل استفاده می کنند. در این روش هر ناحیه سرورهای کلاستر شده ی خود را دارد و بین نواحی از تجهیزات امنیتی و فایروال استفاده می شود. بنابراین متد DMZ در اینجا تقریبا شبیه همان حالت فیزیکی پیاده سازی می شود با این تفاوت که فایروال بین سرورها و کلاسترهای مجازی واقع می گردد تا نواحی امنیتی متفاوت را ایجاد نماید.

مزایا:

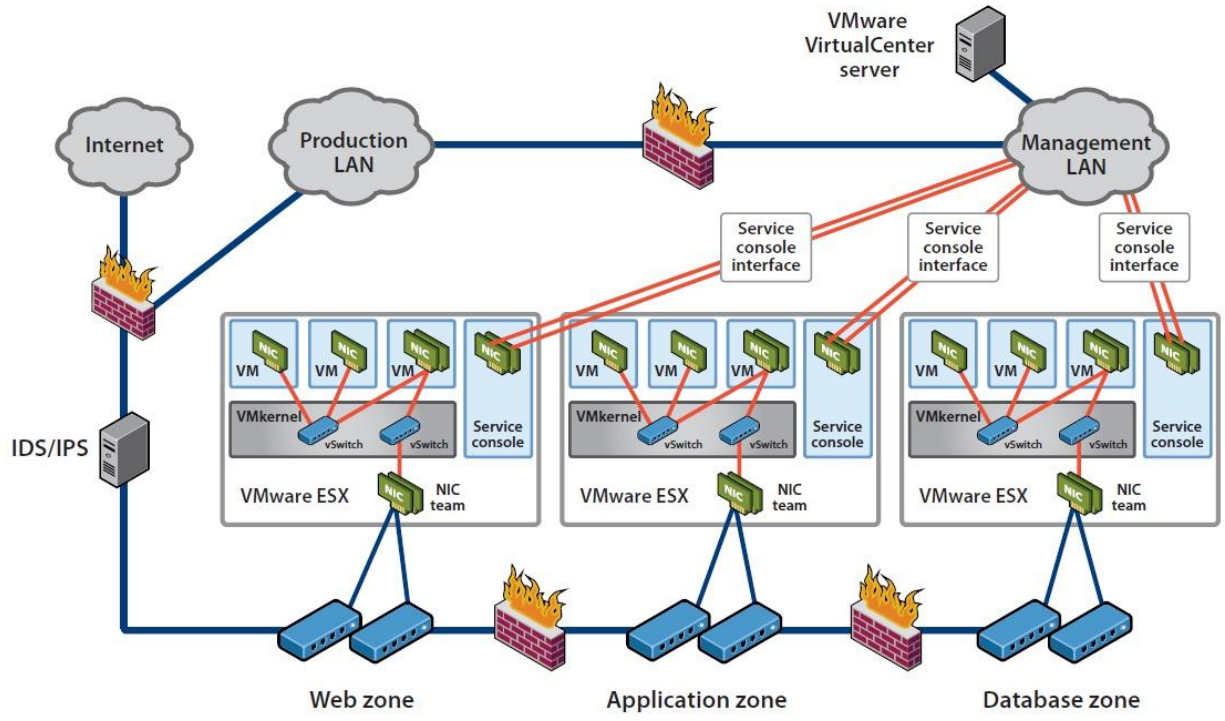
۱) آسان بودن تنظیمات
۲) حداقل تغییر در زیرساخت
۳) نیاز به دانش و تجربه فنی کمتر
۴) کاهش ریسک خطای پیاده سازی

[1] Demilitarized Zone
[2] Partially Collapsed DMZ with Separate Physical Trust Zones

معایب:

۱) افزایش هزینه های خرید لایسنس و تجهیزات

۲) بهره گیری از حداقل مزایای مجازی سازی



۲- جداسازی نواحی مجازی[۳]

در این حالت تمامی سیستم های میزبان[۴] و ماشین های مجازی[۵] بر روی یک تک کلاستر ESX قرار دارند و ترافیک اطلاعات بین سرورهای مجازی از طریق تجهیزات امنیتی چون فایروال ها منتقل می گردند. بدین صورت نواحی امنیتی مختلف بر روی یک

[3] Partially Collapsed DMZ with Virtual Separation of Trusted Zones
[4] Host
[5] Virtual Machine

کلاستر ایجاد شده و ماشین های مجازی در این نواحی و به صورت منطقی جای می گیرند. برای این کار هر سرور مجازی باید حداقل به یک پورت سوییچ فیزیکی مرتبط باشد ولی برای افزایش سطح دسترسی بهتر است به دو پورت از سوییچ فیزیکی متصل شود.

