اولین نرم‌افزار مبتنی بر SDN برای مراکز داده

VMware NSX: مرزبندی جدید مجازی‌سازی

در سال‌های اخیر، ماشین‌های مجازی به کمک مراکز داده آمده‌اند. با استفاده از مجازی‌سازی، می‌توانید سیستم‌هایی با بارهای کاری متفاوت روی زیرساخت فیزیکی بسازید و به سرعت یک ماشین مجازی را از سروری به سرور دیگر منتقل کنید؛ بدون آنکه وقفه‌ای در سرویس‌دهی آن ایجاد شود. بهره‌وری را افزایش می‌دهید. وضعیت یک ماشین مجازی را ذخیره می‌کنید تا در صورت خرابی آن، به‌سرعت ماشین مجازی را بازیابی کنید. این‌ها تعداد محدودی از فواید مجازی‌سازی هستند.

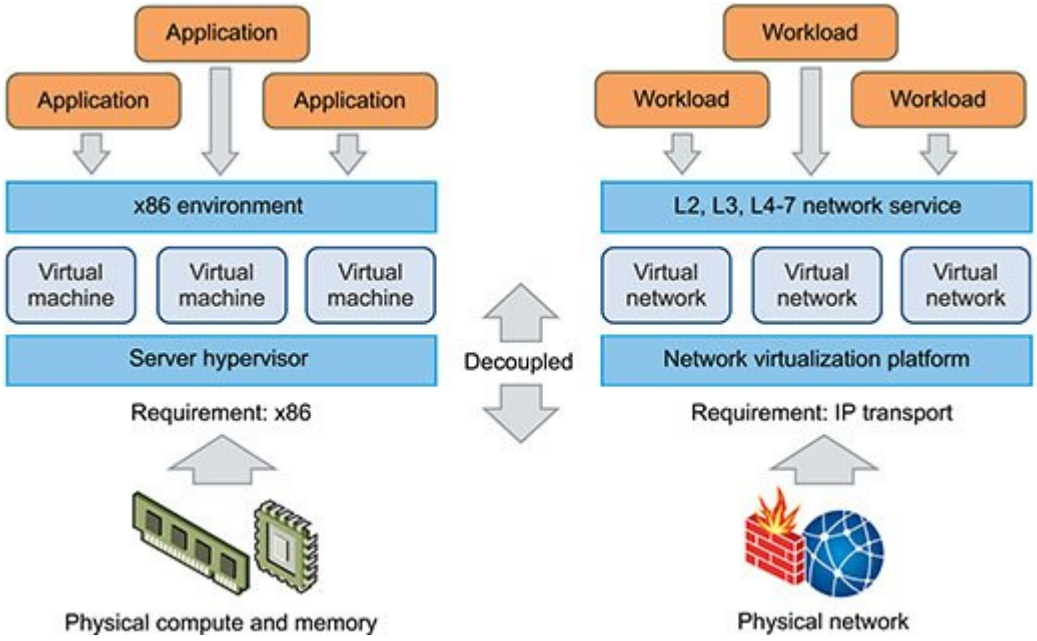
امروزه، استفاده از مجازی‌سازی در مرکز داده اجتناب‌ناپذیر است. به دلیل همین استقبال گسترده و سودمندی آن، مفهوم SDN یا شبکه‌های نرم‌افزارمحور ایجاد شد. شرکت «VMware» با محصول خود با نام «NSX» تمامی مرزهای مجازی‌سازی را از نو تعریف کرد و مفهوم SDN واقعی را در مقیاس بزرگ برای همگان آشنا ساخت.
شبکه‌های نرم‌افزارمحور (Software-Defined Networks) گونه جدیدی از سیستم مدیریت شبکه هستند که شبکه را به دو قسمت سطح مدیریتی و سطح ارسال داده تقسیم می‌کنند. در این نوع شبکه‌ها، سطح مدیریتی مسئولیت کنترل و برنامه‌ریزی برای پیاده‌سازی در سطح ارسال را بر عهده دارند. از سطح ارسال با نام Forwarding Plane نیز یاد می‌شود که مسئولیت هدایت ترافیک به سمت مقصد را عهده‌دار است. SDN باعث می‌شود نمایی متمرکز از شبکه به دست آورید. یکی از معروف‌ترین پروتکل‌هایی که در شبکه‌های نرم‌افزارمحور استفاده می‌شود، پروتکل OpenFlow است.
Network Functions Virtualization (NFV) نیز حوزه جدیدی در شبکه است که با کمک آن می‌توان المان‌های شبکه را به صورت مجازی و نرم‌افزاری پیاده‌سازی کرد. منظور از المان، دستگاه‌های سخت‌افزاری هستند که مجزا پیاده‌سازی می‌شدند؛ دستگاه‌هایی مانند دیواره آتش، مسیریاب، سوییچ، Load Balancer و مانند این‌ها. بدیهی است خرید و پیاده‌سازی هر کدام از این تجهیزات، هزینه‌بر، زمان‌بر و نیازمند به نیروی متخصص است. به همین دلیل NFV به کمک مدیران شبکه آمده است تا هزینه‌ها و پیچیدگی‌های خود را کاهش دهند. NFV مکمل شبکه‌های نرم‌افزارمحور است. شرکت VMware، با استفاده از این دو تکنولوژی محصولی با نام NSX را روانه بازار کرده است. این محصول مزایای هر دو تکنولوژی شبکه‌های نرم‌افزارمحور و NFV را با هم دارد. در سال 2012 شرکت VMware، شرکتی با نام «Nicira» را خریداری کرد که بر روی مجازی‌سازی شبکه و شبکه‌های نرم‌افزارمحور فعالیت می‌کرد و تولد این پروژه به آن زمان بازمی‌گردد.

