Déployer Défense contre les menaces virtuelles à l'aide de VMware

Ce chapitre décrit les procédures pour déployer défense contre les menaces virtuelles dans un environnement VMware vSphere, soit dans un vSphere vCenter, soit sur un hôte ESXi autonome.

Aperçu

Cisco propose des périphériques défense contre les menaces virtuelles 64 bits pour les environnements d'hébergement VMware vSphere vCenter et ESXi. défense contre les menaces virtuelles est distribué dans un progiciel Open Virtualization Format (OVF) disponible sur Cisco.com. Le protocole OVF est une norme ouverte pour le conditionnement et la distribution d'applications logicielles pour des machines virtuelles. Un progiciel OVF contient plusieurs fichiers dans un seul répertoire.

Vous pouvez déployer défense contre les menaces virtuelles sur n'importe quel périphérique compatible avec VMware ESXi. Pour déployer défense contre les menaces virtuelles, vous devez connaître VMware et vSphere, y compris le réseau vSphere, la configuration et le paramétrage de l'hôte ESXi, ainsi que le déploiement des invités de machine virtuelle.

Prise en charge des fonctionnalités de VMware pour Défense contre les menaces virtuelles

Le tableau suivant énumère la prise en charge des fonctionnalités de VMware pour la défense contre les menaces virtuelles.

Tableau 1 : Prise en charge des fonctionnalités de VMware pour Défense contre les menaces virtuelles

Fonctionnalités	Description	Prise en charge (Oui/Non)	Commentaire
Clonage à froid	La machine virtuelle est hors tension pendant le clonage.	Non	–
vMotion	Utilisé pour la migration en direct des machines virtuelles.	Oui	Utiliser le stockage partagé. Voir la prise en charge de vMotion.
Distributed Resource Scheduler (DRS)	Surveille la charge de travail des machines virtuelles et résout les déséquilibres et identifie les machines virtuelles pour la migration en direct avec vMotion.	Non	Non admissible.
Ajout à chaud	La machine virtuelle est en cours d'exécution pendant un ajout.	Non	–
Clonage à chaud	La machine virtuelle est en cours d'exécution pendant le clonage.	Non	–
Suppression à chaud	La machine virtuelle est en cours d'exécution pendant la suppression.	Non	–
Instantané	La machine virtuelle se bloque pendant quelques secondes.	Non	Risque de situations de non-synchronisation entre centre de gestion et les périphériques gérés.
Suspendre et reprendre	La machine virtuelle est suspendue, puis reprend.	Oui	–
vCloud Director	Autorise le déploiement automatique des machines virtuelles.	Non	–
VMware FT	Utilisé pour la haute accessibilité sur les machines virtuelles.	Non	Utilisez la fonctionnalité de basculement pour les basculements de machine virtuelle défense contre les menaces virtuelles.

Fonctionnalités	Description	Prise en charge (Oui/Non)	Commentaire
VMware haute accessibilité avec pulsations de machine virtuelle	Utilisé pour les défaillances de machine virtuelle.	Non	Utilisez la fonctionnalité de basculement pour les basculements de machine virtuelle défense contre les menaces virtuelles.
Client Windows autonome VMware vSphere	Utilisé pour déployer les machines virtuelles.	Oui	–
Client Web VMware vSphere	Utilisé pour déployer les machines virtuelles.	Oui	–

Configuration système requise

Consultez le guide de compatibilité de Cisco Secure Firewall Threat Defense pour obtenir les informations les plus récentes sur la prise en charge de l'hyperviseur pour défense contre les menaces virtuelles.

Le matériel spécifique utilisé pour les déploiements défense contre les menaces virtuelles peut varier en fonction du nombre d'instances déployées et des exigences d'utilisation. Chaque instance de défense contre les menaces virtuelles nécessite une allocation minimale de ressources (quantité de mémoire, nombre de CPU et espace disque) sur le serveur.

Les systèmes exécutant VMware vCenter Server et les instances ESXi doivent satisfaire à des exigences spécifiques en matière de matériel et de système d'exploitation. Pour obtenir la liste des plateformes prises en charge, consultez le Guide de compatibilité en ligne de VMware .

Tableau 2 : Exigences des ressources de l'appareil Défense contre les menaces virtuelles

Paramètres	Valeur
Niveaux de performance	**Version 7.0 ou ultérieure** Le défense contre les menaces virtuelles prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement. • FTDv5 4vCPU/8Go (100 Mbit/s) • FTDv10 4 vCPU/8 Go (1 Gbit/s) • FTDv20 4vCPU/8 Go (3 Gbit/s) • FTDv30 8 vCPU/16 Go (5 Gbit/s) • FTDv50 12 vCPU/24 Go (10 Gbit/s) • FTDv100 16vCPU/32 Go (16 Gbit/s) Consultez le chapitre sur les licences dans le Guide d'administration Cisco Secure Firewall Management Center pour connaître les consignes relatives à l'octroi de licences pour votre périphérique défense contre les menaces virtuelles. **Remarque** Pour modifier les valeurs de vCPU/mémoire, vous devez d'abord éteindre le périphérique défense contre les menaces virtuelles.

Paramètres	Valeur
Nombre de cœurs et de mémoire	**Versions 6.4 à 6.7** Le défense contre les menaces virtuelles se déploie avec des ressources de base et de mémoire ajustables. Trois valeurs de paires de vCPU/mémoire sont prises en charge : • 4vCPU/8 Go (par défaut) • 8vCPU/16 Go • 12vCPU/24 Go **Remarque** Pour modifier les valeurs de vCPU/mémoire, vous devez d'abord éteindre le périphérique défense contre les menaces virtuelles. Seules les trois combinaisons ci-dessus sont prises en charge.
	Version 6.3 et antérieure Le défense contre les menaces virtuelles se déploie avec des ressources de vCPU et de mémoire fixes. Il n'y a qu'une seule valeur de paire vCPU/mémoire prise en charge : • 4vCPU/8 Go **Remarque** Les ajustements des vCPU et de la mémoire ne sont pas pris en charge.
Stockage	En fonction de la sélection du format de disque. • La taille du disque de provisionnement léger est de 48,24 Go.

Paramètres	Valeur
Cartes vNIC	La défense contre les menaces virtuelles prend en charge les adaptateurs de réseau virtuel suivants : • **VMXNET3** : Défense contre les menaces virtuelles sur VMware utilise maintenant les interfaces VMXNET3 par défaut lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Le pilote vmxnet3 utilise deux interfaces de gestion. Les deux premiers adaptateurs Ethernet doivent être configurés en tant qu'interfaces de gestion; une pour la gestion et l'enregistrement du périphérique , une pour les dépistages. • **IXGBE** : Le pilote ixgbe utilise deux interfaces de gestion. Les deux premiers appareils d'interconnexion des composants périphériques (PCI) doivent être configurés en tant qu'interfaces de gestion; l'une destinée à la gestion et à l'enregistrement du périphérique, l'autre ,pour les diagnostics. Le pilote ixgbe ne prend pas en charge les déploiements de basculement (HA) de défense contre les menaces virtuelles. • **E1000** : En utilisant des interfaces e1000, l'interface de gestion défense contre les menaces virtuelles (br1) du pilote e1000 est une interface en pont avec deux adresses MAC, l'une pour la gestion et l'autre pour les diagnostics. **Important** Pour les versions antérieures à 6.4, e1000 était l'interface par défaut pour défense contre les menaces virtuelles sur VMware. À partir de la version 6.4, défense contre les menaces virtuelles sur VMware utilise par défaut les interfaces vmxnet3. Si votre périphérique virtuel utilise actuellement des interfaces e1000, nous vous **recommandons fortement** de modifier vos interfaces vmxnet3. Consultez Configurez les interfaces VMXNET3, à la page 18 pour de plus amples renseignements. • **IXGBE-VF** : le pilote ixgbe-vf (10 Gbit/s) prend en charge les périphériques de fonction virtuels qui ne peuvent être activés que sur des noyaux prenant en charge SR-IOV. SR-IOV nécessite la prise en charge de la plateforme et du système d'exploitation appropriés; consultez la section Prise en charge de SR-IOV pour de plus amples renseignements.