مزایا:

۱) استفاده بهینه از منابع سخت افزاری

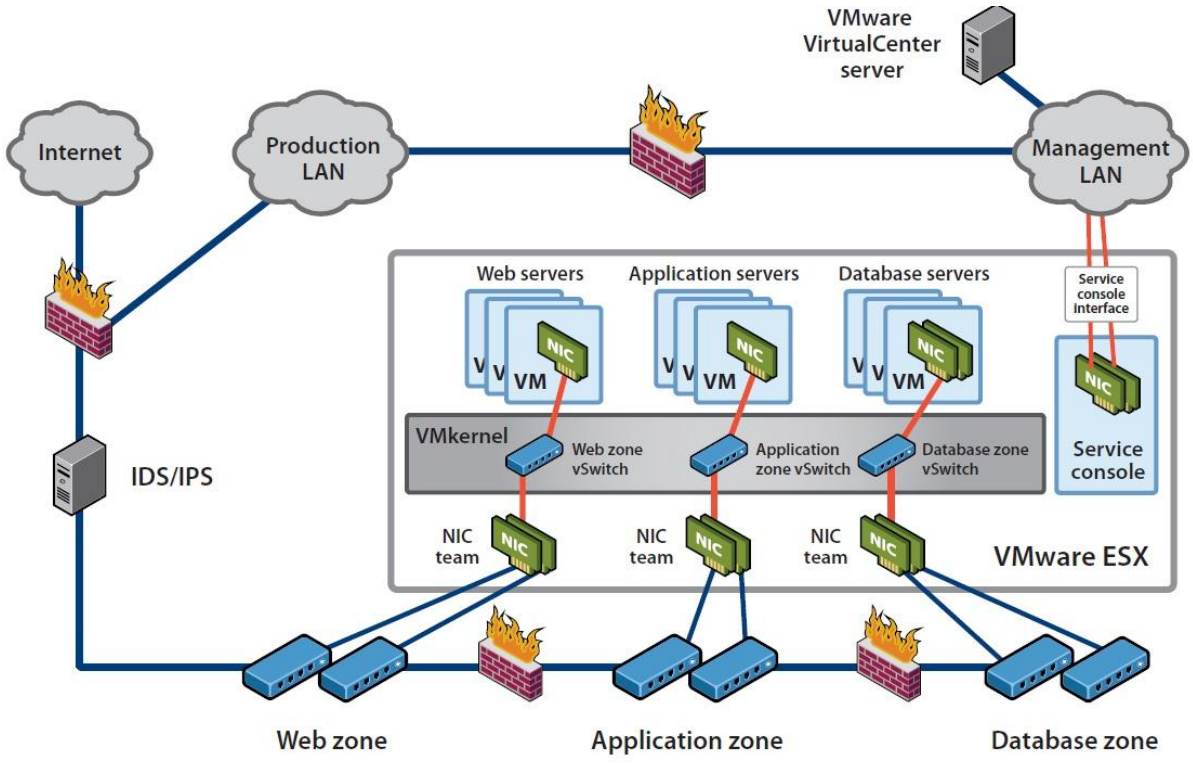
۲) استفاده از مزایای مجازی سازی

۳) کاهش هزینه خرید تجهیزات

معایب:

۱) پیچیدگی فنی بیشتر

۲) امکان بروز اشتباه در پیاده سازی



۳- پیاده سازی متد DMZ به صورت کاملا مجازی

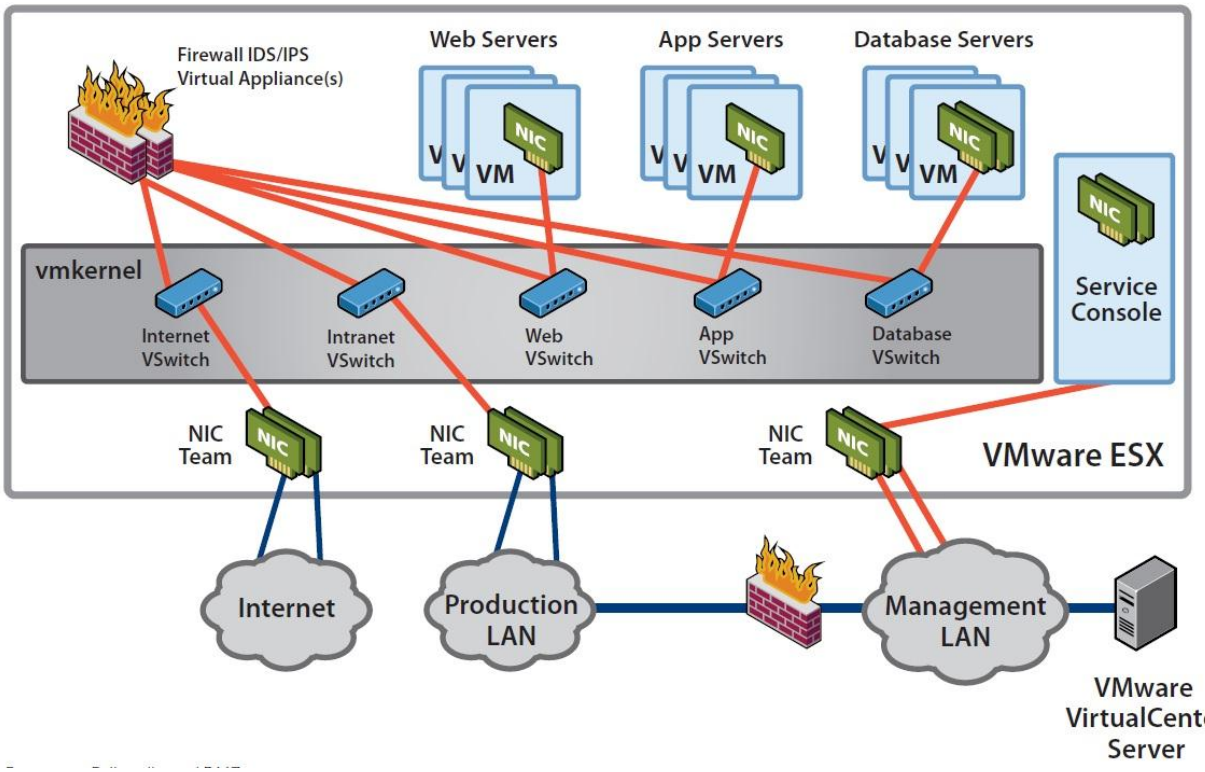
پیچیدگی های فنی این روش به مراتب بیشتر از روش های قبلی می باشد زیرا تمامی زیرساخت شبکه و تجهیزات امنیتی به صورت مجازی پیاده سازی و اجرا می شوند. چنین زیرساختی به شما امکان تعریف محدوده های امنیتی با سطوح دسترسی متفاوت برای یک کلاستر یا مجموعه کلاسترهای موجود را بدون استفاده از تجهیزات سخت افزاری می دهد. زیرا فایروال ها دیگر فیزیکی نبوده و خود ماشین های مجازی هستند که می توانند در کلاستر جای گیرند و ارتباطات هر نقطه از کلاستر را کنترل کنند. ولی باید تمهیداتی برای جلوگیری از خطاهای احتمالی مخصوصا زمان جابجایی ماشین ها توسط vMotion اتخاذ نمود. همچنین گزارش گیری از ماشین ها و مانیتورینگ ارتباطات موجود برای اطمینان از مسیر انتقال دیتا و موارد امنیتی لحاظ شده بسیار مهم می باشد. این نکته را به یاد داشته باشید که در این روش برای هر میزبان ESX نیاز به حداقل ۳ پورت شبکه برای اتصال به اینترنت، شبکه داخلی و کنسول مدیریت ESX یا vCenter دارد که به صورت استاندارد برای افزایش دسترسی از دو پورت برای هر لینک ارتباطی استفاده می شود بنابراین مجموع ۶ پورت برای هر میزبان مورد نیاز است.

مزایا:

۱) مدیریت تمامی زیرساخت شبکه از طریق یک سیستم
۲) کاهش زیاد در هزینه خرید تجهیزات
۳) بهره گیری از حداکثر مزایای مجازی سازی

معایب:

۱) پیچیدگی فنی بسیار زیاد
۲) نیاز به گزارش گیری و مانیتورینگ دقیق



تالیف و ترجمه : محمدرضا نیکوکلام

منبع: vmware.com