مطلب پیشنهادی

اشتراک‌گذاری منابع دیجیتالی در خانه
راه‌اندازی مدیاسرورهای خانگی با DLNA

وظیفه اصلی NSX، ایجاد و مدیریت شبکه‌ای مجازی است. همان‌گونه که با استفاده از بستر مجازی‌سازی می‌توان ماشین مجازی را ایجاد، ذخیره، حذف و بازیابی کرد، با استفاده از NSX نیز می‌توان شبکه‌ای مجازی را ایجاد، ذخیره، حذف و بازیابی کرد. نتیجه این کار، مرکزداده‌ای با انعطاف‌پذیری بسیار زیاد در ارتباطات است که در کمترین زمان می‌تواند تنظیمات متفاوتی را پیاده کند؛ یک مسیر را حذف کند، مسیر جدید بسازد، لینک پشتیبان ایجاد کند و مانند این‌ها. با استفاده از NSX، سخت‌افزار فعلی تنها چیزی است که برای پیاده‌سازی یک مرکزداده مبتنی بر نرم‌افزار نیازمندید.

در حال حاضر دو نسخه متفاوت از NSX وجود دارد. اولین نسخه NSX for vSphere است که برای استفاده از محیط vSphere مناسب است. نسخه دوم، NSX for Multi-Hypervisor است که مناسب محیط‌های ابری همانند اپن‌استک (OpenStack) است. شکل یک، مقایسه دو رویکرد مجازی‌سازی شبکه و بستر مجازی‌سازی برای ساخت ماشین مجازی را نشان می‌دهد. همان‌طور که در سمت چپ این شکل نشان داده شده است، در مجازی‌سازی سخت‌افزاری، یک مجازی‌ساز روی سخت‌افزار نصب می‌شود. در لایه بالاتر، به صورت نرم‌افزاری و منطقی ماشین مجازی ساخته می‌شود که همان ویژگی‌های سخت‌افزار را از خود نشان می‌دهد و به‌راحتی می‌توان مشخصات سخت‌افزاری یک ماشین را تغییر داد. در سمت راست شکل 1، نحوه عملکرد NSX نشان داده شده است. NSX شامل یک پلتفرم مجازی‌ساز شبکه است که ویژگی‌های یک شبکه را شبیه‌سازی می‌کند. بر روی این پلتفرم، شبکه‌های مجازی قرار می‌گیرد و از طریق این شبکه‌های مجازی می‌توان سرویس‌های لایه دو تا لایه هفت ارائه داد. سرویس‌هایی مانند سویچینگ، مسیریابی، دیواره آتش، کیفیت خدمات (QoS) و توازن بار شبکه.