Prise en charge de la technologie de virtualisation

- La technologie de virtualisation (VT) est un ensemble d'améliorations apportées aux nouveaux processeurs qui améliorent les performances des machines virtuelles en cours d'exécution. Votre système doit être doté de CPU qui prennent en charge les extensions Intel VT ou AMD-V pour la virtualisation matérielle. Intel et AMD fournissent tous deux des utilitaires d'identification de processeur en ligne pour vous aider à identifier les CPU et à déterminer leurs capacités.

- La VT peut être désactivée par défaut sur de nombreux serveurs qui comprennent des CPU avec prise en charge de VT, vous devez donc l'activer manuellement. Consultez la documentation du fabricant pour obtenir des instructions sur la façon d'activer la prise en charge de la VT sur votre système.

Remarque Si vos CPU prennent en charge la VT, mais que vous ne voyez pas cette option dans le BIOS, contactez votre fournisseur pour demander une version du BIOS qui vous permet d'activer la prise en charge de la VT.

Désactiver le traitement simultané hyperthreading

Nous vous recommandons de désactiver l'hyperthreading pour vos systèmes qui exécutent défense contre les menaces virtuelles; voir Traitement simultané Hyperthreading non recommandé, à la page 11. Les processeurs suivants prennent en charge l'hyperthreading et ont deux fils par cœur :

- Processeurs basés sur la microarchitecture de processeur Intel Xeon 5500.
- Intel Pentium 4 (compatible avec HT)
- Intel Pentium EE 840 (compatible avec HT)

Pour désactiver la technologie Hyperthreading, vous devez d'abord la désactiver dans les paramètres BIOS de votre système, puis la désactiver dans le client vSphere (notez que l'hyperthreading est activé par défaut pour vSphere). Consultez la documentation de votre système pour déterminer si votre CPU prend en charge l'hyperthreading.

Prise en charge de SR-IOV

Les fonctions virtuelles SR-IOV nécessitent des ressources système spécifiques. Un serveur prenant en charge SR-IOV est requis en plus d'un adaptateur PCIe compatible avec SR-IOV. Vous devez être conscient des considérations matérielles suivantes :

- Les capacités des cartes réseau SR-IOV, y compris le nombre de VF disponibles, varient selon les fournisseurs et les périphériques. Les cartes réseau suivantes sont prises en charge :
  - Adaptateur pour serveur Ethernet Intel X520, DA2
  - Adaptateur Intel pour serveur Ethernet X540
- Tous les logements PCIe ne prennent pas en charge SR-IOV.
- Les logements PCIe compatibles avec SR-IOV peuvent avoir des capacités différentes.
- CPU multicœur x86_64 – Pont Intel Sandy ou version ultérieure (recommandé).

Remarque Nous avons testé le défense contre les menaces virtuelles sur le processeur Broadwell d'Intel (E5-2699-v4) à 2,3 GHz.

- Cœurs
  - Au moins 8 cœurs physiques par connecteur de CPU.

Remarque Défense contre les menaces virtuelles ne prend pas en charge les nœuds multiples d'accès à la mémoire non uniforme (numéro) et plusieurs connecteurs de CPU pour les cœurs physiques.

- Assurez-vous d'affecter tous les cœurs physiques alloués à un seul connecteur.

Remarque L'épinglage de CPU est recommandé pour atteindre le débit maximal.

Consultez la documentation de votre fabricant pour connaître la prise en charge de SR-IOV sur votre système. Vous pouvez effectuer des recherches dans le Guide de compatibilité en ligne de VMware pour des recommandations de systèmes qui incluent la prise en charge de SR-IOV.

Prise en charge de SSSE3

- Défense contre les menaces virtuelles nécessite la prise en charge de SSSE3 ou SSE3S supplémentaire pour la diffusion en continu de SIMD Extensions 3, un ensemble d'instructions SIMD (Single Instruction Multiple Data) créé par Intel.
- Votre système doit être doté de processeurs prenant en charge SSSE3, comme les processeurs Intel Core 2 Duo, Intel Core i7/i5/i3, Intel ATOM, AMD Bulldozer, AMD Bobcat et des processeurs plus récents.
- Consultez cette page de référence pour plus d'informations sur le jeu d'instructions SSSE3 et les CPU qui prennent en charge SSSE3.

Vérifier la prise en charge de la CPU

Vous pouvez utiliser la ligne de commande Linux pour obtenir des informations sur le matériel de la CPU. Par exemple, le fichier **/process/cpuinfo** contient des détails sur les cœurs de CPU individuels. Affiche son contenu avec **less** ou **cat**.z

Vous pouvez consulter la section des indicateurs pour obtenir les valeurs suivantes :

- vmx : extensions VT Intel
- svm : extensions AMD-V
- ssse3 : extensions SSSE3

Utilisez la commande **grep** pour vérifier si l'une de ces valeurs existe dans le fichier en exécutant la commande suivante :

```
egrep "vmx|svm|ssse3" /proc/cpuinfo
```

Si votre système prend en charge la VT ou SSSE3, vous devriez voir vmx, svm ou ssse3 dans la liste d'indicateurs. L'exemple suivant montre la sortie d'un système à deux CPU :

```
flags    : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm
```

```
flags    : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm
```

Lignes directrices et limites relatives à la licence

Niveaux de performance pour les licences Smart Défense contre les menaces virtuelles

Le défense contre les menaces virtuelles prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement.

Tableau 3 : Défense contre les menaces virtuelles Limites des fonctionnalités sous licence en fonction des droits

Niveau de performance	Caractéristiques du périphérique (cœur/RAM)	Limite du débit	Limite de session RA VPN
FTDv5, 100 Mbit/s	4 cœurs/8 Go	100 Mbit/s	50
FTDv10, 1 Gbit/s	4 cœurs/8 Go	1 Gbit/s	250
FTDv20, 3 Gbit/s	4 cœurs/8 Go	3 Gbit/s	250
FTDv30, 5 Gbit/s	8 cœurs/16 Go	5 Gbit/s	250
FTDv50, 10 Gbit/s	12 cœurs/24 Go	10 Gbit/s	750
FTDv100, 16 Gbit/s	16 cœurs/32 Go	16 Gbit/s	10 000

Consultez le chapitre sur les licences dans le Guide d'administration Cisco Secure Firewall Management Center pour connaître les consignes relatives à l'octroi de licences pour votre périphérique défense contre les menaces virtuelles.

Optimisation des performances

Pour obtenir les meilleures résutats avec défense contre les menaces virtuelles, vous pouvez apporter des ajustements à la machine virtuelle et à l'hôte. Pour plus d'informations, consultez Amélioration de la performance pour les configurations ESXi, à la page 37, Lignes directrices NUMA, à la page 37 et Provisionnement d'interface SR-IOV, à la page 38.

Receive Side Scaling (dimensionnement côté réception) : le défense contre les menaces virtuelles prend en charge Receive Côté Scaling (RSS), qui est une technologie utilisée par les adaptateurs réseau pour distribuer le trafic de réception réseau entre plusieurs cœurs de processeur. RSS est pris en charge par les versions 7.0 et ultérieures. Consultez la section sur les files d'attente RX multiples pour le dimensionnement de la réception (RSS) pour en savoir plus.

Mise en grappes

À partir de la version 7.2 : la mise en grappes est prise en charge sur les instances virtuelles de défense contre les menaces déployées sur VMware. Pour en savoir plus, consultez l'information sur la mise en grappes pour Threat Defense Virtual dans un nuage privé.

Mode gestion

- Vous avez deux options pour gérer votre appareil Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense) :
  - Le gestionnaire d'appareil intègre un gestionnaire intégré.

Remarque La défense contre les menaces virtuelles sur VMware prend en charge gestionnaire d'appareil de la version logicielle Cisco 6.2.2 (ou ultérieure). Tout défense contre les menaces virtuelles sur un logiciel VMware exécutant des logiciels antérieurs à la version 6.2.2 ne peut être géré qu'à l'aide du centre de gestion; voir Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual.

  - Section centre de gestion.

- Vous devez installer une nouvelle image (version 6.2.2 ou ultérieure) pour obtenir la prise en charge de gestionnaire d'appareil. Vous ne pouvez pas mettre à niveau une machine défense contre les menaces virtuelles existante à partir d'une version antérieure (à 6.2.2) puis passer à gestionnaire d'appareil.
- Gestionnaire d'appareil (gestionnaire local) est activé par défaut.

