بسمه تعالی

امن‌سازی شبکه در بستر مجازی‌سازی

VMware vSphere

(بخش اول)

فهرست مطالب

۱ مقدمه

امن‌سازی شبکه vSphere یکی از بخش‌های ضروری در حفاظت از محیط مجازی شما است. امنیت شبکه در محیط vSphere ویژگی‌ها و موارد مشترک زیادی با امن‌سازی محیط در یک شبکه فیزیکی دارد، اما همچنین شامل ویژگی‌هایی است که تنها به ماشین‌های مجازی اعمال می‌شوند. در این گزارش به بیان برخی از مهم ترین توصیه‌ها و موارد مربوط به امن‌سازی شبکه در بستر مجازی‌سازی vSphere می‌پردازیم و بهترین تجربه های امنیتی را در این زمینه شرح می‌دهیم.

۲ امن‌سازی سوئیچ‌های مجازی استاندارد

ترافیک سوئیچ مجازی استاندارد[۱] را می‌توان در مقابل حملات لایه ۲ امن کرد. برای این کار می‌توان با استفاده از تنظیمات امنیتی سوئیچ‌ها، برخی از حالت‌های آدرس MAC را محدود کرد. هر آداپتور شبکه ماشین مجازی یک آدرس MAC اولیه[۲] و یک آدرس MAC مؤثر[۳] دارد.

- **آدرس MAC اولیه**: آدرس MAC اولیه زمانی که آداپتور ایجاد می‌شود به آن تخصیص داده می‌شود. اگر چه آدرس MAC اولیه را می‌توان از خارج سیستم‌عامل مهمان دوباره پیکربندی کرد، اما نمی‌تواند توسط سیستم‌عامل مهمان تغییر کند.
- **آدرس MAC مؤثر**: هر آداپتور یک آدرس MAC مؤثر دارد که ترافیک ورودی شبکه که مقصد آن یک آدرس MAC متفاوت با آدرس MAC مؤثر است، را فیلتر می‌کند. سیستم‌عامل مهمان مسئول تنظیم آدرس MAC مؤثر است و معمولاً آدرس MAC مؤثر را به آدرس MAC اولیه منطبق می‌کند.

در ابتدای ایجاد یک آداپتور شبکه ماشین مجازی، آدرس MAC مؤثر و آدرس MAC اولیه یکسان هستند. سیستم‌عامل مهمان می‌تواند در هر زمان دلخواه آدرس MAC مؤثر را به مقدار دلخواه تغییر دهد. اگر یک

---

[۱] Virtual standard switch

[۲] Initial MAC address

[۳] Effective MAC address

سیستم‌عامل آدرس MAC مؤثر را تغییر دهد، آداپتور شبکه آن سیستم ترافیکی که به مقصد آدرس MAC جدید است را دریافت می‌کند.

زمانی‌که بسته‌ها از طریق یک آداپتور شبکه ارسال می‌شوند، معمولاً سیستم‌عامل مهمان آدرس MAC مؤثر آداپتور خود را در فیلد آدرس MAC مبدأ فریم‌های اترنت قرار می‌دهد. همچنین آدرس MAC آداپتور شبکه گیرنده را در فیلد آدرس MAC مقصد قرار می‌دهد. آداپتور گیرنده بسته‌ها را تنها در صورتی پذیرش می‌کند که آدرس MAC مقصد بسته با آدرس MAC مؤثر آداپتور منطبق باشد.

یک سیستم‌عامل می‌تواند فریم‌ها را با یک آدرس MAC منبع جعلی ارسال کند. این بدان معنی است که یک سیستم‌عامل می‌تواند با جعل یک آداپتور شبکه که برای شبکه دریافت‌کننده مجاز است، حملات مخربی را روی دستگاه‌های شبکه انجام دهد.

با پیکربندی یک سیاست امنیتی روی پورت‌گروه‌ها[٤] یا پورت‌ها، ترافیک مجازی را در مقابل حملات جعل و رهگیری لایه ۲ امن نمایید. سیاست امنیتی روی پورت‌گروه‌های توزیع شده و پورت‌ها شامل گزینه‌های زیر است:

- حالت بی‌قاعده[٥]
- تغییرات آدرس MAC[٦]
- انتقال‌های جعلی[٧]

تنظیمات پیش‌فرض را می‌توان با انتخاب سوئیچ مجازی مربوط به میزبان در vSphere Web Client انجام داد.

روش

۱. در vSphere Web Client میزبان مورد نظر را انتخاب کنید.

---

[٤] Port groups

[٥] Promiscuous mode

[٦] MAC address changes

[٧] Forged transmits

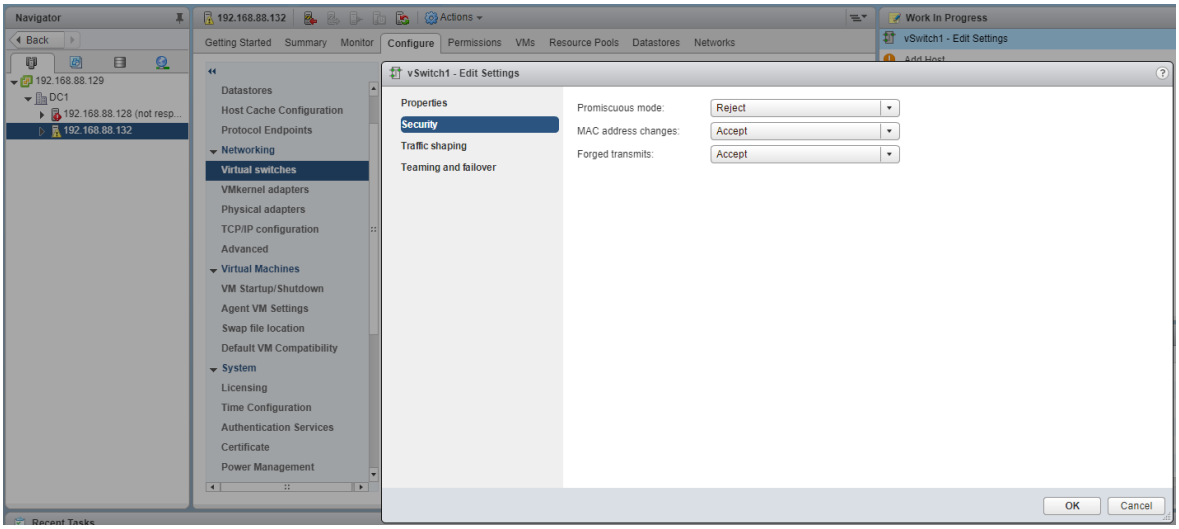
۲. برگه Configure را انتخاب کرده و سپس وارد قسمت Networking شوید.

۳. گزینه Virtual switches را انتخاب کرده تا لیست سوئیچ‌های مجازی موجود نمایش داده شود.

٤. سوئیچ مورد نظر را انتخاب و سپس دکمه Edit settings را کلیک کنید.

۵. در پنجره باز شده وارد بخش Security شوید.

٦. تنظیمات مربوط به حالت بی‌قاعده، تغییر آدرس MAC، و انتقال‌های جعلی در این پنجره قرار دارند که می‌توانید آن‌ها را به Accept یا Reject تنظیم کنید.



شکل ۱ تنظیمات امنیتی مربوط به آدرس MAC

۲-۱ عملکرد حالت بی‌قاعده

حالت بی‌قاعده هرگونه فیلترینگ پذیریشی که آداپتور ماشین مجازی انجام می‌دهد را از بین می‌برد، به‌گونه‌ای که سیستم‌عامل مهمان همه ترافیک‌های مشاهده شده روی سیم را دریافت می‌کند. به طور پیش‌فرض، آداپتور ماشین مجازی نمی‌تواند در حالت بی‌قاعده عمل کند.

اگرچه حالت بی‌قاعده می‌تواند برای ردیابی فعالیت شبکه مفید باشد، اما یک حالت ناامن است، زیرا هر آداپتور در حالت بی‌قاعده به تمام بسته‌ها دسترسی دارد، حتی اگر برخی از بسته‌ها تنها توسط یک آداپتور خاص دریافت شده باشند. این بدین معنی است که یک مدیر یا کاربر ریشه در یک ماشین مجازی، به صورت بالقوه می‌تواند ترافیکی را که به مقصد سایر سیستم‌عامل‌های مهمان یا میزبان است، را ببیند.

نکته: در بعضی موارد ممکن است یک دلیل قانونی وجود داشته باشد که یک سوئیچ مجازی استاندارد یا توزیع شده در حالت بی‌قاعده عمل کند. به عنوان مثال، اگر شما در حال اجرای نرم‌افزار تشخیص نفوذ شبکه یا شنود بسته هستید.

۲-۲ تغییرات آدرس MAC

سیاست امنیتی یک سوئیچ مجازی شامل گزینه MAC address changes است. این گزینه ترافیکی را تحت تأثیر قرار می‌دهد که یک ماشین مجازی دریافت می‌کند.

وقتی که گزینه MAC address changes به Accept تنظیم شده باشد، ESXi درخواست‌های مبنی بر تغییر آدرس MAC مؤثر به آدرسی متفاوت با آدرس MAC اولیه را می‌پذیرد.

وقتی که گزینه MAC address changes به Reject تنظیم شده باشد، ESXi به درخواست‌های مبنی بر تغییر آدرس MAC مؤثر به آدرسی متفاوت با آدرس MAC اولیه توجهی نمی‌کند. این تنظیمات از میزبان در مقابل جعل MAC محافظت می‌کند. پورتی که آداپتور ماشین مجازی از آن برای ارسال درخواست استفاده می‌کند غیرفعال شده و آداپتور ماشین مجازی هیچ فریم دیگری را دریافت نمی‌کند تا زمانی که آدرس MAC مؤثر با آدرس MAC اولیه مطابقت داشته باشد. سیستم‌عامل مهمان تشخیص نمی‌دهد که به درخواستش مبنی بر تغییر آدرس MAC، اهمیتی داده نشده است.

نکته: آغازکننده‌ی iSCSI متکی بر این است که بتواند درخواست تغییر آدرس MAC را از انواع خاصی از ذخیره‌سازی‌ها دریافت کند. در صورتی که از ESXi iSCSI با ذخیره‌سازی iSCSI استفاده می‌کنید، گزینه MAC address changes را به Accept تنظیم کنید.