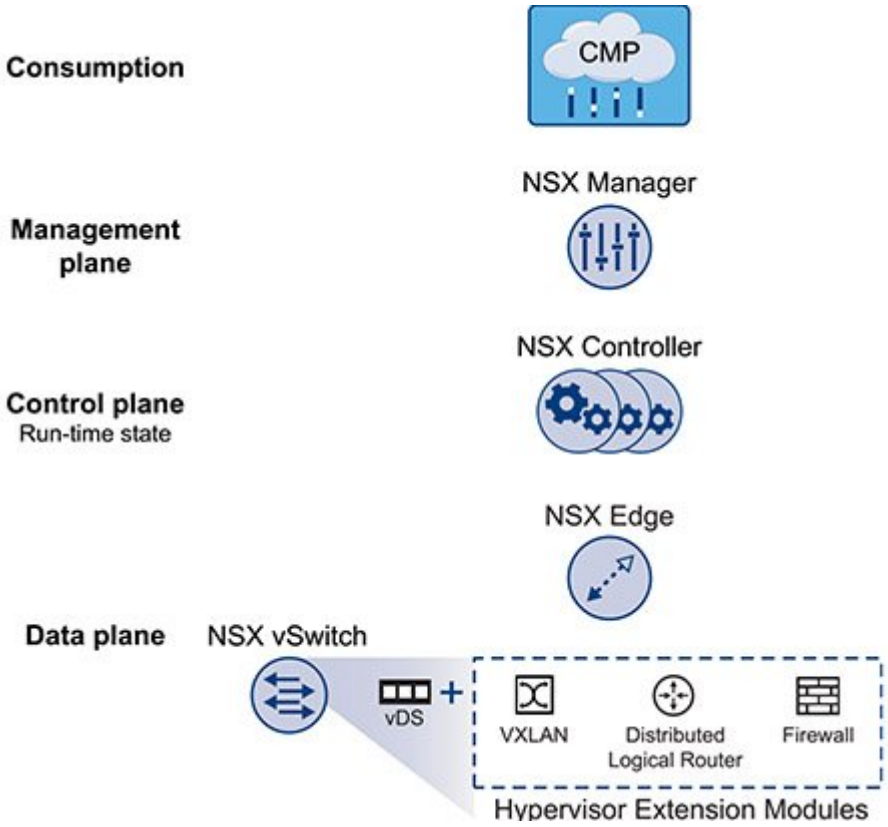


□□□ 1. □□□□□□□ □□ □□□□□□□ □□ □□□□□□□ □□ □□□□□□□□□□

اجزای NSX

NSX چهار جزء دارد. این اجزا در شکل 2 نشان داده شده‌اند که شامل این اجزا می‌شود:

1. Cloud Consumption
2. Management Plane
3. Control Plane
4. Data Plane



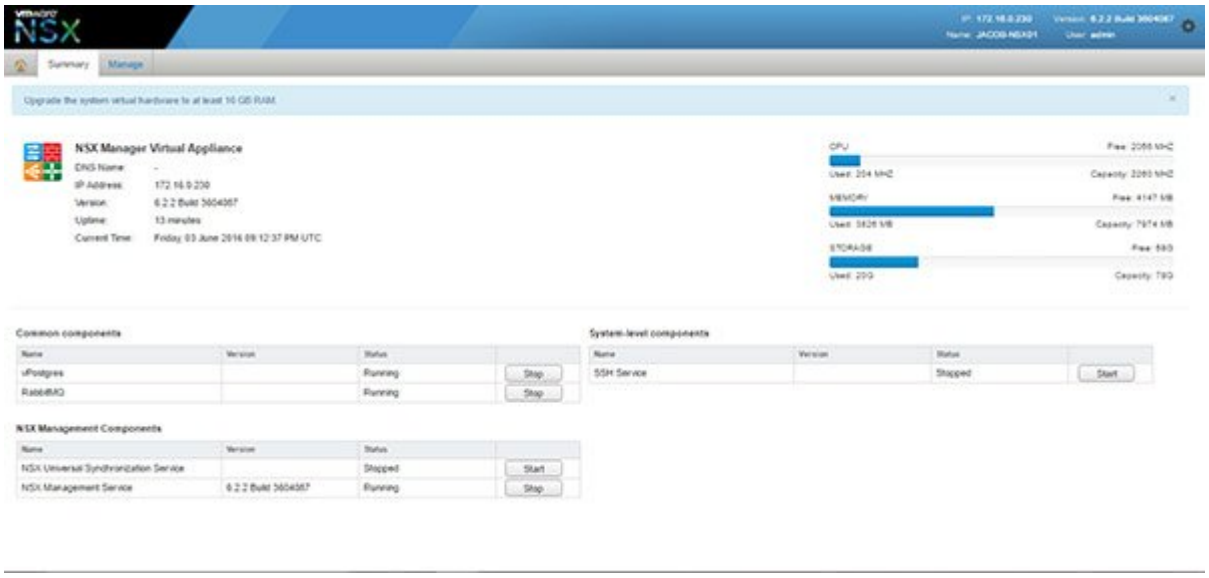
در ادامه به بررسی بیشتر این اجزا می‌پردازیم.

Cloud Consumption-1

Cloud Management Platform (CMP) که در شکل نشان داده شده است، طبق گفته VMware از اجزای اصلی نیست، اما به دلیل اینکه از طریق REST APIهای NSX می‌توان به صورت مجازی آن را با هر CMPای یکپارچه کرد، آن را یکی از اجزای NSX به حساب می‌آورند. طبق ادعای VMware از طریق API این لایه، به‌راحتی می‌توان ماژول‌های خاص NSX برای هر محیط ابری‌ای را ایجاد کرد. به گفته این شرکت، در حال حاضر NSX برای یکپارچه شدن با vCloud Director، VMware vCloud Automation Center و اپن‌استک آماده است. این شرکت، این ویژگی را out-of-box integration نامیده است. برای ارتباط با اپن‌استک از طریق پلاگینی که برای Neutron وجود دارد، می‌توان NSX را با اپن‌استک یکپارچه کرد.

Management Plane -2

این قسمت شامل NSX Manager می‌شود. قسمتی که به کمک آن می‌توانید شبکه را به صورت متمرکز مدیریت کنید. اکثر صاحب نظران این قسمت را همان سطح مدیریتی در SDN می‌دانند که به آن اشاره شد. با NSX Manager، می‌توان به «Single point of configuration» دست یافت. در شکل 3، کنسول NSX Manager نشان داده شده است که از طریق مرورگر قابل دسترسی است.