Remarque Lorsque vous choisissez **Yes** (oui) pour **Enable Local Manager** (activer le gestionnaire local), le mode de pare-feu passe à « routed » (avec routage). C'est le seul mode pris en charge lors de l'utilisation de gestionnaire d'appareil.

Lignes directrices relatives aux fichiers OVF

Les options suivantes s'offrent pour l'installation d'un appareil défense contre les menaces virtuelles :

```
Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf
```

où X.X.X-xxx est la version et le numéro de version du fichier d'archive que vous avez téléchargé.

- Si vous effectuez le déploiement avec un modèle VI OVF, le processus d'installation vous permet d'effectuer la configuration initiale complète de l'appareil défense contre les menaces virtuelles. Vous pouvez préciser :
  - Un nouveau mot de passe du compte administrateur.
  - Paramètres réseau qui permettent à l'appareil de communiquer sur votre réseau de gestion.
  - La gestion, soit la gestion locale à l'aide du gestionnaire d'appareil (par défaut), soit la gestion à distance à l'aide du centre de gestion.
  - Mode de pare-feu : lorsque vous choisissez Yes (oui) pour Enable Local Manager (activer le gestionnaire local), le mode de pare-feu passe à « routed » (avec routage). C'est le seul mode pris en charge lors de l'utilisation de gestionnaire d'appareil.

Remarque Vous devez gérer cette appliance virtuelle à l'aide de VMware vCenter.

- Si vous effectuez un déploiement à l'aide d'un modèle OVF ESXi, vous devez configurer les paramètres requis par le système après l'installation. Vous gérez défense contre les menaces virtuelles en tant qu'appareil autonome sur ESXi; consultez Déployer Défense contre les menaces virtuelles sur un hôte ESXi vSphere, à la page 32 pour de plus amples renseignements.

Impossible d'enregistrer la configuration de la machine virtuelle (VM) dans vSphere 7.0.2

Si vous utilisez vSphere 7.0.2, vous ne serez peut-être pas autorisé à enregistrer la configuration de la machine virtuelle.

Remarque Vous pouvez résoudre ce problème en suivant les instructions dans l'article de base de connaissances de VMware : https@kb.vmware.com/s/article/83898.

Prise en charge de vMotion

Nous vous recommandons d'utiliser le stockage partagé uniquement si vous prévoyez utiliser vMotion. Pendant le déploiement, si vous avez une grappe d'hôtes, vous pouvez provisionner le stockage localement (sur un hôte précis) ou sur un hôte partagé. Cependant, si vous essayez d'utiliser vMotion pour Cisco Secure Firewall Management Center Virtual (anciennement Firepower Management Center Virtual) vers un autre hôte, l'utilisation du stockage local produira une erreur.

Traitement simultané Hyperthreading non recommandé

La technologie Hyperthreading permet à un seul cœur de processeur physique de se comporter comme deux processeurs logiques. Nous vous recommandons de désactiver l'hyperthreading pour vos systèmes qui exécutent défense contre les menaces virtuelles. Le processus Snort optimise déjà les ressources de traitement dans un cœur de CPU. Lorsque vous tentez de pousser deux fils d'utilisation de CPU dans chaque processeur, vous n'obtenez aucune amélioration des performances. Vous pouvez en fait constater une diminution des performances en raison du surdébit requis pour le processus d'hyperthreading.

Symptôme des messages d'erreur de relecture INIT

Vous pouvez voir le message d'erreur suivant sur la console défense contre les menaces virtuelles s'exécutant sur ESXi 6 et ESXi 6.5 :

```
"INIT: Id "ftdv" respawning too fast: disabled for 5 minutes"
```

Solution de contournement : modifiez les paramètres de la machine virtuelle dans vSphere pour ajouter un port série lorsque le périphérique est hors tension.

1. Faites un clic droit sur la machine virtuelle et sélectionnez **Edit Settings** (modifier les paramètres).
2. Sous l'onglet Virtual Hardware (matériel virtuel), sélectionnez **Serial port** (port série) dans le menu déroulant **New device** (nouveau périphérique), puis cliquez sur **Add** (ajouter).

   Le port série apparaît au bas de la liste des périphériques virtuels.

3. Sous l'onglet **Virtual Hardware** (matériel virtuel), développez **Serial port** (port série) et sélectionnez le type de connexion **Use physical serial port** (port série physique).
4. Décochez la case **Connect at power on** (connecter à l'alimentation).

   Cliquez sur **OK** pour enregistrer les paramètres.

Exclure les machines virtuelles de la protection de pare-feu

Dans un environnement vSphere où le serveur vCenter est intégré à VMware NSX Manager, un pare-feu distribué (DFW) s'exécute dans le noyau en tant que paquet VIB sur toutes les grappes d'hôtes ESXi qui sont prêtes pour NSX. La préparation de l'hôte active automatiquement DFW sur les grappes d'hôte ESXi.

défense contre les menaces virtuelles fonctionne avec le mode de proximité, et les performances des machines virtuelles qui nécessitent ce mode peuvent être affectées de manière négative si ces machines virtuelles sont protégées par un pare-feu distribué. VMware vous recommande d'exclure de la protection par pare-feu distribuée les machines virtuelles qui nécessitent un mode de proximité.

1. Accédez aux paramètres de la liste d'exclusion.
   - Dans NSX 6.4.1 et les versions ultérieures, accédez à **Networking & Security (réseau et sécurité)** > **Security (sécurité)** > **Firewall Settings (paramètres de pare-feu)** > **Exclusion List (liste d'exclusion)**.
   - Dans NSX 6.4.0, accédez à **Networking & Security (réseau et sécurité)** > **Security (sécurité)** > **Firewall (pare-feu)** > **Exclusion List (liste d'exclusion)**.
2. Cliquez sur **Add** (ajouter).
3. Déplacez les machines virtuelles que vous souhaitez exclure vers **Selected Objects** (objets sélectionnés).
4. Cliquez sur **OK**.

Si une machine virtuelle a plusieurs cartes vNIC, toutes sont exclues de la protection. Si vous ajoutez des cartes vNIC à une machine virtuelle après qu'elle a été ajoutée à la liste d'exclusion, le pare-feu est automatiquement déployé sur les vNIC nouvellement ajoutées. Pour exclure les nouvelles vNIC de la protection par pare-feu, vous devez supprimer la machine virtuelle de la liste d'exclusion, puis l'ajouter de nouveau à la liste d'exclusion. Une autre solution de contournement consiste à exécuter un cycle d'alimentation (éteindre puis rallumer) la machine virtuelle, mais la première option est moins perturbatrice.

Modifier les paramètres de la politique de sécurité pour un commutateur standard vSphere

Pour un commutateur standard vSphere, les trois éléments de la politique de sécurité de couche 2 sont le mode de proximité, les changements d'adresses MAC et les transmissions falsifiées. Défense contre les menaces virtuelles utilise le mode de proximité pour fonctionner, et le bon fonctionnement de défense contre les menaces virtuellesla haute accessibilité virtuelle dépend du changement d'adresse MAC entre l'unité active et l'unité en veille.

Les paramètres par défaut bloqueront le bon fonctionnement de défense contre les menaces virtuelles. Consultez les paramètres requis suivants :

Tableau 4 : Options de politique de sécurité du commutateur standard vSphere

Option	Paramètre requis	Action
Mode de proximité	Accepter	Vous devez modifier la politique de sécurité d'un commutateur standard vSphere dans le client Web vSphere et définir l'option du mode de proximité (Promiscuous mode) sur Accept pour l'accepter. Les pare-feu, les analyses de ports, les systèmes de détection d'intrusion, etc. doivent fonctionner en mode de proximité.
Modifications d'adresses MAC :	Accepter	Vous devez vérifier la politique de sécurité d'un commutateur standard vSphere dans le client Web vSphere et confirmer que l'option de changements d'adresse MAC (MAC address changes) est réglée sur Accept pour l'accepter.
Transmissions forgées	Accepter	Vous devez vérifier la politique de sécurité d'un commutateur standard vSphere dans le client Web vSphere et confirmer que l'option de transmissions forgées (Forged transmits) est réglée sur Accept pour l'accepter.