۲-۳ انتقال‌های جعلی

گزینه Forged transmits ترافیکی را تحت تأثیر قرار می‌دهد که از یک ماشین مجازی انتقال داده شده است. زمانی‌که این گزینه به Accept تنظیم شده باشد، ESXi آدرس MAC منبع را با آدرس MAC مؤثر مقایسه نمی‌کند. برای محافظت در مقابل جعل MAC، می‌توانید گزینه Forged transmits را به Reject تنظیم کنید. اگر این کار را انجام دهید میزبان، آدرس MAC منبع که توسط سیستم‌عامل مهمان انتقال داده شده است را با

آدرس MAC مؤثر ماشین مجازی خود مقایسه می‌کند. در صورتی که این دو آدرس بر هم منطبق نباشند، میزبان ESXi بسته را نادیده می‌گیرد.

سیستم‌عامل مهمان تشخیص نمی‌دهد که آداپتور ماشین مجازی‌اش نمی‌تواند بسته‌ها را با استفاده از آدرس MAC جعلی ارسال کند. میزبان ESXi هر بسته‌ای با آدرس‌های جعلی را، قبل از تحویل، می‌پذیرد، و سیستم عامل مهمان ممکن است فرض را بر این بگذارد که بسته‌ها نادیده گرفته شده‌اند.

۳ جداسازی ترافیک شبکه با استفاده از VLANها

شبکه‌های محلی مجازی[۸] (VLANها) به ما اجازه می‌دهند که یک شبکه را به چندین دامنه همه‌پخشی منطقی در لایه ۲ از پشته پروتکلی شبکه، قطعه‌بندی کنیم.

۳-۱ مزایای استفاده از VLAN در vSphere

پیکربندی VLAN در محیط vSphere مزایای خاصی را فراهم می‌کند.

- میزبان‌های ESXi را به یک توپولوژی VLAN که از قبل وجود دارد یکپارچه می‌کند.
- جداسازی و امن‌سازی ترافیک شبکه را انجام می‌دهد.
- ازدحام ترافیک شبکه را کاهش می‌دهد.

۳-۲ حالت‌های برچسب‌گذاری VLAN

vSphere از سه حالت برچسب‌گذاری[۹] VLAN در ESXi پشتیبانی می‌کند: برچسب‌گذاری سوئیچ خارجی[۱۰] (EST)، برچسب‌گذاری سوئیچ مجازی[۱۱] (VST)، و برچسب‌گذاری مهمان مجازی[۱۲] (VGT). توضیحات مربوط به این سه حالت در جدول ۱ آمده است.

---

[۸] Virtual Local Area Networks

[۹] Tagging

[۱۰] External Switch Tagging

[۱۱] Virtual Switch Tagging

[۱۲] Virtual Guest Tagging

جدول ۱ حالت‌های مختلف برچسب‌گذاری VLAN

حالت برچسب گذاری	شناسه VLAN روی پورت گروه‌های سوئیچ	توصیف
EST	صفر	سوئیچ فیزیکی برچسب‌گذاری VLAN را انجام می دهد. آداپتورهای شبکه میزبان به پورت‌های دسترسی سوئیچ فیزیکی متصل می‌شوند.
VST	بین ۱ تا ٤٠٩٤	سوئیچ مجازی قبل از این‌که بسته‌ها میزبان را ترک کنند، برچسب‌گذاری VLAN را انجام می‌دهد. آداپتورهای شبکه میزبان باید به پورت‌های trunk سوئیچ فیزیکی متصل شوند.
VGT	• ٤٠٩٥ برای سوئیچ استاندارد • محدوده و VLANهای منحصربه‌فرد برای سوئیچ توزیع‌شده	ماشین مجازی برچسب‌گذاری VLAN را انجام می دهد. سوئیچ مجازی هنگامی که بسته‌ها را بین پشته شبکه ماشین مجازی و سوئیچ خارجی انتقال می‌دهد، برچسب‌های VLAN را حفظ می‌کند. آداپتورهای شبکه میزبان باید به پورت‌های trunk سوئیچ فیزیکی متصل شوند. سوئیچ توزیع‌شده vSphere از یک نسخه اصلاح شده از VGT استفاده می‌کند. به دلایل امنیتی، شما می‌توانید یک سوئیچ توزیع‌شده را به گونه‌ای پیکربندی کنید تا تنها بسته‌هایی را که به VLANهای خاصی تعلق دارند را منتقل کند.

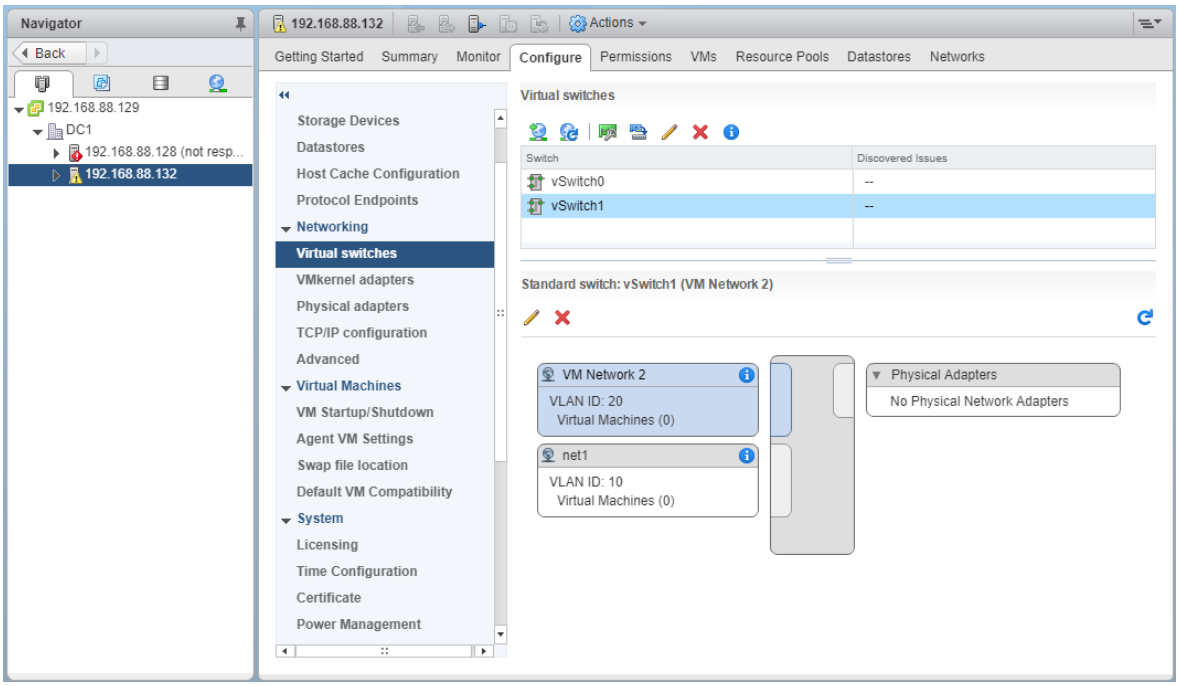
یادآوری: به منظور استفاده از VGT باید یک راه‌انداز 802.1Q VLAN truncking روی سیستم‌عامل مهمان ماشین مجازی نصب شده باشد.

به منظور ایجاد یک پورت‌گروه با یک VLAN ID مورد نظر بر روی یک سوئیچ مجازی استاندارد به صورت زیر عمل کنید.

روش:

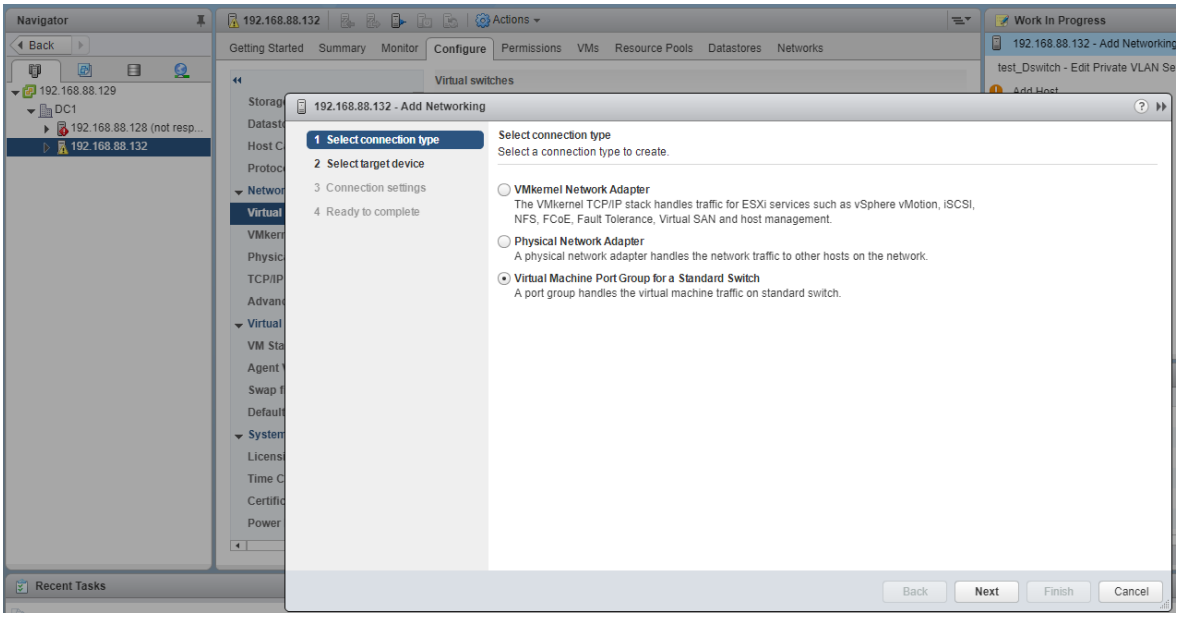
۱. در vSphere WebClient، میزبان مورد نظر را انتخاب کنید.

۲. به برگه Configure رفته، و در بخش Networking گزینه Virtual switches را انتخاب کنید. پنجره‌ای مشابه با پنجره زیر نمایش داده می‌شود که در آن لیست سوئیچ‌های مجازی استاندارد موجود بر روی این میزبان وجود دارد.