.3 □□□ □□□□□ NSX Manager

NSX Manager به صورت یک ماشین مجازی در vCenter اجرا می‌شود و برای نصب و راه‌اندازی نیز باید از طریق OVF installation اقدام و تنظیمات مربوط به آن انجام شود. به گفته VMware برای هر vCenter تنها یک NSX Manager می‌توان داشت. در صورتی که چندین vCenter مجزا داشته باشید و بین آن‌ها ارتباط برقرار کرده باشید، محیط Cross vCenter ایجاد کرده‌اید. معمولاً در چنین محیطی یک NSX Manager اصلی و چندین NSX Manager ثانویه وجود دارد. در چنین محیطی حداکثر یک NSX Manager اصلی و هفت عدد ثانویه می‌توان داشت. وظیفه NSX Manager اصلی، ایجاد قوانین برای سوییچ‌ها، مسیریاب‌ها و دیواره‌های آتشِ منطقی در سطح کل محیط Cross vCenter است. وظیفه ثانویه‌ها نیز مدیریت سرویس‌های شبکه در سطح محلی و مخصوص به هر vCenter است.

Control Plane -3

Control Plane نیز از NSX Controller Cluster تشکیل شده است. همان‌طور که از نام این کنترلر مشخص است، یک سیستم توزیع‌شده مدیریتی است که وظایف مدیریتی سوییچ‌ها و مسیریاب‌های منطقی را انجام می‌دهد. از این کنترلر هیچ‌گونه ترافیکی عبور نمی‌کند و خراب شدن آن، Data Plane و جریان ترافیک عبوری را تحت تأثیر قرار نمی‌دهد.

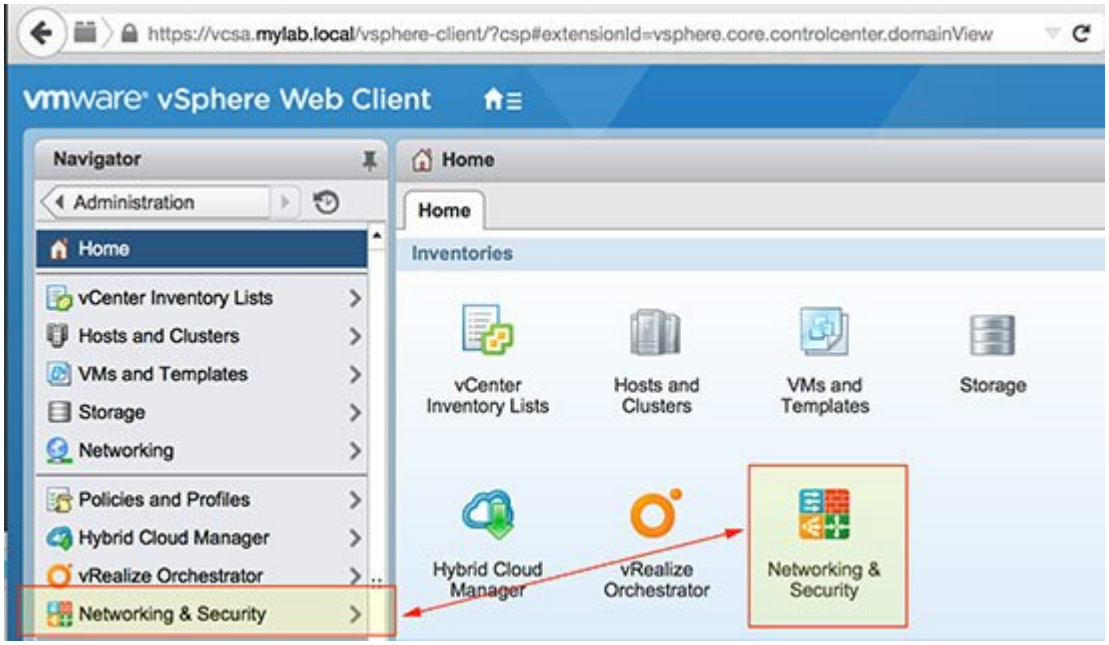
NSX Controller اطلاعات شبکه را به هاست‌ها ارسال می‌کند. اطلاعاتی که از NSX Controller به سایر قسمت‌ها ارسال می‌شود، اهمیت بسیار زیادی دارد؛ زیرا اگر اطلاعات اشتباه فرستاده شود، تنظیمات شبکه به هم خواهد ریخت و کل شبکه از کار خواهد افتاد. به همین دلیل باید احتمال خرابی را کاهش داد. VMware برای حل این مشکل، از ساده‌ترین روش برای افزایش افزونگی (Redundancy) استفاده کرده است. در این روش، به جای پیاده‌سازی یک NSX Controller، باید سه NSX Controller پیاده‌سازی شده و بین دستورات آن‌ها رأی‌گیری شود. اگر دستور یا فرمانی حداقل دو رأی را به خود اختصاص دهد، اجرا خواهد شد و این‌گونه، خرابی یک NSX Controller مشخص شده و از اجرای دستورات اشتباه جلوگیری می‌شود. در صورتی که از دو NSX Controller استفاده شود، اگر جواب‌های آن‌ها با هم متفاوت باشد، نمی‌توان جواب صحیح را تشخیص داد و مشکل «Split-Brain scenario» به وجود می‌آید. با پیاده‌سازی این کلاستر که شامل سه کنترلر است، به High Availability نیز دست خواهید یافت. برای اطلاع از تکنیک‌های افزایش افزونگی و آشنایی با روش‌های آن، به کتاب Design and Analysis of Fault-Tolerant Digital Systems نوشته Barry W.Johnson رجوع کنید.