Remarque Nous n'avons aucune recommandation pour la configuration des paramètres de politique de sécurité NSX-T pour un commutateur standard vSphere, car l'utilisation de VMware avec NSX-T n'a pas été mise à l'essai.

Snort

- Si vous observez un comportement anormal comme un délai d'arrêt du Snort long, un ralentissement de la machine virtuelle en général ou l'exécution d'un processus spécifique, collectez les journaux de défense contre les menaces virtuelles et de l'hôte VM. La collecte de l'utilisation globale du processeur, de la mémoire, de l'utilisation des E/S et de la vitesse de lecture/écriture vous aidera à résoudre les problèmes.
- Une utilisation élevée de la CPU et des E/S est observée lors de l'arrêt Snort. Si un certain nombre d'instances défense contre les menaces virtuelles ont été créées sur un seul hôte avec une mémoire insuffisante et aucun processeur dédié, Snort mettra beaucoup de temps à s'arrêter, ce qui entraînera la création de cœurs Snort.

Modifier les paramètres de la politique de sécurité pour un commutateur standard vSphere

Les paramètres par défaut bloqueront le bon fonctionnement de défense contre les menaces virtuelles.

Procédure

Étape 1 Dans le client Web vSphere, accédez à l'hôte.

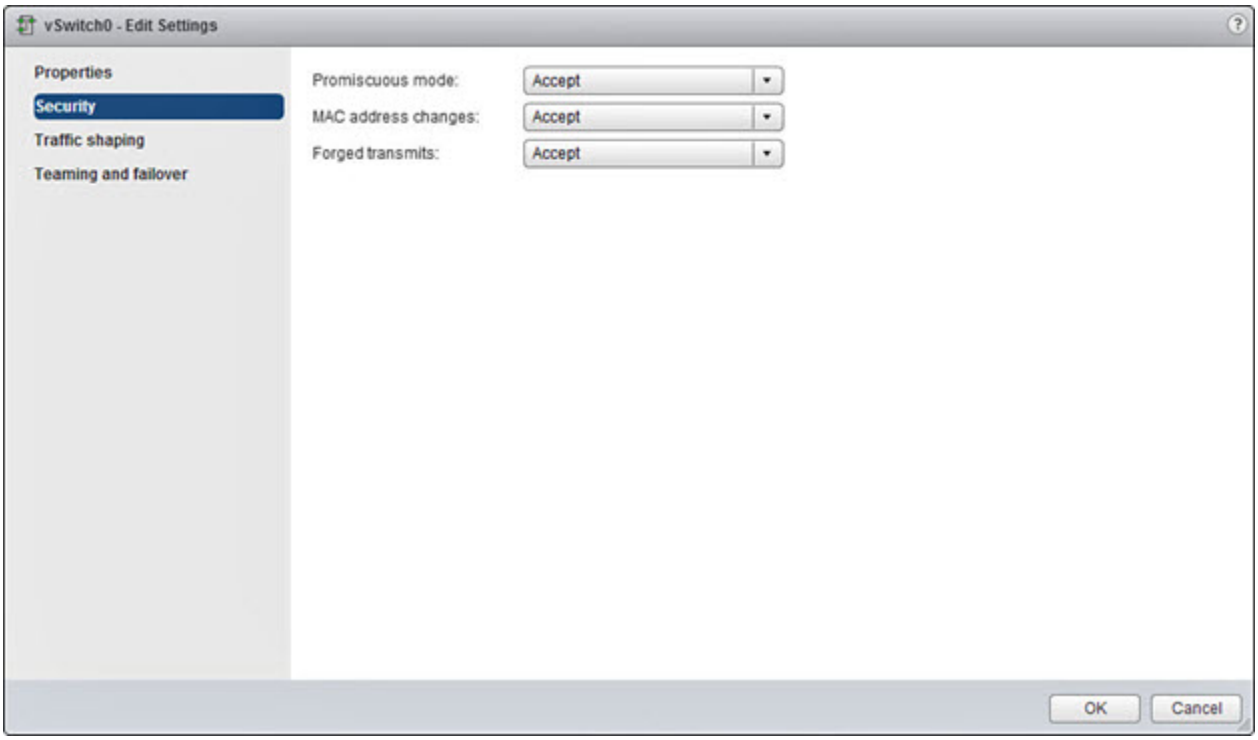
Étape 2 Dans l'onglet **Manage** (gérer), sélectionnez **Networking** (mise en réseau), puis **Virtual switches** (commutateurs virtuels).

Étape 3 Sélectionnez un commutateur standard dans la liste et cliquez sur **Edit settings** (modifier les paramètres).

Étape 4 Sélectionnez **Security** (sécurité) et affichez les paramètres actuels.

Étape 5 **Acceptez** l'activation en mode de proximité, les modifications d'adresses MAC et les transmissions forgées dans le système d'exploitation invité des machines virtuelles connectées au commutateur standard.

Illustration 1 : Paramètres de modification de vSwitch



Étape 6 Cliquez sur **OK**.

Prochaine étape

- Assurez-vous que ces paramètres sont les mêmes sur tous les réseaux configurés pour les interfaces de gestion et de basculement (HA) sur les périphériques défense contre les menaces virtuelles.

Planifier les interfaces

Vous pouvez éviter les redémarrages et les problèmes de configuration en planifiant le mappage de la vNIC et de l'interface défense contre les menaces virtuelles avant le déploiement. défense contre les menaces virtuelles est déployé avec dix interfaces et doit être activé au premier démarrage avec au moins quatre interfaces.

défense contre les menaces virtuelles prend en charge les adaptateurs de réseau virtuel vmxnet3 (par défaut), ixgbe et e1000. En outre, avec un système correctement configuré, défense contre les menaces virtuelles prend également en charge le pilote ixgbe-vf pour SR-IOV; consultez Configuration système requise, à la page 3 pour de plus amples renseignements.

Important Défense contre les menaces virtuelles sur VMware utilise maintenant les interfaces vmxnet3 par défaut lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Si vous utilisez des interfaces e1000, nous vous **recommandons fortement** de changer. Les pilotes de périphérique vmxnet3 et le traitement réseau sont intégrés à l'hyperviseur ESXi. Ils utilisent donc moins de ressources et offrent de meilleures performances réseau.

Lignes directrices et limites relatives aux interfaces

Les sections suivantes présentent les lignes directrices et les limites pour les adaptateurs de réseaux virtuels pris en charge qui sont utilisés avec défense contre les menaces virtuelles sur VMware. Il est important de garder ces lignes directrices à l'esprit lors de la planification de votre déploiement.

Lignes directrices générales

- Comme indiqué précédemment, défense contre les menaces virtuelles est déployé avec dix interfaces et doit être activé au premier démarrage avec au moins quatre interfaces. Vous devez attribuer un réseau à **AU MOINS QUATRE INTERFACES**.
- Nous vous recommandons d'éviter d'utiliser le groupe de ports de rétention (HOLDING) pour l'interface défense contre les menaces virtuelles. Le groupe de ports HOLDING de vSphere entraîne une connectivité d'interface incohérente. Un port de rétention fait partie d'un groupe de ports génériques qui est affecté à un ID VLAN. Cela peut entraîner des problèmes lors de la création d'une paire de haute accessibilité avec l'appareil défense contre les menaces virtuelles secondaire.
- Vous n'avez pas besoin d'utiliser les 10 interfaces défense contre les menaces virtuelles; pour les interfaces que vous n'avez pas l'intention d'utiliser, vous pouvez simplement laisser l'interface désactivée dans la configuration défense contre les menaces virtuelles.
- Gardez à l'esprit que vous ne pouvez pas ajouter d'autres interfaces virtuelles à la machine virtuelle après le déploiement. Si vous supprimez certaines interfaces, puis décidez que vous en voulez plus, vous devrez supprimer la machine virtuelle et recommencer.
- Dans la version 6.7 ou ultérieure : Vous pouvez éventuellement configurer une interface de données pour la gestion de centre de gestion au lieu de l'interface de gestion. L'interface de gestion est une condition préalable à la gestion de l'interface de données, vous devez donc toujours la configurer dans votre configuration initiale. Notez que l'accès centre de gestion à partir d'une interface de données n'est pas pris en charge dans les déploiements à haute accessibilité. Pour en savoir plus sur la configuration d'une

interface de données pour l'accès centre de gestion, consultez la commande **configure network management-data-interface** dans Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

- Avec deux cartes d'interface réseau virtuelles pour le groupe de ports ESX, qui est utilisé dans l'interface interne défense contre les menaces virtuelles ou dans le lien de basculement à haute accessibilité, l'ordre de basculement doit être configuré de manière à ce qu'une carte virtuelle agisse en tant que liaison ascendante active et l'autre, en tant que liaison ascendante de secours. C'est nécessaire pour que les deux machines virtuelles s'envoient des messages Ping ou que le lien virtuel à haute accessibilité (HA) de la défense contre les menaces soit actif.