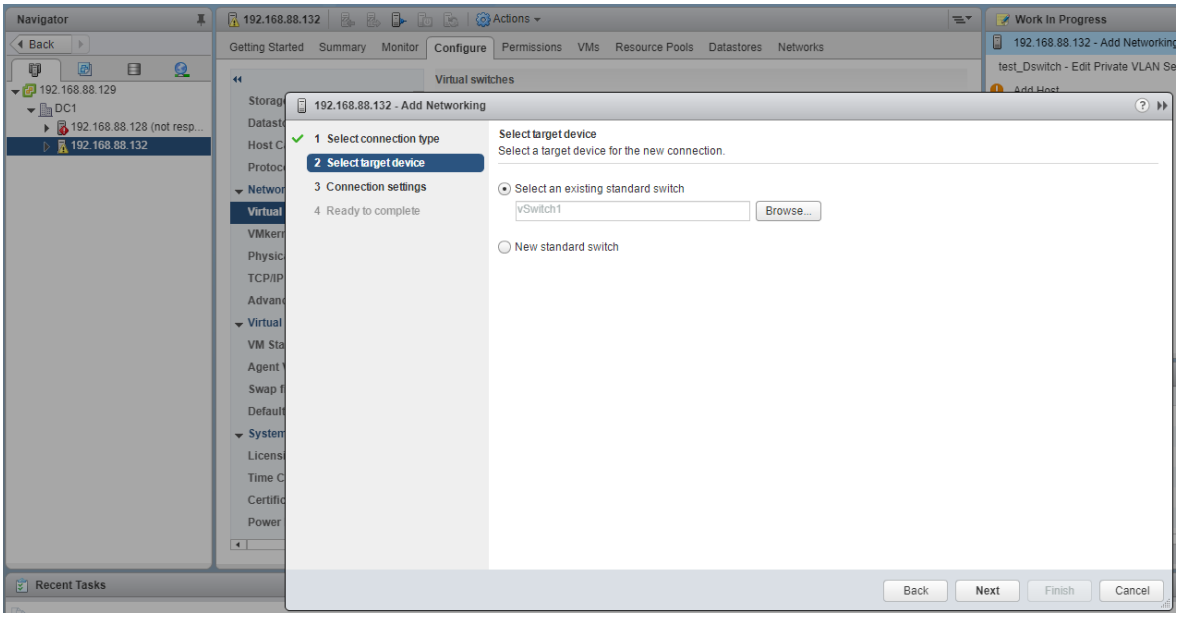
شکل ۲ ایجاد یک پورت‌گروه (۱)

۳. آیکون Add host networking را کلیک کرده و در صفحه نمایش داده شده Virtual Machine Port Group for a Standard Switch را انتخاب کنید.



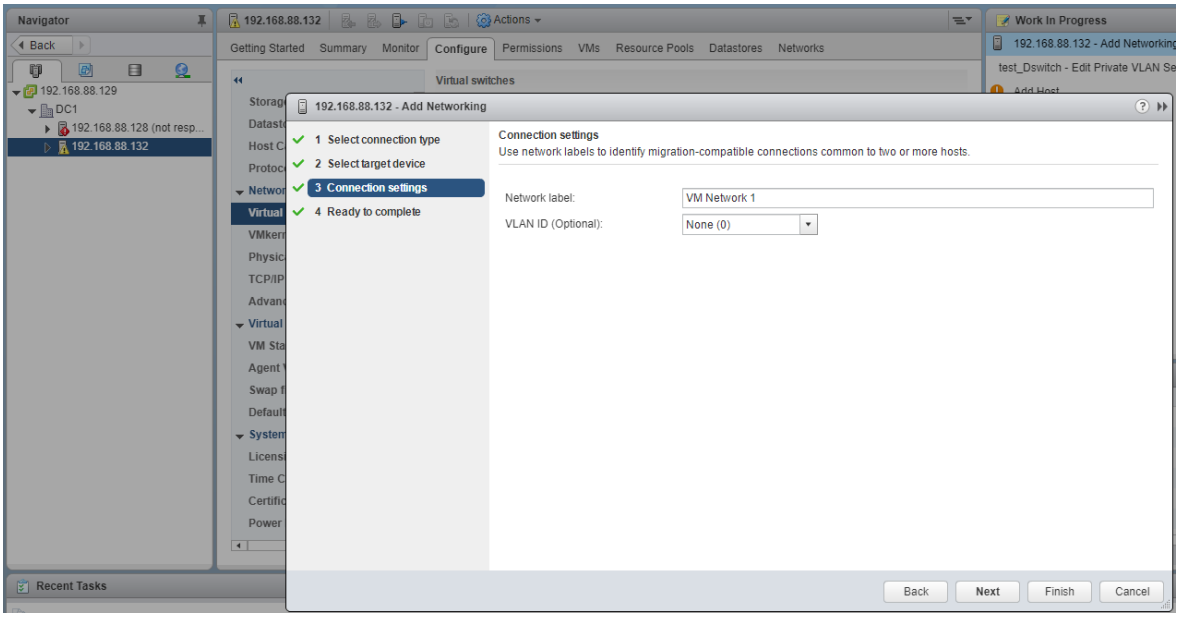
شکل ۳ ایجاد یک پورت‌گروه (۲)

۴. در قسمت Select an existing standard switch سوئیچ مجازی مورد نظر را انتخاب کنید.



شکل ٤ ایجاد یک پورت‌گروه (۳)

۵. در صفحه نمایش داده شده، Network label و VLAN ID مورد نظر را وارد کنید.



شکل ۵ ایجاد یک پورت‌گروه (٤)

۶. در نهایت با کلیک بر روی دکمه Finish پورت‌گروه مورد نظر با VLAN ID مشخص شده ساخته می شود.

۳-۳ VLANهای خصوصی

VLANهای خصوصی[۱۳] برای حل محدودیت‌های مربوط به شناسه VLAN مورد استفاده قرار می‌گیرند، و این کار را با اضافه کردن قطعه‌های بیشتر به یک دامنه همه‌پخشی منطقی و تبدیل آن به چندین زیردامنه‌ی همه پخشی کوچکتر انجام می‌دهند.

یک VLAN خصوصی توسط شناسه VLAN اصلی[۱٤] خود شناخته می‌شود. یک شناسه VLAN اصلی می تواند چندین شناسه VLAN جانبی[۱۵] را همراه با خود داشته باشد. VLANهای اصلی بی‌قاعده هستند، و بنابراین پورت‌های روی یک VLAN خصوصی می‌توانند با پورت‌های پیکربندی شده به‌عنوان VLAN اصلی، ارتباط داشته باشند. پورت‌های روی یک VLAN جانبی می‌توانند Isolated باشند، یعنی تنها با پورت‌های بی

[۱۳] Private VLANs
[۱٤] Primary VLAN ID
[۱۵] Secondary VLAN ID

قاعده ارتباط داشته باشند، یا Community باشند، یعنی هم با پورت‌های بی‌قاعده و هم با سایر پورت‌های VLAN جانبی خود ارتباط داشته باشند.

برای این که بتوانیم از VLANهای خصوصی بین یک میزبان و بقیه شبکه فیزیکی استفاده کنیم، سوئیچ فیزیکی متصل به میزبان لازم است که سازگار با VLAN خصوصی بوده و با شناسه‌های VLAN که توسط ESXi استفاده می‌شوند، پیکربندی شده باشد. برای سوئیچ‌های فیزیکی که از یادگیری مبتنی بر MAC+VLAN ID پویا استفاده می‌کنند، همه شناسه‌های VLAN خصوصی متناظر باید ابتدا در پایگاه‌داده VLAN سوئیچ وارد شوند.

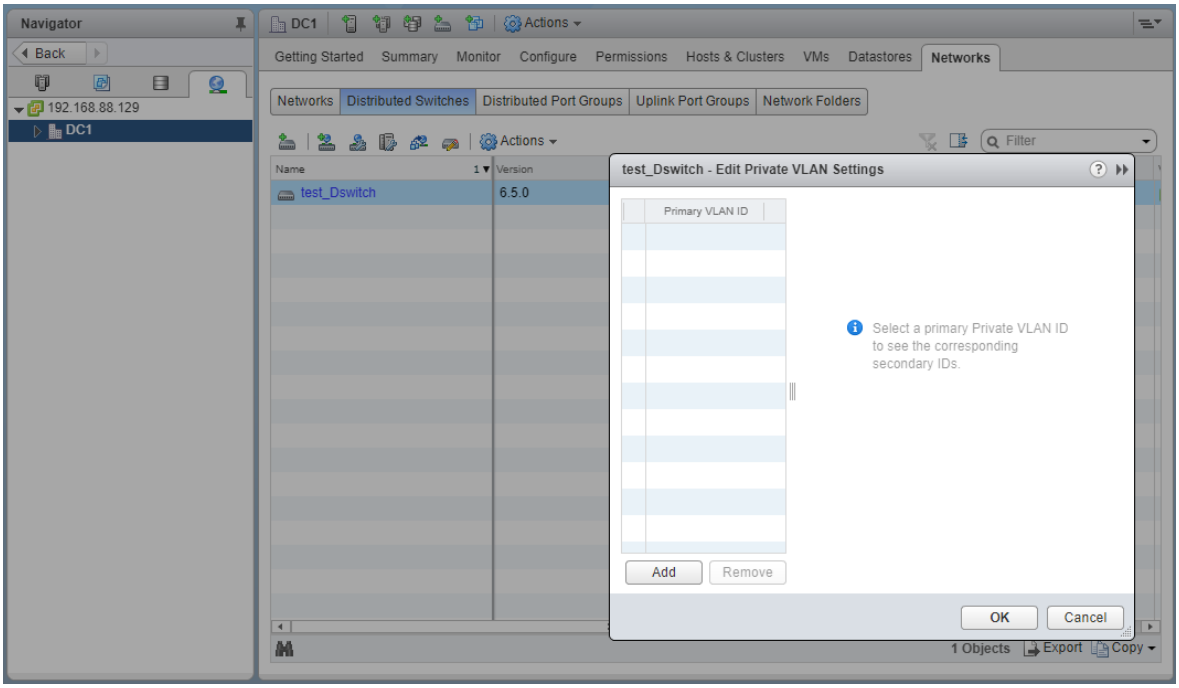
۳-٤ ایجاد یک VLAN خصوصی

VLANهای خصوصی مورد نیاز را روی سوئیچ توزیع‌شده vSphere ایجاد کنید تا توانایی تخصیص پورت های توزیع‌شده برای مشارکت در یک VLAN خصوصی را داشته باشید.