در هر کلاستر، یک نود به عنوان NSX Controller اصلی وجود دارد. در صورتی که یک NSX Controller اصلی دچار خرابی شود، در کلاستر مربوطه نود دیگری برگزیده شده و به عنوان NSX Controller اصلی شناخته می‌شود. سایر نودهای موجود در کلاستر، باید با آن هماهنگ باشند و دائماً همگام‌سازی اتفاق افتد.

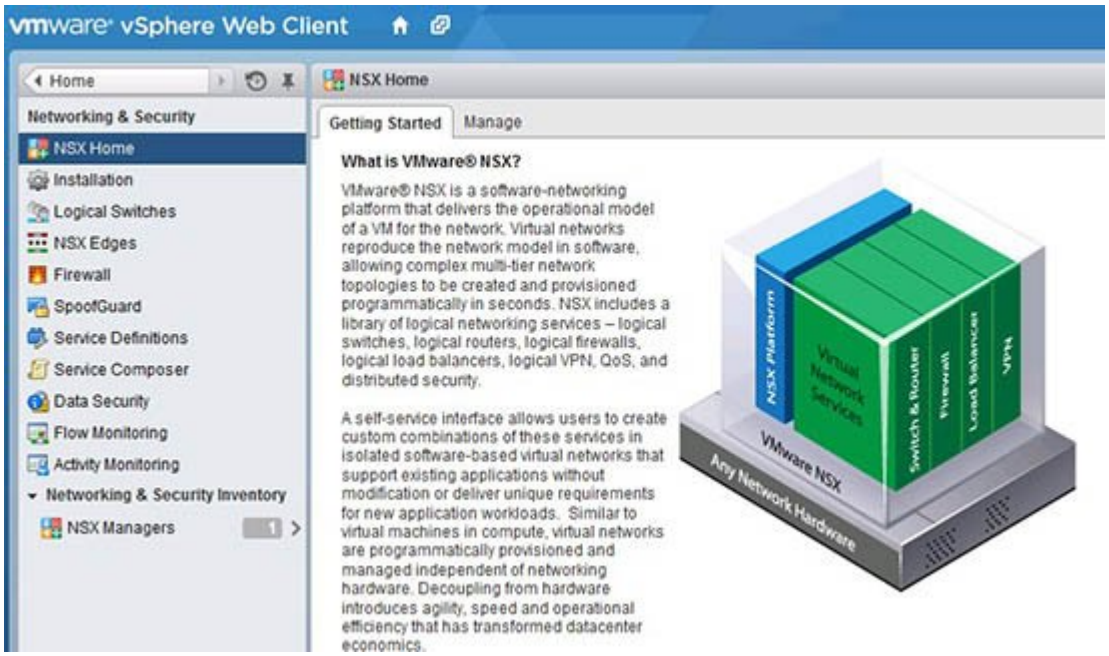
Data Plane -4

Data Plane شامل NSX vSwitch است که بر اساس vSphere Distributed Switch (VDS) کار می‌کند. کرنل ماژول‌های userspace agent، NSX، فایل‌های تنظیمات و اسکریپت‌های نصب در VIBها گنجانده شده‌اند و پس از نصب، با کرنل vSphere اجرا می‌شوند تا سرویس‌هایی همچون مسیریابی توزیع‌شده، دیواره آتش منطقی و VXLAN bridging فعال شوند. شکل 4 تصویری از vSphere web client پس از نصب NSX است. پس

از نصب، در قسمت Inventory آیکونی به نام Networking and Security اضافه می‌شود. پس از کلیک بر روی این آیکون، به صفحه اصلی NSX هدایت می‌شوید. این صفحه در شکل 5 نشان داده شده است.