Interfaces VMXNET3 par défaut

Important Défense contre les menaces virtuelles sur VMware utilise maintenant les interfaces vmxnet3 par défaut lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Si vous utilisez des interfaces e1000, nous vous **recommandons fortement** de changer. Les pilotes de périphérique vmxnet3 et le traitement réseau sont intégrés à l'hyperviseur ESXi. Ils utilisent donc moins de ressources et offrent de meilleures performances réseau.

- Le pilote vmxnet3 utilise deux interfaces de gestion. Les deux premiers adaptateurs Ethernet doivent être configurés en tant qu'interfaces de gestion; l'une destinée à la gestion et à l'enregistrement du périphérique, pour les diagnostics.
- Pour vmxnet3, Cisco recommande d'utiliser un hôte géré par VMware vCenter lorsque vous utilisez plus de quatre interfaces réseau vmxnet3. Lorsqu'elles sont déployées sur un ESXi autonome, les interfaces réseau supplémentaires ne sont pas ajoutées à la machine virtuelle avec des adresses bus d'interconnexion des composants périphériques (PCI) séquentielles. Lorsque l'hôte est géré avec un VMware vCenter, le bon ordre peut être obtenu à partir du fichier XML dans le CD-ROM de configuration. Lorsque l'hôte exécute un ESXi autonome, le seul moyen de déterminer l'ordre des interfaces réseau est de comparer manuellement les adresses MAC sur le défense contre les menaces virtuelles aux adresses MAC vues à partir de l'outil de configuration VMware.

La tableau suivant décrit la concordance de l'adaptateur réseau, des réseaux sources et des réseaux de destination pour défense contre les menaces virtuelles pour les interfaces vmxnet3 et ixgbe.

Tableau 5 : Mappage du réseau source au réseau de destination : VMXNET3 et IXGBE

Adaptateur réseau	Réseaux sources	Réseaux de destination	Fonction
Adaptateur réseau 1	Gestion 0-0	Gestion 0/0	Gestion
Adaptateur réseau 2	Diagnostic 0-0	Diagnostic 0/0	Diagnostic
Adaptateur réseau 3	GigabitEthernet 0-0	GigabitEthernet 0/0	Données externes
Adaptateur réseau 4	GigabitEthernet 0-1	GigabitEthernet 0/1	Données internes
Adaptateur réseau 5	GigabitEthernet 0-2	GigabitEthernet 0/2	Trafic de données (facultatif)

Adaptateur réseau	Réseaux sources	Réseaux de destination	Fonction
Adaptateur réseau 6	GigabitEthernet 0-3	GigabitEthernet 0/3	Trafic de données (facultatif)
Adaptateur réseau 7	GigabitEthernet 0-4	GigabitEthernet 0/4	Trafic de données (facultatif)
Adaptateur réseau 8	GigabitEthernet 0-5	GigabitEthernet 0/5	Trafic de données (facultatif)
Adaptateur réseau 9	GigabitEthernet 0-6	GigabitEthernet 0/6	Trafic de données (facultatif)
Adaptateur réseau 10	GigabitEthernet 0-7	GigabitEthernet 0/7	Trafic de données (facultatif)

Interfaces IXGBE

- Le pilote ixgbe utilise deux interfaces de gestion. Les deux premiers appareils d'interconnexion des composants périphériques (PCI) doivent être configurés en tant qu'interfaces de gestion; l'une destinée à la gestion et à l'enregistrement du périphérique, l'autre ,pour les diagnostics.
- Pour ixgbe, la plateforme ESXi nécessite que la carte d'interface réseau ixgbe prenne en charge le périphérique PCI ixgbe. En outre, la plateforme ESXi a des exigences spécifiques de BIOS et de configuration qui sont nécessaires pour prendre en charge les périphériques PCI ixgbe. Consultez la section sur la technologie Intel pour obtenir plus de renseignements.
- Les seuls types d'interfaces de trafic ixgbe pris en charge sont l'interface de routage et l'interface ERSPAN passive. C'est ainsi en raison des limites de VMware en ce qui concerne le filtrage des adresses MAC.
- Le pilote ixgbe ne prend pas en charge les déploiements de basculement (HA) de défense contre les menaces virtuelles.

Interfaces E1000

Important Défense contre les menaces virtuelles sur VMware utilise maintenant les interfaces vmxnet3 par défaut lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Si vous utilisez des interfaces e1000, nous vous **recommandons fortement** de changer. Les pilotes de périphérique vmxnet3 et le traitement réseau sont intégrés à l'hyperviseur ESXi. Ils utilisent donc moins de ressources et offrent de meilleures performances réseau.

- L'interface de gestion (br1) du pilote e1000 est une interface en pont avec deux adresses MAC, l'une pour la gestion et l'autre pour les diagnostics.
- Si vous mettez à niveau votre défense contre les menaces virtuelles vers la version 6.4 et utilisez des interfaces e1000, vous devez remplacer les interfaces e1000 par des interfaces vmxnet3 ou ixgbe pour un plus grand débit réseau.

La tableau suivant décrit la concordance de l'adaptateur réseau, des réseaux sources et des réseaux de destination pour défense contre les menaces virtuelles pour les interfaces e1000 par défaut.

Tableau 6 : Mappage du réseau source au réseau de destination : interfaces E1000

Adaptateur réseau	Réseaux sources	Réseaux de destination	Fonction
Adaptateur réseau 1	Gestion 0-0	Diagnostic 0/0	Gestion et diagnostic
Adaptateur réseau 2	GigabitEthernet 0-0	GigabitEthernet 0/0	Données externes
Adaptateur réseau 3	GigabitEthernet 0-1	GigabitEthernet 0/1	Données internes
Adaptateur réseau 4	GigabitEthernet 0-2	GigabitEthernet 0/2	Trafic de données (obligatoire)
Adaptateur réseau 5	GigabitEthernet 0-3	GigabitEthernet 0/3	Trafic de données (facultatif)
Adaptateur réseau 6	GigabitEthernet 0-4	GigabitEthernet 0/4	Trafic de données (facultatif)
Adaptateur réseau 7	GigabitEthernet 0-5	GigabitEthernet 0/5	Trafic de données (facultatif)
Adaptateur réseau 8	GigabitEthernet 0-6	GigabitEthernet 0/6	Trafic de données (facultatif)
Adaptateur réseau 9	GigabitEthernet 0-7	GigabitEthernet 0/7	Trafic de données (facultatif)
Adaptateur réseau 10	GigabitEthernet 0-8	GigabitEthernet 0/8	Trafic de données (facultatif)

Configurez les interfaces VMXNET3

Important À partir de la version 6.4, défense contre les menaces virtuelles et centre de gestion virtuel sur VMware utilisent les interfaces vmxnet3 lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Si vous utilisez des interfaces e1000, nous vous **recommandons fortement** de changer. Les pilotes de périphérique vmxnet3 et le traitement réseau sont intégrés à l'hyperviseur ESXi. Ils utilisent donc moins de ressources et offrent de meilleures performances réseau.

Pour remplacer les interfaces e1000 par vmxnet3, vous devez supprimer TOUTES les interfaces et les réinstaller avec le pilote vmxnet3.