روش

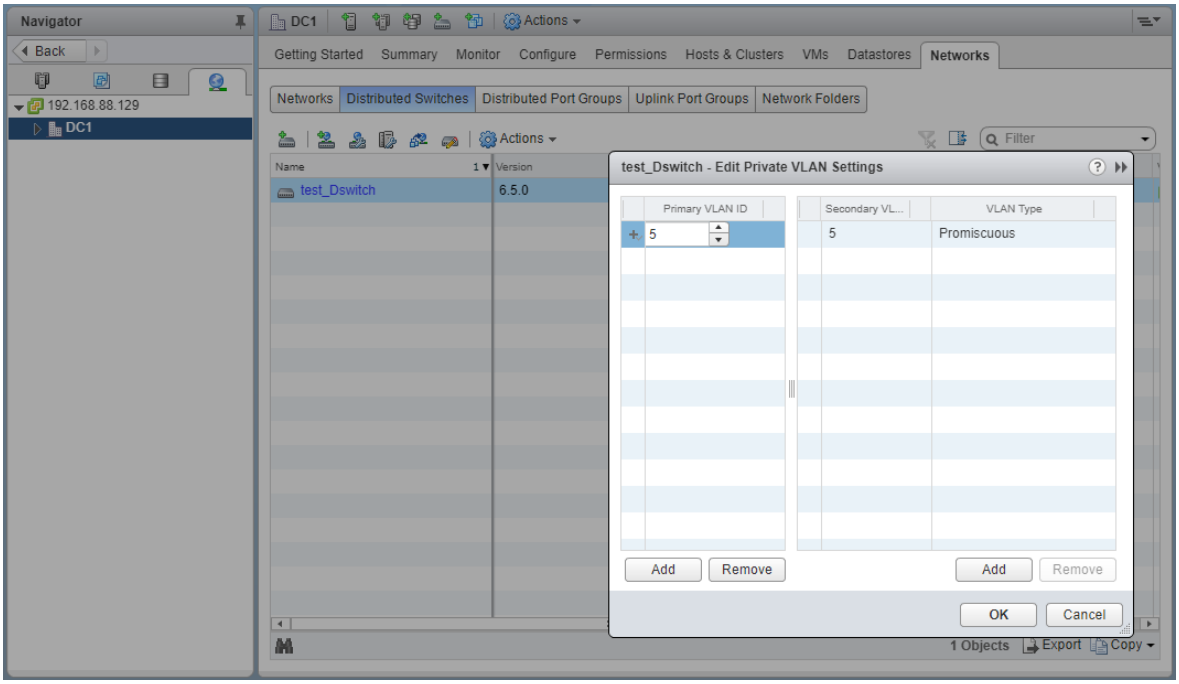
۷. در vSphere WebClient، سوئیچ توزیع‌شده را انتخاب کنید.

۸. به برگه Configure رفته، Settings را باز کرده و Private VLAN را انتخاب و Edit را کلیک کنید.



شکل ٦ ایجاد یک VLAN خصوصی (۱)

۹. برای اضافه کردن یک VLAN اصلی، زیر Primary VLAN ID بر روی Add کلیک کرده و ID یک VLAN اصلی را وارد کنید.



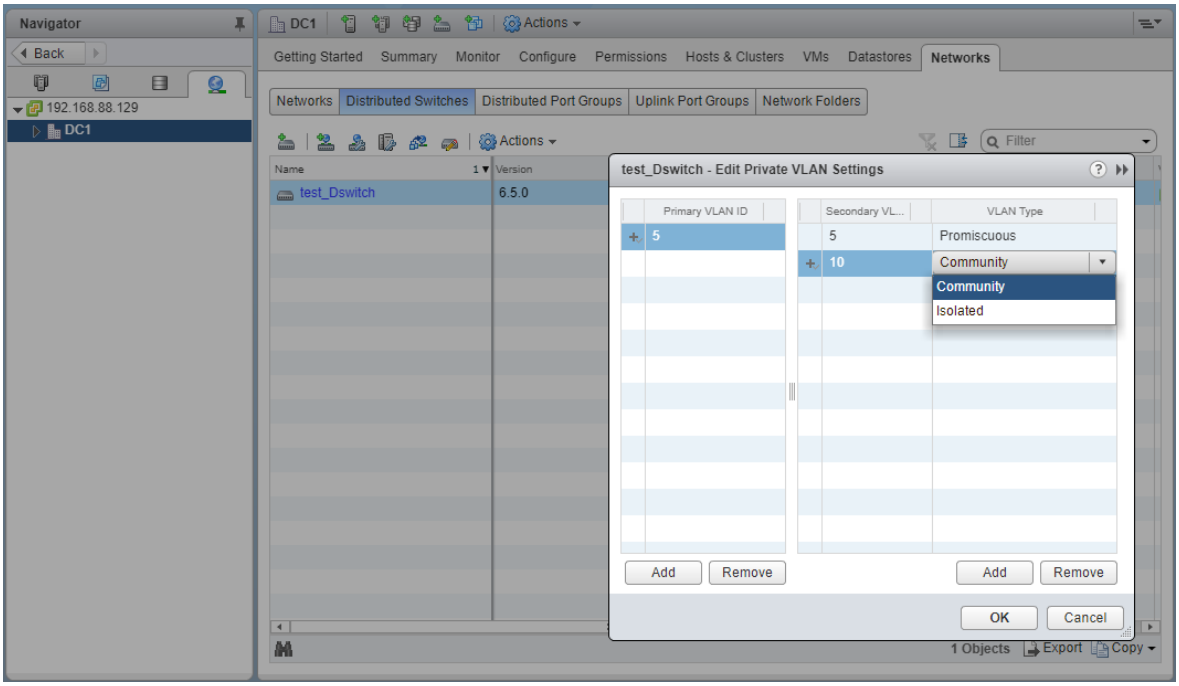
شکل ۷ ایجاد یک VLAN خصوصی (۲)

۱۰. روی علامت + که در جلوی شناسه VLAN اصلی قرار دارد کلیک کرده تا VLAN اصلی به لیست اضافه شود. VLAN خصوصی اصلی در جدول شناسه VLAN خصوصی جانبی نیز نمایش داده می‌شود.

۱۱. برای اضافه کردن یک VLAN جانبی، در پنجره سمت راست، بر روی Add کلیک کرده و شناسه VLAN را وارد کنید.

۱۲. روی علامت + که در جلوی شناسه VLAN جانبی قرار دارد کلیک کرده تا آن را به لیست اضافه کنید.

۱۳. از منوی کشویی ستون secondary VLAN type، یا Isolated و یا Community را انتخاب کنید.



شکل ۸ ایجاد یک VLAN خصوصی (۲)

۱۴. OK را کلیک کنید.

۳-۵ حذف یک VLAN خصوصی اصلی

بهتر است که VLANهای خصوصی اصلی بدون استفاده را از پیکربندی سوئیچ توزیع‌شده VSphere خود حذف کنید. زمانی که یک VLAN خصوصی اصلی را حذف می‌کنید، تمام VLANهای خصوصی جانبی مرتبط با آن نیز حذف می‌شوند.

پیش‌نیازها

مطمئن شوید که هیچ پورت‌گروهی از VLAN اصلی و VLANهای جانبی مرتبط با آن استفاده نمی‌کند.

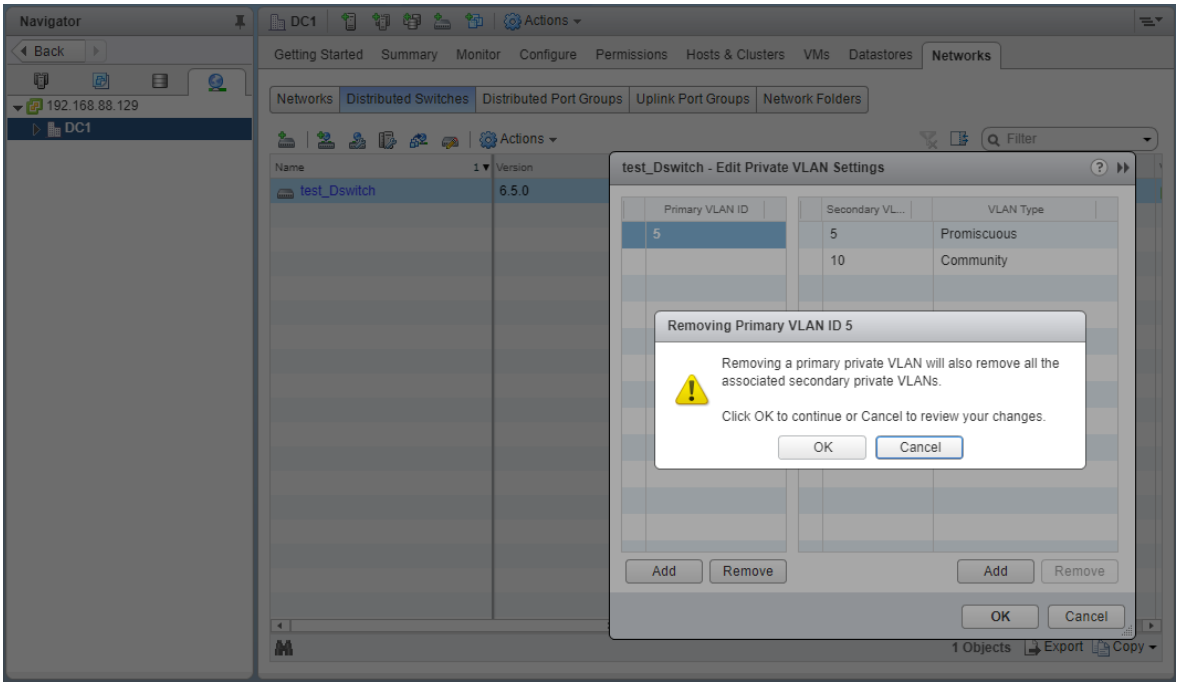
روش

۱. در vSphere WebClient، سوئیچ توزیع‌شده را انتخاب کنید.

۲. به برگه Configure رفته، Settings را باز کرده و Private VLAN را انتخاب کنید.

۳. Edit را کلیک کنید.

٤. VLAN خصوصی اصلی مورد نظر را انتخاب کرده و بر روی Remove و سپس OK کلیک کنید.



شکل ۹ حذف یک VLAN خصوصی اصلی

۶-۳ حذف یک VLAN خصوصی جانبی

بهتر است که VLANهای خصوصی جانبی بدون استفاده را از پیکربندی سوئیچ توزیع‌شده VSphere خود حذف کنید.

پیش‌نیازها

مطمئن شوید که هیچ پورت‌گروهی از VLAN جانبی استفاده نمی‌کند.

روش

۱. در vSphere WebClient، سوئیچ توزیع‌شده را انتخاب کنید.