□□□ 4. □□□□□
□□□ □□□□ □□□
vSphere □□
Inventory



□□□ 5. □□□□
NSX □□□□

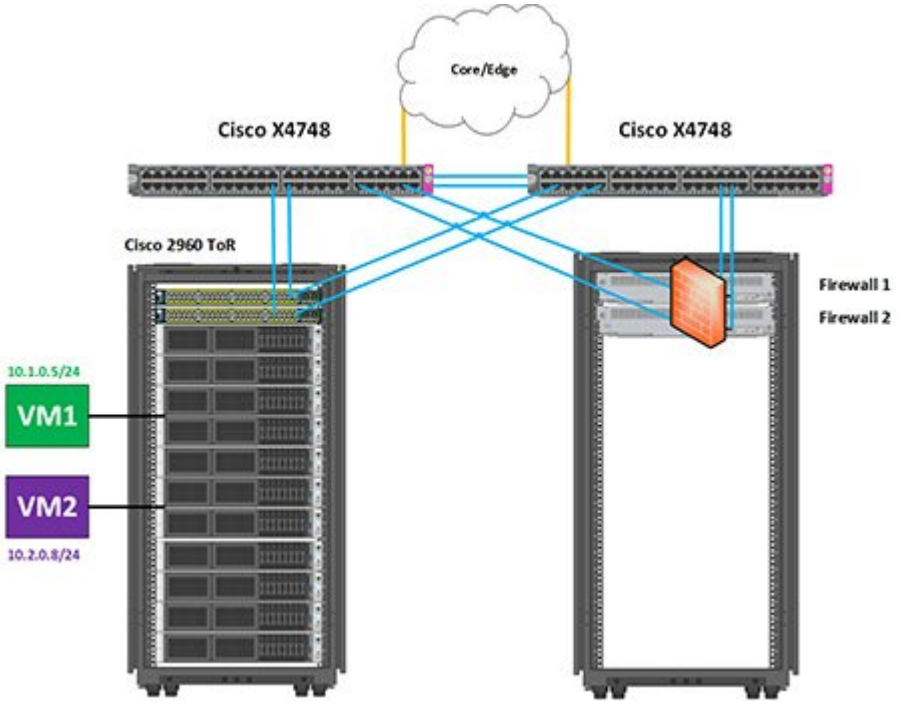
VIB، مخفف عبارت vSphere Installation Bundle، عملکردی تقریباً شبیه به فایل‌های ZIP دارد، با این تفاوت که این فرمت برای vSphere است. VXLAN نیز مخفف Virtual Extensible LAN است. VXLAN یک تکنولوژی مجازی‌سازی شبکه بوده و برای حل مشکلات مقیاس‌پذیر نبودن شبکه ایجاد شده است. VXLAN از تکنیک‌های کپسوله کردن (مانند VLAN) استفاده می‌کند تا فریم‌های اترنت لایه دو OSI را که بر اساس مک آدرس هستند، در بسته‌های لایه چهار UDP قرار دهد. برای اطلاعات دقیق‌تر در این خصوص می‌توانید به RFC7348 مراجعه کنید.
برخی از مزایای استفاده از NSX vSwitch به این شرح است:

- پشتیبانی از Overlay با استفاده از پروتکل‌هایی مانند VXLAN و انجام تنظیمات شبکه به صورت متمرکز
- تسهیل پیاده‌سازی تعداد زیادی ماشین مجازی
- قابلیت‌هایی همچون LACP، NetFlow/IPFIX، Port Mirroring، پشتیبان‌گیری و بازیابی تنظیمات کل شبکه، بررسی سلامت شبکه، کیفیت خدمات (QoS)، ابزارهای کارآمد و بسیار مفید برای مدیریت و نظارت ترافیک و در نهایت عیب‌یابی شبکه

صحبت درباره این نرم‌افزار، محدود به مباحث مذکور نمی‌شود و مسائل مربوط به آن، به اندازه‌ای بزرگ و پیچیده هستند که کتاب‌های متفاوت برای تشریح آن‌ها نوشته شده است. به همین دلیل قصد داریم با مثالی عملی و ساده، توضیحات ساده‌تری ارائه دهیم.

یک سناریو ساده

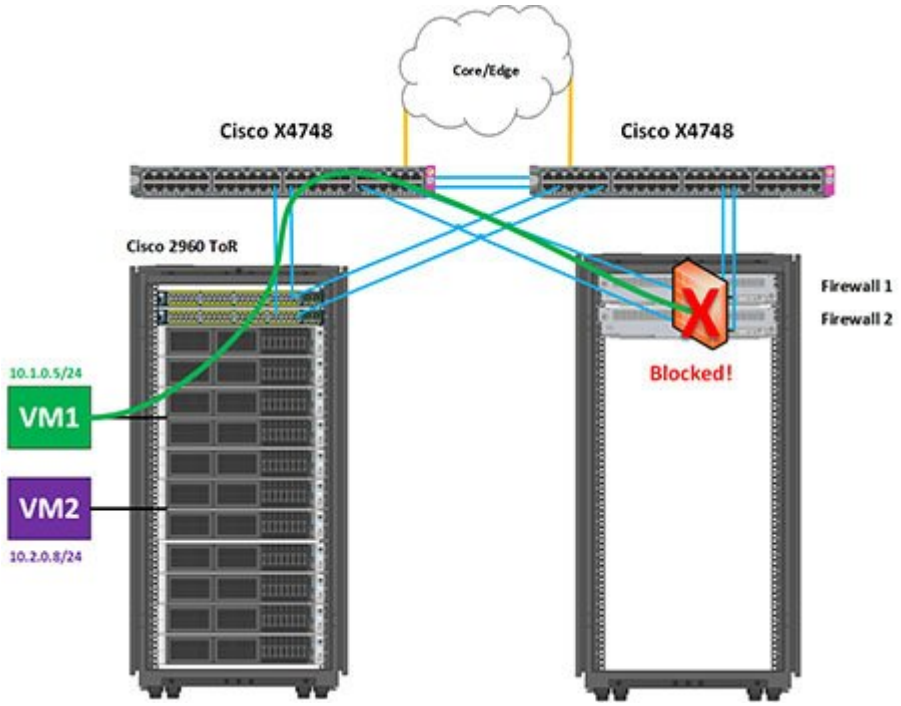
یکی از قابلیت‌های NSX، دیواره آتش است. تجهیزات موجود در این سناریو و ارتباطات شبکه آن در شکل 6 نشان داده شده است. دو عدد سوییچ Cisco 2960 ToR در رک، دو عدد سوییچ Cisco X4748 در لایه Aggregation، دو عدد دیواره آتش سخت‌افزاری، چند عدد سرور و دو ماشین مجازی موجود هستند. ToR مخفف عبارت Top of Rack و به معنای بالا رک است.