Bien que vous puissiez combiner des interfaces dans votre déploiement (p. ex. en déployant les interfaces e1000 sur centre de gestion et les interfaces vmxnet3 sur son périphérique virtuel géré), vous ne pouvez pas mélanger des types d'interfaces sur la même appliance virtuelle. Toutes les interfaces de détection et de gestion de l'appliance virtuelle doivent être du même type.

Procédure

Étape 1 Mettez hors tension défense contre les menaces virtuelles ou la machine centre de gestion virtuel.

Pour modifier les interfaces, vous devez éteindre l'appareil.

Étape 2 Faites un clic droit sur défense contre les menaces virtuelles ou la machine centre de gestion virtuel dans l'inventaire et sélectionnez **Edit Settings** (modifier les paramètres).

Étape 3 Sélectionnez les adaptateurs de réseau applicables, puis sélectionnez **Remove** (supprimer).

Étape 4 Cliquez sur **Add** (ajouter) pour ouvrir **Add Hardware Wizard** (assistant d'ajout de matériel).

Étape 5 Sélectionnez **Ethernet adapter** (adaptateur Ethernet) et cliquez sur **Next** (suivant).

Étape 6 Sélectionnez l'adaptateur vmxnet3, puis choisissez l'étiquette du réseau.

Étape 7 Répétez l'opération pour toutes les interfaces sur défense contre les menaces virtuelles.

Prochaine étape

- Démarrez défense contre les menaces virtuelles ou centre de gestion virtuel à partir de la console VMware.

Ajout d'interfaces

Vous pouvez avoir un total de 10 interfaces (une gestion, une interne, huit interfaces de données) lorsque vous déployez un périphérique défense contre les menaces virtuelles. Pour les interfaces de données, assurez-vous que les réseaux sources (**Source Networks**) correspondent aux réseaux de destination (**Destination Networks**) appropriés et que chaque interface de données est mappée à un sous-réseau ou à un VLAN unique.

Mise en garde Vous ne pouvez pas ajouter d'autres interfaces virtuelles à la machine virtuelle et faire en sorte que défense contre les menaces virtuelles les reconnaisse automatiquement. L'ajout d'interfaces à une machine virtuelle nécessite d'effacer complètement la configuration de défense contre les menaces virtuelles. La seule partie de la configuration qui reste intacte est l'adresse de gestion et les paramètres de la passerelle.

Si vous avez besoin de plus d'équivalents d'interface physique pour le périphérique défense contre les menaces virtuelles, vous devez fondamentalement recommencer. Vous pouvez soit déployer une nouvelle machine virtuelle, soit utiliser la procédure de recherche de modifications d'interface et de migration d'une interface dans Guide Cisco Secure Firewall Device Manager Configuration.

À propos du déploiement de VMware

Vous pouvez déployer défense contre les menaces virtuelles sur un serveur ESXi autonome ou, si vous avez vSphere vCenter, vous pouvez procéder au déploiement à l'aide du client vSphere ou du client Web vSphere. Pour déployer avec succès le défense contre les menaces virtuelles, vous devez connaître VMware et vSphere, y compris le réseau vSphere, la configuration et le paramétrage de l'hôte ESXi, ainsi que le déploiement des invités de machine virtuelle.

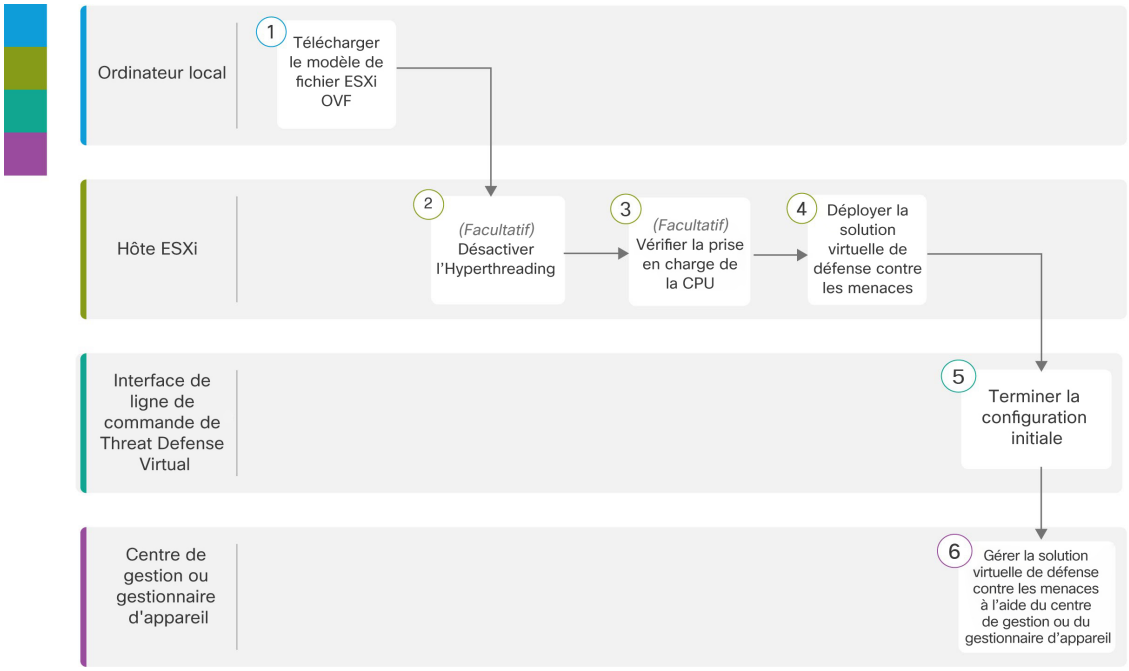
Défense contre les menaces virtuelles pour VMware est distribué à l'aide du format Open Virtualization Format (OVF), qui est une méthode standard d'emballage et de déploiement des machines virtuelles. VMware fournit plusieurs méthodes pour provisionner les machines virtuelles vSphere. La méthode optimale pour votre environnement dépend de facteurs tels que la taille et le type de votre infrastructure et les objectifs que vous souhaitez atteindre.

Le client Web VMware vSphere et le client vSphere sont des interfaces pour le serveur vCenter, les hôtes ESXi et les machines virtuelles. Avec le client Web vSphere et le client vSphere, vous pouvez vous connecter à distance au serveur vCenter. Avec le client vSphere, vous pouvez également vous connecter directement à ESXi à partir de n'importe quel système Windows. Le client Web vSphere et le client vSphere sont les principales interfaces pour la gestion de tous les aspects de l'environnement vSphere. Ils fournissent également un accès de console aux machines virtuelles.

Toutes les fonctions administratives sont accessibles par l'intermédiaire de client Web vSphere. Un sous-ensemble de ces fonctions est disponible par l'entremise de client vSphere.

Procédure de bout en bout

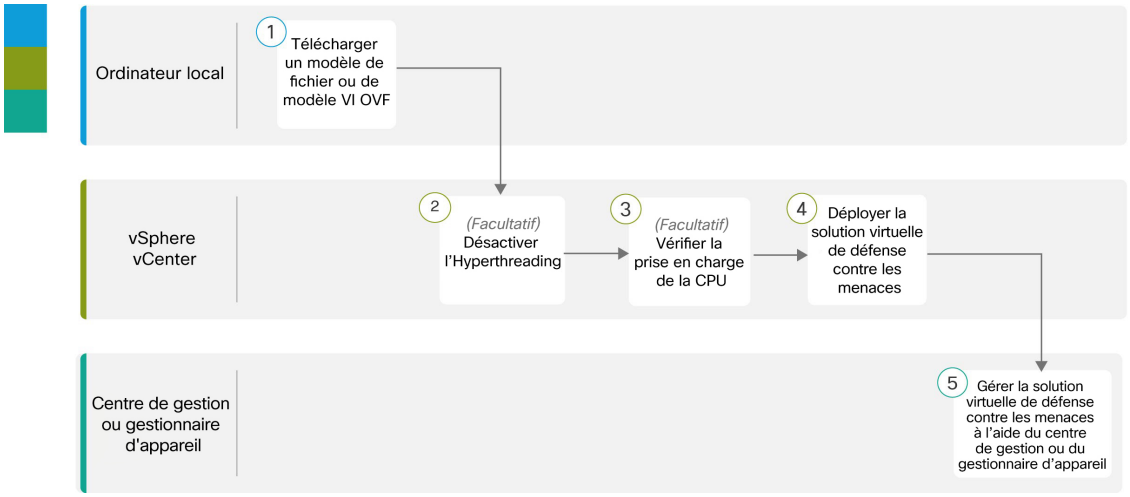
Le diagramme suivant illustre le flux de travail pour le déploiement de défense contre les menaces virtuelles sur l'hôte ESXi.