۲. به برگه Configure رفته، Settings را باز کرده و Private VLAN را انتخاب کنید.

۳. Edit را کلیک کنید.

٤. یک VLAN خصوصی اصلی را انتخاب کنید، VLANهای خصوصی جانبی مرتبط با آن در سمت راست ظاهر می‌شوند.

۵. VLAN خصوصی جانبی مورد نظر را انتخاب کنید.

٦. بر روی Remove و سپس OK کلیک کنید.

٤ پیکربندی SNMP

از پیکربندی صحیح SNMP مطمئن شوید. اگر SNMP به صورت درست پیکربندی نشده باشد، اطلاعات تحت نظارت می‌توانند به یک میزبان مخرب فرستاده شوند. سپس میزبان مخرب می‌تواند از این اطلاعات استفاده کرده و طراحی یک حمله را انجام دهد. SNMP باید بر روی هر میزبان ESXi پیکربندی شود. شما می‌توانید از vCLI، PowerCLI یا vSphere Web Services SDK برای پیکربندی استفاده کنید.

روش

۱. دستور esxcli system snmp get را اجرا کنید تا تعیین شود که آیا میزبان در حال استفاده از SNMP است.

```
The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~] esxcli system snmp get
   Authentication:
   Communities:
   Enable: false
   Engineid:
   Hwsrc: indications
   Largestorage: true
   Loglevel: info
   Notraps:
   Port: 161
   Privacy:
   Remoteusers:
   Syscontact:
   Syslocation:
   Targets:
   Users:
   V3targets:
[root@localhost:~]
```

شکل ۱۰ بررسی فعال بودن SNMP

۲. اگر سیستم شما به SNMP نیاز دارد، با اجرای دستور esxcli system snmp set --enable true مطمئن شوید که در حال اجرا است.

٥ امنیت پروتکل اینترنت

امنیت پروتکل اینترنت (IPsec) ارتباطات IP که از یک میزبان می‌آیند یا به یک میزبان می‌رسند را امن می‌کند. میزبان‌های ESXi از IPsec با استفاده از IPv6 پشتیبانی می‌کنند.

وقتی که IPsec را روی یک میزبان تنظیم می‌کنید، در حقیقت احرازاصالت و رمزنگاری را برای بسته‌های ورودی و خروجی فعال می‌کنید. زمان و چگونگی رمزنگاری ترافیک IP بستگی به نحوه‌ی تنظیم انجمن‌های امنیتی[۱۶] و سیاست‌های امنیتی[۱۷] دارد.

یک انجمن امنیتی مشخص می‌کند که سیستم چگونه ترافیک را رمزنگاری کند. زمانی که یک انجمن امنیتی را ایجاد می‌کنید، منبع و مقصد، پارامترهای رمزنگاری، و یک نام برای انجمن امنیتی را مشخص می‌کنید.

یک سیاست امنیتی مشخص می‌کند که سیستم چه زمانی باید رمزنگاری را انجام دهد. سیاست امنیتی شامل اطلاعات منبع و مقصد، پروتکل و جهتی است که ترافیک باید رمزنگاری شود، حالت (انتقال[۱۸] یا تونل[۱۹])، و انجمن امنیتی مورد استفاده است.

۱-۵ فهرست کردن انجمن‌های امنیتی موجود

ESXi می‌تواند تمام انجمن‌های امنیتی موجود برای استفاده توسط سیاست‌های امنیتی را فهرست کند. این فهرست هم شامل انجمن‌های امنیتی ایجاد شده توسط کاربر است و هم شامل انجمن‌های امنیتی که VMkernel با استفاده از Internet Key Exchange نصب کرده است. می‌توان با استفاده از دستور esxcli vSphere CLI، فهرستی انجمن‌های امنیتی موجود را مشاهده کرد.

روش

- در خط فرمان، دستور esxcli network ip ipsec sa list را وارد کنید.

```
[root@localhost:~] esxcli network ip ipsec sa list
Name  Source Address             Destination Address       State   SPI     Mode       Encryption Algorithm  Integrity Algorithm  Lifetime
----  ------------------------  ------------------------  ------  ------  ---------  --------------------  -------------------  --------
sa1   fe80::ec5a:5699:9ac4:a2fe  fe80::20c:29ff:fe63:b6a0  mature  0x1000  transport  3des-cbc              hmac-sha1            infinite
[root@localhost:~]
```

شکل ۱۱ نمایش فهرست انجمن‌های امنیتی موجود

[۱۶] security associations

[۱۷] security policies

[۱۸] Transport

[۱۹] Tunnel

۲-۵ اضافه کردن یک انجمن امنیتی IPsec

می‌توان یک انجمن امنیتی را برای مشخص کردن پارامترهای رمزنگاری برای ترافیک IP مشخص، اضافه کرد. این کار را می‌توان با استفاده از دستور esxcli vSphere CLI انجام داد.

روش

- در خط فرمان، دستور esxcli network ip ipsec sa add را با یک یا چند تا از گزینه‌هایی که در جدول ۲ آمده است، وارد کنید.

جدول ۲ گزینه‌های موجود برای دستور اضافه کردن انجمن امنیتی جدید

گزینه	توصیف
--sa-source= source address	ضروری. آدرس منبع را مشخص می‌کند.
--sa-destination= destination address	ضروری. آدرس مقصد را مشخص می‌کند.
--sa-mode= mode	ضروری. حالت انتقال یا تونل را مشخص می‌کند.
--sa-spi= security parameter index	ضروری. شاخص پارامتر امنیتی را مشخص می‌کند. شاخص پارامتر امنیتی، انجمن امنیتی را به میزبان معرفی می‌کند. این گزینه باید هگزادسیمال با پیشوند 0x باشد. هر انجمن امنیتی که ایجاد می‌کنید باید یک ترکیب منحصربه‌فرد از پروتکل و شاخص پارامتر امنیتی داشته باشد.
--encryption-algorithm= encryption algorithm	ضروری. با استفاده از یکی از پارامترهای زیر الگوریتم رمزنگاری را مشخص می‌کند. • 3des-cbc • aes128-cbc • null (رمزنگاری انجام نمی‌دهد)
--encryption-key= encryption key	این گزینه زمانی مورد نیاز است که یک الگوریتم رمزنگاری مشخص شده باشد. کلید رمزنگاری را تعیین می‌کند. کلیدها را

می‌توان به صورت متن اسکی یا با یک هگزادسیمال با یک پیشوند 0x، وارد کرد.	
ضروری. الگوریتم احرازاصالت را مشخص می‌کند، hmac-sha1 یا hmac-sha2-256.	--integrity-algorithm= authentication algorithm
ضروری. کلید احرازاصالت را تعیین می‌کند. کلیدها را می‌توان به صورت متن اسکی یا با یک هگزادسیمال با یک پیشوند 0x، وارد کرد.	--integrity-key= authentication key
ضروری. یک نام برای انجمن امنیتی ارائه می‌کند.	--sa-name=name

مثال: دستور ایجاد انجمن امنیتی جدید

مثال زیر به منظور خوانایی بیشتر حاوی خطوط اضافی است.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x697076367265616479 6c6f676f33646573736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x697076367265616479 6c6f67736861316f757432
--sa-name sa1
```

```
[root@localhost:~] esxcli network ip ipsec sa add --sa-source fe80::ec5a:5699:9ac4:a2fe --sa-destination fe80:
:20c:29ff:fe63:b6a0 --sa-mode transport --sa-spi 0x1000 --encryption-algorithm 3des-cbc --encryption-key 0x697
07636726561647 96c6f676f33646573736362636f757432 --integrity-algorithm hmac-sha1 --integrity-key 0x69707636726561
64796c6f67736861316f757432 --sa-name sa1
[root@localhost:~]
```

شکل ۱۲ ایجاد انجمن امنیتی جدید

۵-۳ حذف یک انجمن امنیتی IPsec

می‌توان یک انجمن امنیتی را با استفاده از دستور ESXCLI vSphere CLI command حذف کرد. به این منظور باید اطمینان حاصل کنید که انجمن امنیتی که قصد حذف کردن آن را دارید، در حال حاضر در حال استفاده نباشد. در صورتی که سعی کنید که یک انجمن امنیتی که در حال استفاده است را حذف کنید، عملیات با شکست مواجه می‌شود.

روش

- در خط فرمان، دستور زیر را وارد کنید.

esxcli network ip ipsec sa remove --sa-name security_association_name

۵-۴ فهرست کردن سیاست‌های امنیتی IPsec موجود

فهرست سیاست‌های امنیتی موجود را می‌توان با استفاده از دستور ESXCLI vSphere CLI مشاهده کرد.

روش

- در خط فرمان دستور esxcli network ip ipsec sp list را وارد کنید.