شکل 6. توپولوژی شبکه مورد استفاده در مثال NSX

مهندسان شبکه قصد دارند از طریق دیواره آتش، ترافیک لایه سه را محدود کنند. در این حالت این موارد رخ خواهند داد:

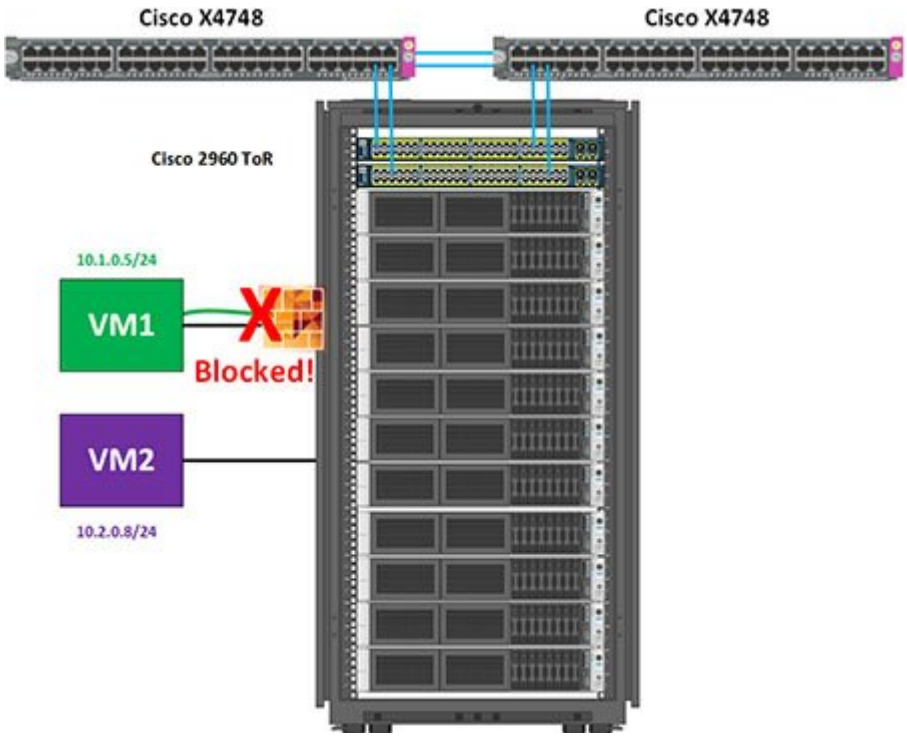
1. مهندسان شبکه باید خود را درگیر قوانین سخت برای مهندسی ترافیک کنند.
2. ممکن است دیواره آتش باعث ایجاد گلوگاه شود.
3. با بیشتر شدن وسعت شبکه، باید تعداد دستگاه‌های دیواره آتش بیشتری خرید و این موضوع باعث افزایش هزینه‌های سخت‌افزار (هزینه‌های Capex) می‌شود.
4. در صورت نفوذ به دیواره آتش، می‌توان به ترافیک کل شبکه دسترسی پیدا کرد.
5. این گونه ساختار پهنای باند زیادی مصرف می‌کند و کارایی شبکه را پایین خواهد آورد. برای مورد شماره پنج، شکل 7 را در نظر بگیرید. در این شکل ماشین مجازی شماره یک که با رنگ سبز مشخص شده است، آی‌پی آدرس 10.1.0.5/24 را دارد و قصد دارد با ماشین مجازی شماره دو که با رنگ بنفش مشخص شده و دارای آدرس آی‌پی 10.2.0.8/24 است، ارتباط برقرار کند برای برقراری ارتباط با ماشین مجازی شماره دو، ترافیک ماشین مجازی یک باید از سوییچ‌های ToR عبور کند و سوییچ Cisco X4748 را پشت سر بگذارد تا به دیواره آتش برسد. پس از آنکه به دیواره آتش رسید، ترافیک دریافتی بررسی شده و مشخص می‌شود که اجازه دسترسی را ندارد و ترافیک ارسالی مسدود می‌شود.



شکل 7. نحوه عملکرد فایروال‌های سنتی

برخی از تولیدکنندگان تجهیزات شبکه، محصولاتی تولید کرده‌اند که ترافیک یک ماشین مجازی به یک ماشین مجازی دیگر را مانیتور کنند و مسیری را که این ترافیک طی می‌کند تا بررسی شود، کوتاه‌تر کرده‌اند، اما هنوز مشکل هدررفت پهنای باند برای این موضوع باقی است.