	Espace de travail	Étapes
1	Ordinateur local	Télécharger le modèle OVF ESXi : Téléchargez le progiciel Open Virtualization Format (OVF) disponible sur Cisco.com.
2	Hôte ESXi	(Facultatif) Désactiver l'hyperthreading : désactivez l'hyperthreading pour vos systèmes qui exécutent le défense contre les menaces virtuelles.

	Espace de travail	Étapes
3	Hôte ESXi	(Facutatif) Verify CPU Support (vérifier le soutien CPU) : Vous pouvez utiliser la ligne de commande Linux pour obtenir des informations sur le matériel de la CPU.
4	Hôte ESXi	Déployer Threat Defense Virtual : Déployez l'appareil défense contre les menaces virtuelles sur un seul hôte ESXi.
5	CLI Défense contre les menaces virtuelles	Terminer la configuration initiale : Si vous avez déployé un modèle OVF ESXi, vous devez configurer défense contre les menaces virtuelles à l'aide de la CLI.
6	Centre de gestion ou Gestionnaire d'appareil	Gérer défense contre les menaces virtuelles : • Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Management Center • Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Device Manager

Le diagramme suivant illustre le flux de travail pour le déploiement de défense contre les menaces virtuelles sur vSphere vCenter.



	Espace de travail	Étapes
1	Ordinateur local	Télécharger le modèle OVF VI : Téléchargez le progiciel Open Virtualization Format (OVF) disponible sur Cisco.com.
2	vSphere vCenter	(Facultatif) Désactiver l'hyperthreading : désactivez l'hyperthreading pour vos systèmes qui exécutent le défense contre les menaces virtuelles.
3	vSphere vCenter	(Facutatif) Verify CPU Support (vérifier le soutien CPU) : Vous pouvez utiliser la ligne de commande Linux pour obtenir des informations sur le matériel de la CPU.

	Espace de travail	Étapes
4	vSphere vCenter	Déployer Threat Defense Virtual : Déployez l'appareil défense contre les menaces virtuelles sur un seul hôte ESXi.
5	Centre de gestion ou Gestionnaire d'appareil	Gérer défense contre les menaces virtuelles : • Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Management Center • Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Device Manager

Déployer Défense contre les menaces virtuelles dans vSphere vCenter

Utilisez cette procédure pour déployer l'appareil défense contre les menaces virtuelles sur VMware vSphere vCenter. Vous pouvez utiliser le client web VMware (ou le client vSphere) pour déployer et configurer les machines défense contre les menaces virtuelles.

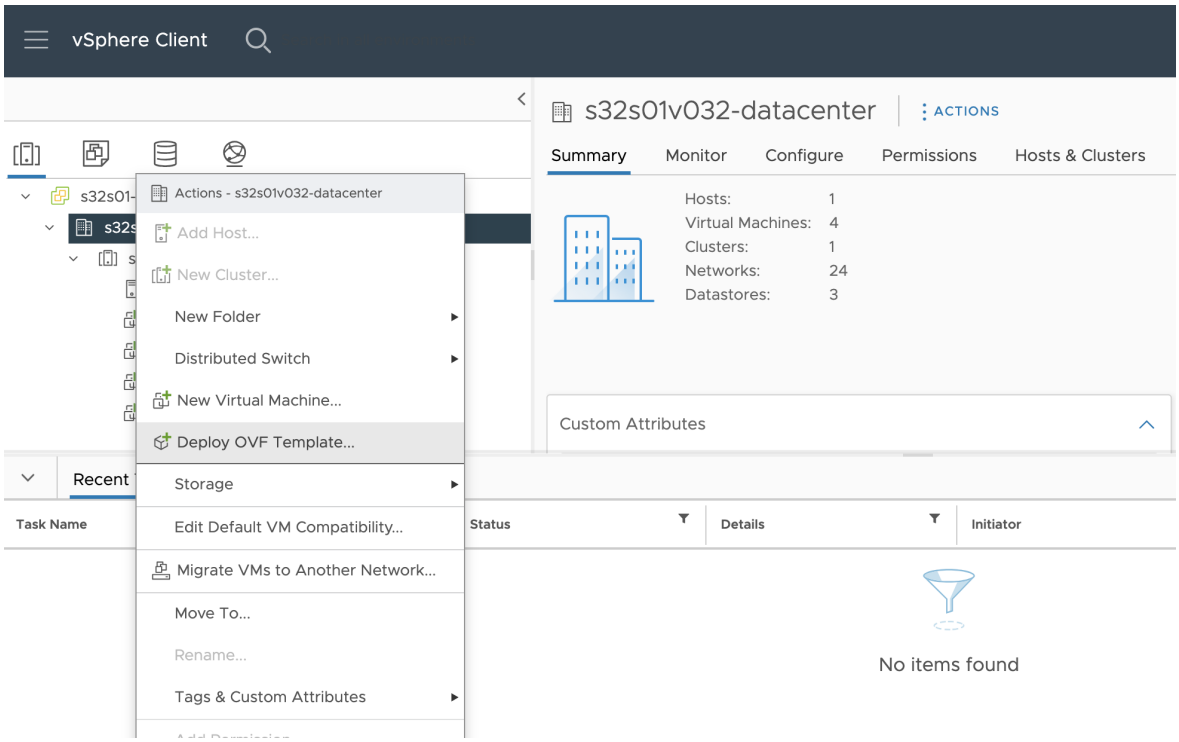
Avant de commencer

- Vous devez avoir au moins un réseau configuré dans vSphere (pour la gestion) avant de déployer le défense contre les menaces virtuelles.

Procédure

Étape 1 Connectez-vous au client Web vSphere (ou au client vSphere).

Étape 2 À l'aide du client Web vSphere (ou du client vSpherde), déployez le fichier de modèle OVF que vous avez téléchargé précédemment en cliquant sur **File (fichier)** > **Deploy OVF Template (déployer le modèle OVF)**.



L'assistant de déploiement du modèle OVF s'affiche.

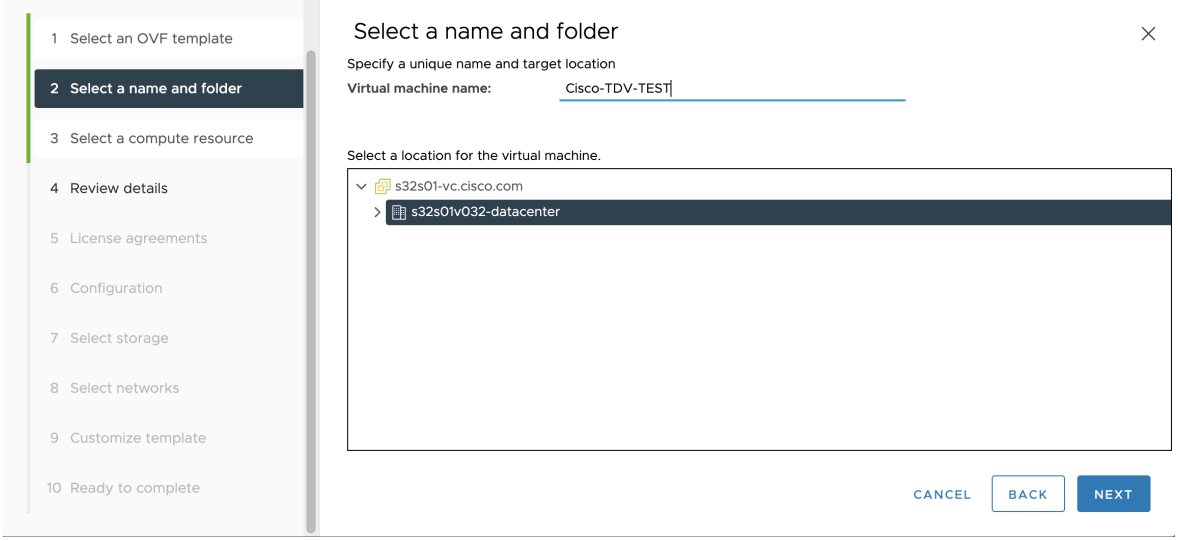
Étape 3 Parcourez votre système de fichiers à la recherche de l'emplacement de la source du modèle OVF, puis cliquez sur **Next** (suivant).