```
[root@localhost:~] esxcli network ip ipsec sp list
Name  Source Address              Source Port  Destination Address         Destination Port  Protocol  Flow  Action   Mode     SA Name
----  --------------------------  -----------  --------------------------  ----------------  --------  ----  -------  -------  -------
sp1   fe80::ec5a:5699:9ac4:a2fe/64           0  fe80::20c:29ff:fe63:b6a0/64              22  tcp       out   discard  unknown  none
[root@localhost:~]
```

شکل ۱۳ نمایش فهرست سیاست‌های امنیتی موجود

۵-۵ ایجاد یک سیاست امنیتی IPsec

برای تعیین زمان استفاده از پارامترهای احرازاصالت و رمزنگاری که در یک انجمن امنیتی تنظیم شده است، باید یک سیاست امنیتی تعریف شود. یک سیاست امنیتی را می‌توان با استفاده از دستور ESXCLI vSphere CLI command اضافه کرد. قبل از ایجاد یک سیاست امنیتی، بایستی یک انجمن امنیتی با پارامترهای احرازاصالت و رمزنگاری مناسب، اضافه شود.

روش

- در خط فرمان دستور esxcli network ip ipsec sp add را با یکی یا بیشتر از گزینه‌های زیر وارد کنید.

جدول ۳ گزینه‌های موجود برای دستور اضافه کردن سیاست امنیتی جدید

گزینه	توصیف
--sp-source= source address	ضروری. آدرس منبع و طول پیشوند را مشخص می‌کند.
--sp-destination= destination address	ضروری. آدرس مقصد و طول پیشوند را مشخص می‌کند.
--source-port= port	ضروری. پورت مبدأ را مشخص می‌کند. پورت مبدأ باید یک عدد بین صفر تا ۶۵۵۳۵ باشد.
--destination-port= port	ضروری. پورت مقصد را مشخص می‌کند. پورت مقصد باید یک عدد بین صفر تا ۶۵۵۳۵ باشد.
--upper-layer-protocol= protocol	پروتکل لایه بالاتر را مشخص می‌کند که یکی از موارد زیر است. • tcp • udp • icmp6 • any
--flow-direction= direction	جهتی را مشخص می‌کند که قصد نظارت بر ترافیک آن را داریم، که یکی از موارد in یا out است.
--action= action	به وسیله‌ی یکی از موارد زیر، مشخص می‌کند که در مواجه شدن با ترافیکی با پارامترهای مشخص شده چه عملی انجام شود. • none: هیچ عملی انجام نمی‌دهد. • discard: اجازه نمی‌دهد که داده وارد یا خارج شود. • ipsec: از اطلاعات احرازاصالت و رمزنگاری عرضه شده در انجمن امنیتی استفاده می‌کند تا تعیین کند که آیا داده‌ها از یک منبع امن می‌آیند.

--sp-mode= mode	حالت tunnel یا transport را مشخص می‌کند.
--sa-name=security association name	ضروری. نام انجمن امنیتی را مشخص می‌کند که این سیاست امنیتی باید از آن استفاده کند.
--sp-name=name	ضروری. یک نام برای سیاست امنیتی ارائه می‌کند.

مثال: دستور ایجاد سیاست امنیتی جدید

مثال زیر به منظور خوانایی بیشتر حاوی خطوط اضافی است.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

۶-۵ حذف یک سیاست امنیتی IPsec

یک سیاست امنیتی از یک میزبان EXSi را می‌توان با استفاده از دستور ESXCLI vSphere CLI حذف کرد. به این منظور باید اطمینان حاصل کنید که سیاست امنیتی که قصد حذف کردن آن را دارید، در حال حاضر در حال استفاده نباشد. در صورتی که سعی کنید که یک سیاست امنیتی که در حال استفاده است را حذف کنید، عملیات با شکست مواجه می‌شود.

روش

- در خط فرمان، دستور زیر را وارد کنید.

esxcli network ip ipsec sp remove --sp-name security policy name

برای حذف همه سیاست‌های امنیتی می‌توان از دستور esxcli network ip ipsec sp remove --remove-all استفاده کرد.

٦ بهترین تجربه‌های امنیتی شبکه vSphere

با دنبال کردن بهترین تجربه‌ها برای امن کردن شبکه می‌توانید از صحت محیط vSphere خود اطمینان حاصل کنید.

٦-١ توصیه‌های عمومی امنیت شبکه

دنبال کردن توصیه‌های عمومی امنیت شبکه، اولین قدم در امن‌سازی محیط شبکه است. پس از آن می‌توانید به موارد خاصی مانند امن کردن شبکه با استفاده از دیواره آتش یا استفاده از IPsec بپردازید.

- در صورتی که پروتکل درخت پوشا[٢٠] (STP) فعال است، مطمئن شوید که پورت‌های سوئیچ فیزیکی به Portfast پیکربندی شده‌اند. از آنجایی که سوئیچ‌های مجازی VMware از STP پشتیبانی نمی کنند، پورت‌های سوئیچ فیزیکی متصل به یک ESXi باید به منظور اجتناب از به وجود آمدن حلقه در شبکه سوئیچ فیزیکی، به Portfast پیکربندی شده باشند. در صورتی که Portfast تنظیم نشده باشد، ممکن است مسائل و مشکلات مربوط به کارایی و اتصال به وجود آید.
- مطمئن شوید که ترافیک Netflow برای یک سوئیچ مجازی توزیع‌شده[٢١] تنها به آدرس‌های IP جمع کننده[٢٢]های مجاز فرستاده می‌شود. از آنجا که ارسال‌های Netflow رمزنگاری نمی‌شوند و ممکن است شامل اطلاعاتی در مورد شبکه مجازی باشند، این اطلاعات پتانسیل انجام حمله مردی در میانه موفق را افزایش می‌دهد. همچنین مطمئن شوید که همه آدرس‌های IP هدف Netflow صحیح هستند.

[٢٠] Spanning tree protocol

[٢١] Distributed virtual switch

[٢٢] Collector

- مطمئن شوید که تنها مدیران مجاز با استفاده از کنترل دسترسی‌های مبتنی بر نقش، به مؤلفه‌های شبکه مجازی دسترسی دارند. به عنوان مثال، به مدیران ماشین مجازی تنها اجازه دسترسی به پورت‌گروه هایی[۲۳] را بدهید که ماشین‌های مجازی‌شان در آن‌ها قرار دارند. به مدیران شبکه اجازه دسترسی به همه مؤلفه‌های شبکه مجازی را بدهید، اما اجازه دسترسی به ماشین‌های مجازی را نه. محدود کردن دسترسی‌ها خطر پیکربندی‌های اشتباه، چه تصادفی باشد و چه مخرب، را کاهش داده و مفاهیم امنیتی کلیدی برای جدا کردن وظایف و دادن کمترین امتیازات را اجرا می‌کند.