NSX قابلیتی با نام Distributed Firewall (DFW) دارد که یک دیواره آتش توزیع‌شده است. این قابلیت، در هنگام نصب پلاگین NSX Manager vCenter فعال می‌شود. یکی از مزایای اصلی این قابلیت این است که دیواره آتش به سطح ماشین مجازی آورده شده است؛ به این معنی که هر بسته‌ای که از ماشین مجازی خارج شود یا بخواهد داخل شود، در بدو خروج یا ورود DFW آن را بررسی می‌کند. مطابق شکل 8، تفاوت این ساختار با ساختار سنتی این است که DFW می‌داند ماشین مجازی شماره یک مجاز نیست به ماشین مجازی شماره دو ترافیک ارسال کند. پس ترافیک آن را در لحظه خروج از ماشین مجازی بررسی می‌کند و اجازه وارد شدن به بستر شبکه را نمی‌دهد. با این رویکرد ترافیک غیرضروری از شبکه حذف شده و کارایی آن بیشتر می‌شود؛ با وجود اینکه برای خرید سخت‌افزار و نگهداری آن هزینه‌ای نشده است.



شکل 8. نحوه عملکرد فایروال‌های توزیع‌شده در NSX

در صورتی که ماشین مجازی خود را از سروری به سرور دیگر جابه‌جا کنید، ممکن است ساختار شبکه در سرور جدید متفاوت باشد و ترافیک شما از دیوار آتش سخت‌افزاری برای بررسی شدن عبور نکند یا نیاز به تغییرات جدید بر روی دیواره آتش سخت‌افزاری خود داشته باشید. حال با استفاده از NSX DFW، تمام قوانین و سیاست‌هایی که برای ترافیک یک ماشین مجازی تعریف کرده‌اید، با جابه‌جایی آن از قسمتی به قسمت دیگر، همراه ماشین مجازی منتقل می‌شود و از ساختار فیزیکی شبکه شما تبعیت نمی‌کند.

سخن آخر

شرکت VMware که محصولات بسیاری در خصوص مجازی‌سازی دارد، این بار نیز توانسته است با مجازی‌ساز جدیدی که شبکه را مجازی‌سازی می‌کند، به بهبود کارایی و علمکرد شبکه در مرکز داده کمک فراوانی کند. NSX، مثال بارزی از ترکیب شبکه‌های مبتنی بر نرم‌افزار و NFV است. با استفاده از NSX می‌توانید به SDDC) Software Defined Data Center) دست یابید و هزینه‌های ثابت و حتی متغیر خود را کاهش دهید. بحث و تبادل نظر در خصوص این نرم‌افزار بسیار جالب و مفید، به همین نقطه ختم نمی‌شود. تمام مواردی که ذکر شد، پیش درآمدی بر این نرم‌افزار و بررسی دقیق ساختار و قابلیت‌های آن خارج از بحث این مقاله است. در نگاه اول، این نرم‌افزار بسیار مفید است، اما هنوز پرسش‌هایی در ذهن ما وجود دارند که برای پاسخ به آن‌ها باید بیشتر بر روی نحوه کار این نرم‌افزار تحقیق شود. اول اینکه هرچقدر شبکه مجازی باشد، قطعاً نیاز به عبور ترافیک از زیرساخت فیزیکی را خواهد داشت. حال برای اینکه بار ترافیک بر روی یک لینک فیزیکی زیاد نباشد، چه تمهیداتی در نظر گرفته شده است؟ آیا این نرم‌افزار می‌تواند بار لینک فیزیکی را تشخیص دهد؟ چگونه نزدیک‌ترین مسیر منطقی برای رسیدن به یک آدرس را پیدا می‌کند و مشخصات فیزیکی را در نظر خواهد گرفت؟ ممکن است سؤالاتی از این قبیل، برای شما نیز اهمیت فراوانی داشته باشد. به همین سبب پیشنهاد می‌کنیم برای پیاده‌سازی NSX اطلاعات بیشتری کسب کنید و شرایط فیزیکی شبکه خود را در نظر داشته باشید.

==========

شاید به این مقالات هم علاقمند باشید:

چگونه یک دوربین مراقبت از کودک مناسب انتخاب کنیم؟

امسال به کام مراکزداده داخلی می‌شود!

پروژه تحقیقاتی بومی‌سازی فناوری SDN در ایران کلید خورد

چگونه رمزعبور وای‌فای را در ویندوز پیدا کنیم؟

علاقه‌مندان 5G حتما این ۱۳ مطلب را بخوانند!

ظرفیت مراکزداده Equinix دو برابر می‌شود!

فناوری‌های جدید مرکز داده ماژولار سیار و میکرو داده (بخش اول)

فناوری‌های جدید مرکز داده ماژولار سیار و میکرو داده (بخش پایانی)

تاریخ انتشار:
04 مهر 1395

نشانی منبع: https://www.shabakeh-mag.com/networking-technology/4664