- مطمئن شوید که پورت‌گروه‌ها به مقدار Native VLAN پیکربندی نشده‌اند. سوئیچ‌های فیزیکی از VLAN 1 به عنوان Native VLAN استفاده می‌کنند. فریم‌های روی یک Native VLAN با ۱ برچسب‌گذاری نمی‌شوند. ESXi دارای Native VLAN نیست. فریم‌هایی که در یک پورت‌گروه با VLAN مشخص هستند برچسب دارند، و فریم‌هایی که در پورت‌گروهی هستند که برای آن VLAN تعریف نشده است برچسب ندارند. این مسأله می‌تواند یک مشکل را به وجود آورد. به عنوان مثال، فریم‌های روی VLAN 1 از یک سوئیچ فیزیکی سیسکو برچسب‌گذاری نشده‌اند، چون VLAN 1 روی آن سوئیچ فیزیکی Native VLAN است. اما، فریم‌هایی از میزبان ESXi که مربوط به VLAN 1 هستند با ۱ برچسب‌گذاری شده‌اند. در نتیجه، ترافیکی که از یک میزبان ESXi به مقصد Native VLAN ارسال می‌شود به صورت درست مسیریابی نمی‌شود، چون به جای این‌که برچسب‌گذاری نشده باشد با ۱ برچسب‌گذاری شده است. ترافیکی از سوئیچ فیزیکی که از Native VLAN می‌آید نیز قابل مشاهده نیست، چون برچسب‌گذاری نشده است. اگر پورت‌گروه سوئیچ مجازی ESXi از Native VLAN ID استفاده کند، ترافیک ماشین‌های مجازی روی آن پورت قابل مشاهده توسط Native VLAN روی سوئیچ نیست، چون سوئیچ انتظار ترافیک برچسب‌گذاری نشده را دارد.
- مطمئن شوید که پورت‌گروه‌ها برای VLANهای خود به مقادیری که توسط سوئیچ‌های فیزیکی رزرو شده است، پیکربندی نشده باشند. سوئیچ‌های فیزیکی VLAN IDهای خاصی را برای اهداف داخلی خود رزرو می‌کنند و اغلب اجازه عبور به ترافیک‌هایی که به این مقادیر پیکربندی شده باشند را نمی

[۲۳] Port groups

دهند. به عنوان مثال، سوئیچ‌های سیسکو کاتالیست معمولاً VLANهای ۱۰۲۴-۱۰۰۱ و ۴۰۹۴ را رزرو می‌کنند. استفاده از VLANهای رزرو شده ممکن است موجب وقفه در سرویس شبکه شود.

- مطمئن شوید که پورت‌گروه‌ها به VLAN با مقدار ۴۰۹۵ پیکربندی نشده باشند، مگر برای VGT. تنظیم یک پورت‌گروه به VLAN با مقدار ۴۰۹۵ حالت VGT را فعال می‌کند. در این حالت، سوئیچ مجازی همه فریم‌های شبکه را، بدون تغییر در برچسب VLAN به ماشین مجازی عبور می‌دهد، و برخورد با آن‌ها را به عهده ماشین مجازی می‌گذارد.
- پیکربندی مربوط به نادیده‌گرفتن[۲۴] پیکربندی‌های سطح پورت روی یک سوئیچ مجازی توزیع‌شده، را محدود کنید. نادیده‌گرفتن پیکربندی سطح پورت، به صورت پیش‌فرض غیرفعال است. وقتی فعال می‌شود، شما می‌توانید برای یک ماشین مجازی، از تنظیمات امنیتی متفاوتی، نسبت به تنظیمات سطح پورت‌گروه استفاده کنید. برخی ماشین‌های مجازی خاص نیاز به پیکربندی‌های منحصربه‌فردی دارند، اما نظارت در این موارد ضروری است. اگر بر overrideها نظارت نشود، هر کسی که با یک سوئیچ مجازی توزیع‌شده‌ی با پیکربندی امنیت پایین‌تر، به یک ماشین مجازی دسترسی داشته باشد، ممکن است تلاش کند که از دسترسی خود بهره‌برداری کند.
- مطمئن شوید که ترافیک mirror پورت سوئیچ مجازی توزیع‌شده، فقط به پورت‌های جمع‌کننده‌ی مجاز یا VLANهای مجاز ارسال می‌شود. یک سوئیچ توزیع‌شده vSphere می‌تواند ترافیک را از یک پورت به پورت دیگر mirror کند تا به وسیله‌های مربوط به ضبط بسته‌ها اجازه‌ی جمع‌آوری جریان های ترافیک خاص را بدهد. Port mirroring یک کپی از همه ترافیک مشخص شده را به صورت غیر رمزشده ارسال می‌کند. این ترافیک شامل کل داده‌های بسته‌های ضبط شده است و در صورت هدایت اشتباه می‌تواند منجر به افشای کل داده شود. در صورتی که port mirroring مورد نیاز است، مطمئن شوید که تمام VLANها، پورت‌ها و شناسه‌های uplink مقصد درست هستند.

[۲۴] Override

۶-۲ برچسب‌گذاری مؤلفه‌های شبکه

شناسایی مؤلفه‌های متفاوت معماری شبکه شما مهم است و به شما اطمینان می‌دهد که هیچ خطایی در هنگام رشد شبکه به وجود نمی‌آید.

بهترین تجربه‌های زیر را دنبال کنید:

- اطمینان حاصل کنید که پورت‌گروه‌ها با یک برچسب شبکه[۲۵] واضح پیکربندی شده‌اند. این برچسب ها به عنوان یک توصیف‌گر کاربردی برای پورت‌گروه شناخته می‌شوند و به شما کمک می‌کنند تا در هنگام پیچیده‌تر شدن شبکه، عملکرد هر پورت‌گروه را شناسایی کنید.
- اطمینان حاصل کنید که هر سوئیچ توزیع‌شده‌ی vSphere دارای برچسب شبکه واضح است که نشان دهنده‌ی عملکرد یا زیرشبکه IP سوئیچ است. این برچسب به عنوان یک توصیف‌گر کاربردی برای سوئیچ است، درست همان‌طور که سوئیچ‌های فیزیکی نیاز به نام میزبان دارند. به‌عنوان مثال، شما می توانید یک سوئیچ را با عنوان internal برچسب بزنید تا نشان دهید که آن برای شبکه داخلی است. برچسب یک سوئیچ مجازی استاندارد را نمی‌توان تغییر داد.

۶-۳ مستندسازی و بررسی محیط vSphere VLAN

به منظور اجتناب از مشکلات، به طور مرتب محیط VLAN خود را بررسی کنید. به طور کامل محیط VLAN را مستند کرده و مطمئن شوید که شناسه‌های VLAN تنها یک بار استفاده می‌شوند. مستندات شما می‌تواند به عیب‌یابی کمک کند و همچنین زمانی که می‌خواهید محیط را گسترش دهید، این مستندات ضروری است.

روش

۱. اطمینان حاصل کنید که تمام سوئیچ‌های مجازی و شناسه‌های VLANها به طور کامل مستند شده‌اند.
۲. اطمینان حاصل کنید که شناسه‌های VLAN برای همه پورت‌گروه‌های مجازی توزیع‌شده به طور کامل مستند شده‌اند.

[۲۵] Network label

۳. اطمینان حاصل کنید که شناسه‌های VLAN خصوصی برای همه سوئیچ‌های مجازی توزیع‌شده به طور کامل مستند شده‌اند.

٤. اطمینان حاصل کنید که لینک‌های VLAN trunk تنها به پورت‌هایی از سوئیچ فیزیکی متصل می‌شوند که به عنوان لینک‌های trunk عمل می‌کنند.

٤-٦ اقدامات مربوط به جداسازی شبکه‌های با اهمیت بیشتر

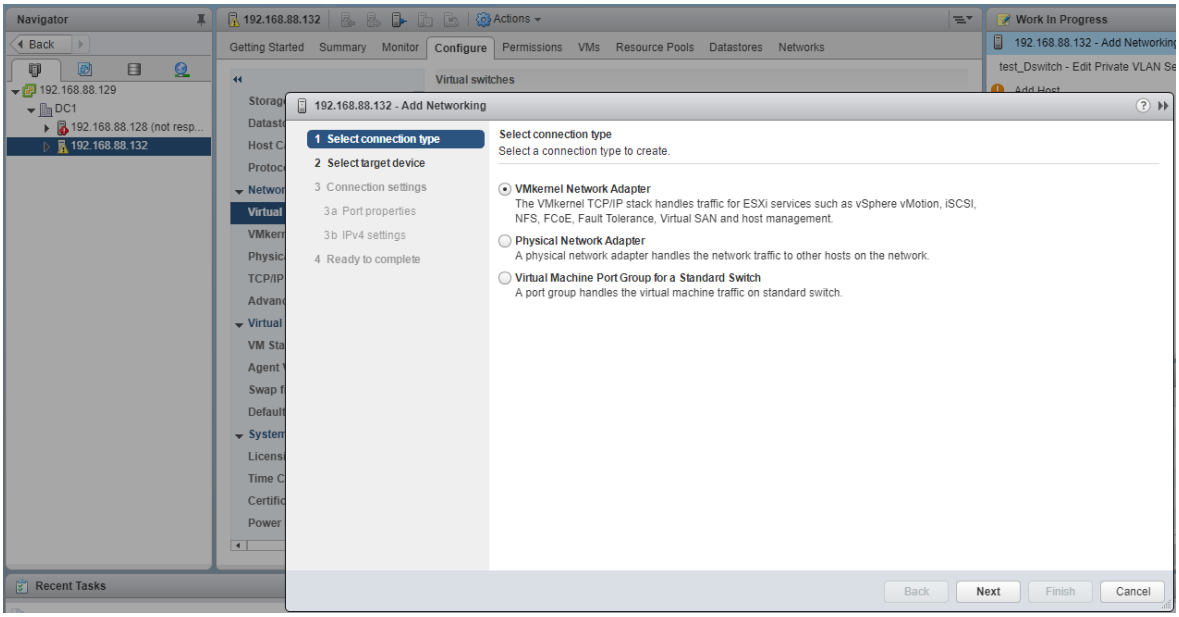
پذیرفتن اقدامات مربوط به جداسازی[۲۶] شبکه‌های با اهمیت بیشتر به طور قابل توجهی امنیت شبکه در محیط vSphere شما را تقویت می‌کند. به منظور جداسازی نوع خاصی از ترافیک، به صورت زیر عمل کنید.

روش:

۱. در vSphere WebClient، میزبان مورد نظر را انتخاب کنید.

۲. به برگه Configure رفته، و در بخش Networking گزینه Virtual switches را انتخاب کنید.

۳. آیکون Add host networking را کلیک کرده و در صفحه نمایش داده شده VMkernel Network Adaptor را انتخاب کنید.

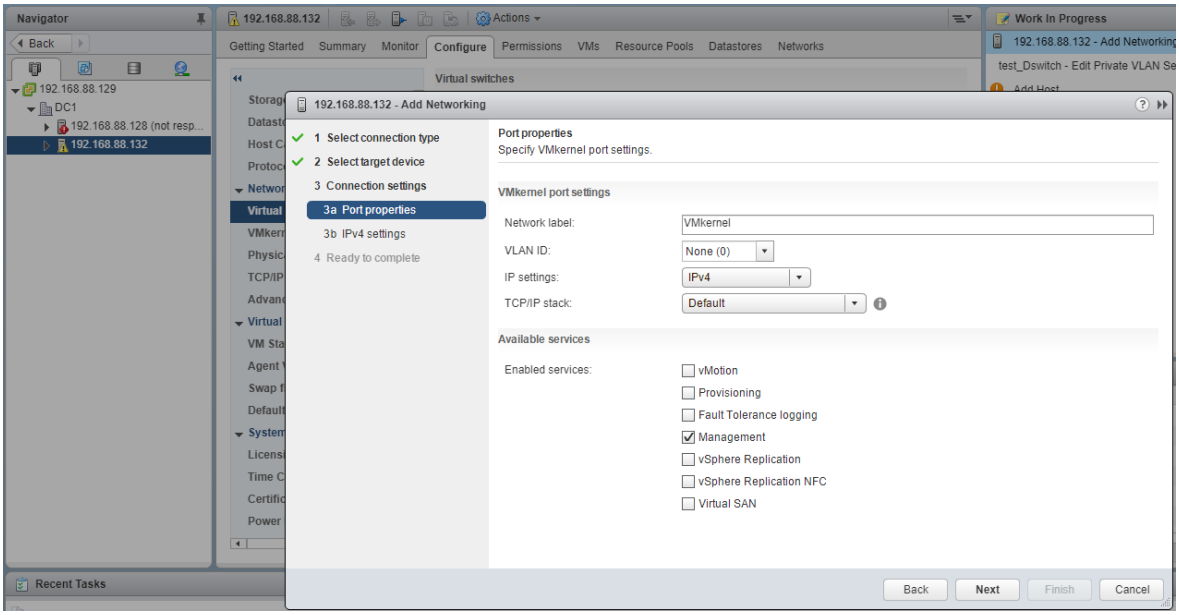


[۲۶] Isolation

شکل ۱۴ جداسازی ترافیک (۱)

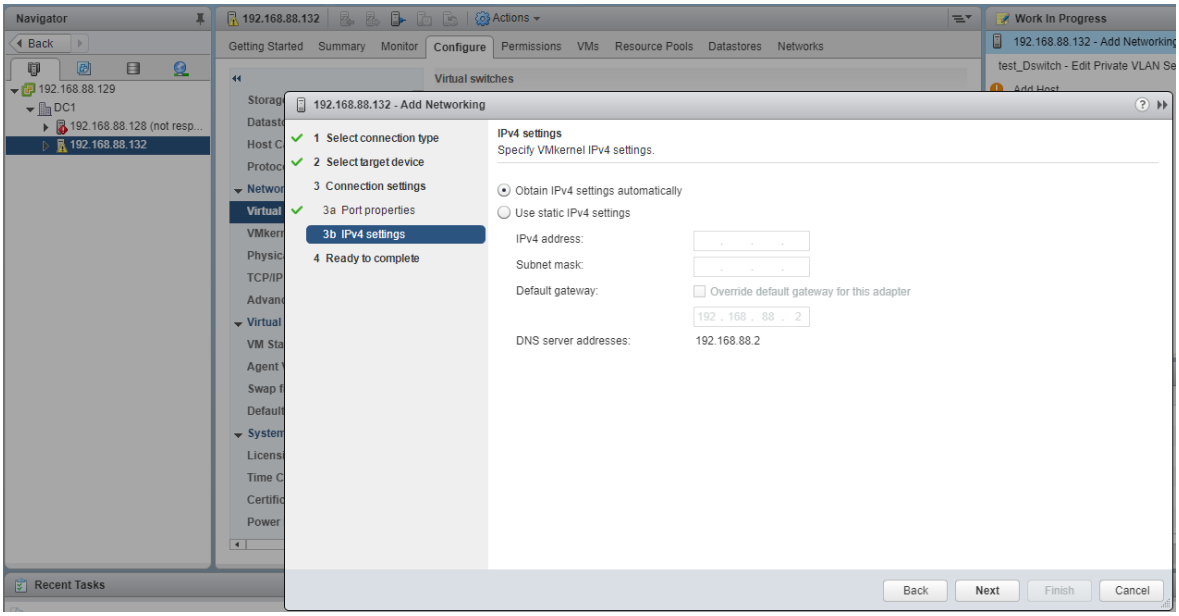
۴. در قسمت Select an existing standard switch سوئیچ مجازی مورد نظر را انتخاب کنید.

۵. در صفحه نمایش داده شده می‌توان Network label و VLAN ID را مشخص کرده و سایر تنظیمات مربوط به شبکه را انجام داد. در قسمت Available services با انتخاب هر کدام از گزینه‌ها می‌توان VLAN را به آن ترافیک اختصاص داد.



شکل ۱۵ جداسازی ترافیک (۲)

۶. در صفحه بعد تنظیمات مربوط به IP را انجام داده و در نهایت با کلیک بر روی دکمه Finish پورت‌گروه مورد نظر با VLAN ID مشخص شده به منظور عبور دادن نوع ترافیک مشخص شده، ساخته می‌شود.



شکل ۱۶ جداسازی ترافیک (۳)

۶-۴-۱ جداسازی شبکه مدیریتی

شبکه مدیریتی vSphere امکان دسترسی به واسط مدیریتی vSphere روی هر مؤلفه را به وجود می‌آورد. سرویس‌هایی که روی واسط مدیریتی اجرا می‌شوند، برای یک مهاجم فرصت دسترسی دارای امتیاز به سیستم‌ها را به وجود می‌آورند. به احتمال زیاد با دسترسی به این شبکه حملات از راه دور آغاز خواهد شد. اگر یک مهاجم به شبکه مدیریتی دسترسی پیدا کند، زمینه برای نفوذ بیشتر فراهم خواهد شد. دسترسی به شبکه مدیریتی را با محافظت از آن در سطح امنیتی امن‌ترین ماشین مجازی که روی میزبان ESXi یا روی کلاستر اجرا می شود، به شدت کنترل کنید. مهم نیست که چقدر شبکه مدیریتی محدود شده است، در هر صورت مدیران باید اجازه دسترسی به این شبکه را داشته باشند تا بتوانند پیکربندی میزبان‌های ESXi و سیستم سرویس‌دهنده vCenter را انجام دهند.

پورت‌گروه مدیریتی vSphere را در یک VLAN اختصاصی روی یک سوئیچ مجازی مشترک قرار دهید. تا زمانی که VLAN مربوط به پورت‌گروه مدیریتی به وسیله‌ی ترافیک تولیدی توسط ماشین‌های مجازی استفاده نشود، سوئیچ مجازی می‌تواند با ترافیک تولید (ترافیک ماشین مجازی) به اشتراک گذاشته شود. بررسی کنید که قطعه این شبکه (مدیریت) مسیریابی نشود، مگر به شبکه‌هایی که در آن‌ها دیگر موجودیت‌های مدیریتی وجود داشته باشند. به طور خاص، اطمینان حاصل کنید که ترافیک تولیدی ماشین مجازی به این شبکه (مدیریت) مسیریابی نشود.

با استفاده از یکی از رویکردهای زیر، دسترسی به عملکردهای مدیریت را با یک کنترل دقیق فعال کنید.

- برای محیط‌های بسیار حساس، یک دروازه کنترل‌شده یا سایر روش‌های کنترل‌شده را برای دسترسی به شبکه مدیریت، پیکربندی کنید. به عنوان مثال، لازم است که مدیران از طریق یک VPN به شبکه مدیریت متصل شوند و اجازه دسترسی را تنها به مدیران مورد اعتماد بدهند.
- جعبه‌های پرش که سرویس‌گیرنده‌های مدیریت را اجرا می‌کنند، را پیکربندی کنید.

٦-٤-٢ جداسازی ترافیک ذخیره‌سازی

اطمینان حاصل کنید که ترافیک ذخیره‌سازی مبتنی بر IP جداسازی شده است. ذخیره‌سازی مبتنی بر IP شامل iSCSI و NFS است. ماشین‌های مجازی ممکن است که سوئیچ‌های مجازی و VLANها را با پیکربندی‌های ذخیره‌سازی مبتنی بر IP به اشتراک بگذارند. این نوع پیکربندی ممکن است ترافیک ذخیره‌سازی مبتنی بر IP را در اختیار کاربران غیرمجاز ماشین مجازی قرار دهد.

ذخیره‌سازی مبتنی بر IP اغلب رمزنگاری نمی‌شود؛ هر کسی که به این شبکه دسترسی داشته باشد می‌تواند آن را ببیند. برای محدودکردن کاربران غیرمجاز از مشاهده ترافیک ذخیره‌سازی مبتنی بر IP، به صورت منطقی ترافیک شبکه‌ای ذخیره‌سازی مبتنی بر IP را از ترافیک تولیدی جدا کنید. همچنین آداپتورهای ذخیره‌سازی مبتنی بر IP را روی VLANها یا قطعات شبکه‌ای مجزا از شبکه مدیریتی VMkernel، پیکربندی کنید تا کاربران غیرمجاز را در دیدن ترافیک محدود کنید.

٦-٤-٣ جداسازی ترافیک VMotion

ترافیک مهاجرت Vmotion به صورت متن آشکار انتقال داده می‌شود. هر کسی با دسترسی به شبکه‌ای که این ترافیک روی آن جریان دارد، می‌تواند آن را مشاهده کند. مهاجمان بالقوه می‌توانند با شنود ترافیک VMotion، محتویات حافظه یک ماشین مجازی را به دست آورند. همچنین آن‌ها می‌توانند با انجام حمله مردی در میانه، محتویات را در حین مهاجرت تغییر دهند.

ترافیک VMotion را روی یک شبکه مجزا، از ترافیک تولید جدا کنید. شبکه را به گونه‌ای تنظیم کنید که غیرقابل مسیریابی باشد، یعنی مطمئن شوید که هیچ مسیریابی لایه ۳ بین این شبکه و دیگر شبکه‌ها انجام نمی شود، تا بتوانید از دسترسی خارجی به شبکه جلوگیری کنید.

پورت‌گروه VMotion باید در یک VLAN اختصاصی روی سوئیچ مجازی مشترک قرار داده شود. تا زمانی که VLAN مربوط به پورت‌گروه VMotion توسط ترافیک تولیدی ماشین‌های مجازی استفاده نمی‌شود، می توان سوئیچ مجازی را با ترافیک تولیدی ماشین مجازی به اشتراک گذاشت.

٦-٥ محدودکردن استفاده از سوئیچ‌های مجازی با vSphere Network Appliance API

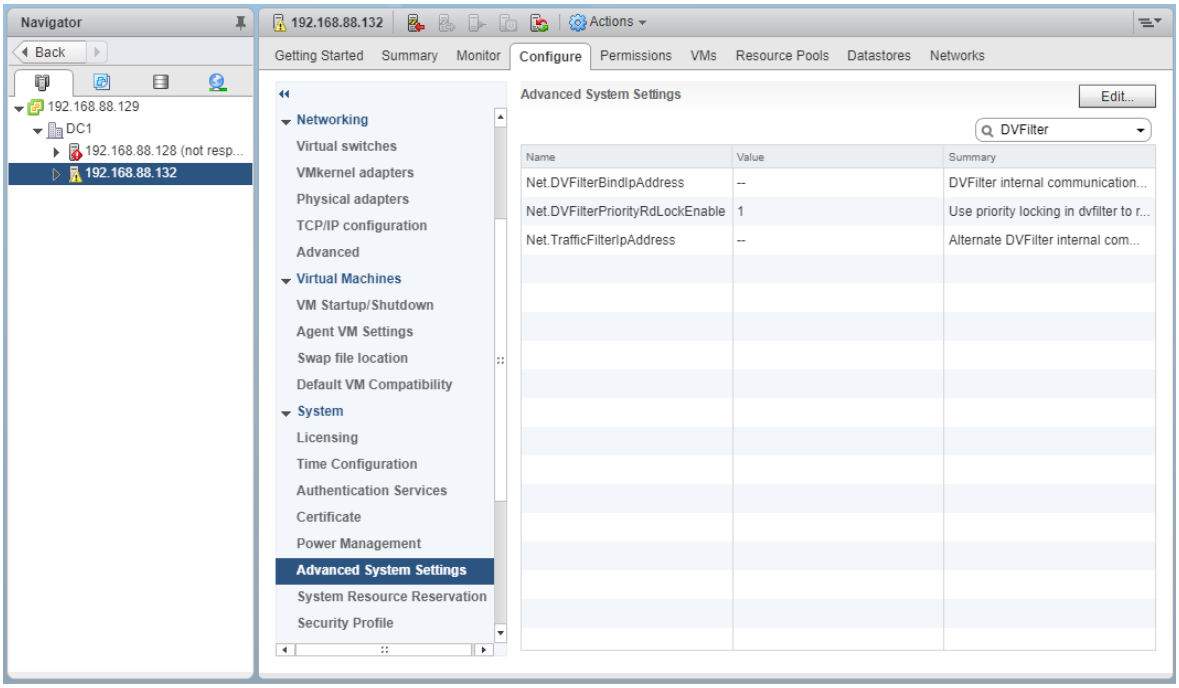
فقط در صورت نیاز از سوئیچ‌های مجازی با vSphere Network Appliance API استفاده کنید. اگر از محصولاتی استفاده نمی‌کنید که از vSphere Network Appliance API (DvFilter) استفاده می‌کنند، میزبان خود را به گونه‌ای پیکربندی نکنید که اطلاعات شبکه را به یک ماشین مجازی ارسال کند. اگر vSphere Network Appliance API فعال باشد، یک مهاجم ممکن است برای اتصال یک ماشین مجازی به فیلتر تلاش کند. این اتصال ممکن است دسترسی به شبکه دیگر ماشین‌های مجازی روی میزبان را فراهم آورد.

اگر از محصولی استفاده می‌کنید که از این API استفاده می‌کند، مطمئن شوید که میزبان به درستی پیکربندی شده است. بخش‌های مربوط به DvFilter در Developing and Deploying vSphere Solutions، vServices، و ESX Agents، را ببینید. اگر میزبان شما برای استفاده از API تنظیم شده باشد، مطمئن شوید که مقدار پارامتر Net.DVFilterBindIpAddress مطابق با محصولی است که از API استفاده می‌کند.

روش

١. به vSphere Web Client وارد شوید.
٢. میزبان را انتخاب کرده و بر روی Configure کلیک کنید.
٣. در قسمت System گزینه Advanced System Settings را انتخاب کنید.
٤. مطمئن شوید که مقدار پارامتر Net.DVFilterBindIpAddress خالی است.
٥. تنظیمات زیر را بررسی کنید.

- اگر شما از تنظیمات DvFilter استفاده نمی‌کنید، مطمئن شوید که مقدار پارامتر خالی است.
- اگر شما از تنظیمات DvFilter استفاده می‌کنید، اطمینان حاصل کنید که مقدار پارامتر مطابق با مقداری است که محصولی که از DvFilter استفاده می‌کند، از آن استفاده کرده است.



شکل ۱۷ تنظیم پارامترهای DVFilter