Sélectionnez le modèle VI OVF défense contre les menaces virtuelles :

Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf

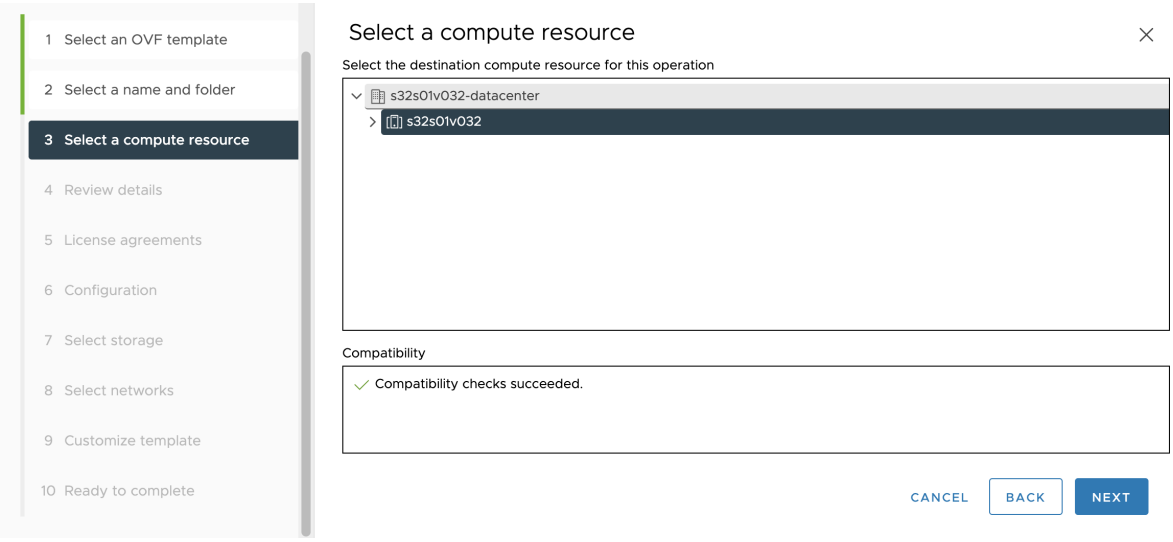
où *X.X.X-xxx* est la version et le numéro de version du fichier d'archive que vous avez téléchargé.

Étape 4 Dans la page **Name and Location** (nom et emplacement), saisissez un nom pour ce déploiement et sélectionnez l'emplacement dans l'inventaire (hôte ou grappe) sur lequel vous souhaitez déployer défense contre les menaces virtuelles, puis cliquez sur **Next** (suivant). Le nom doit être unique dans le dossier d'inventaire et peut contenir jusqu'à 80 caractères.



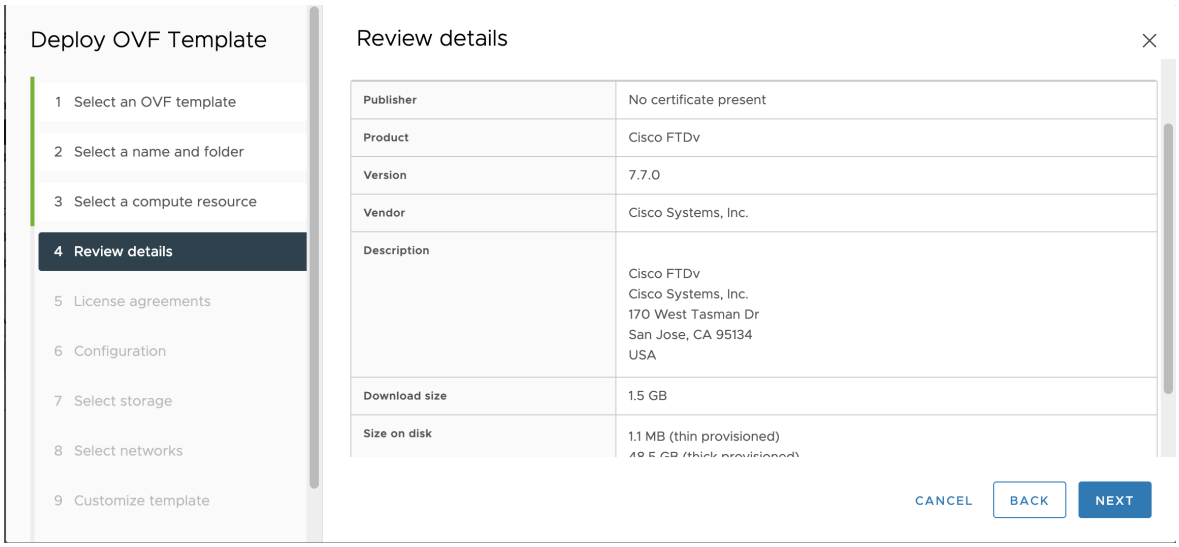
Le client Web vSphere présente la hiérarchie organisationnelle des objets gérés dans des vues d'inventaire. Les inventaires sont la structure hiérarchique utilisée par le serveur vCenter ou l'hôte pour organiser les objets gérés. Cette hiérarchie inclut tous les objets surveillés dans le serveur vCenter.

Étape 5 Accédez à et sélectionnez l'ensemble de ressources dans lequel vous souhaitez exécuter défense contre les menaces virtuelles, puis cliquez sur **Next** (suivant).



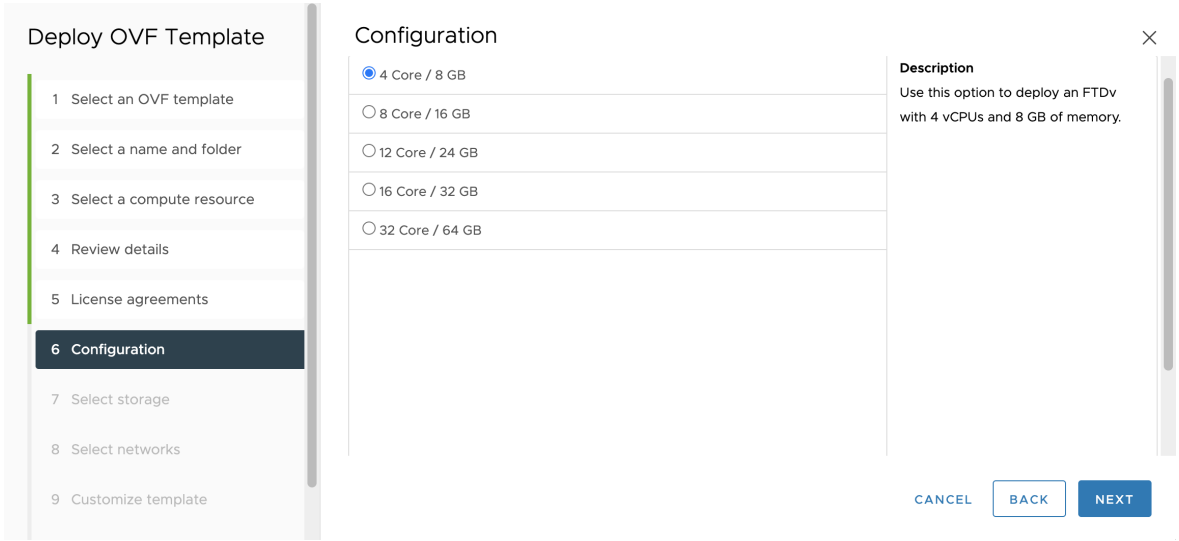
Remarque
Cette page s'affiche uniquement si la grappe contient un ensemble de ressources.

Étape 6 Passez en revue la page **OVF Template Details** (détails du modèle OVF) et vérifiez les renseignements sur le modèle OVF (nom du produit, version, prestataire, taille de téléchargement, taille sur le disque et description), puis cliquez sur **Next** (suivant).



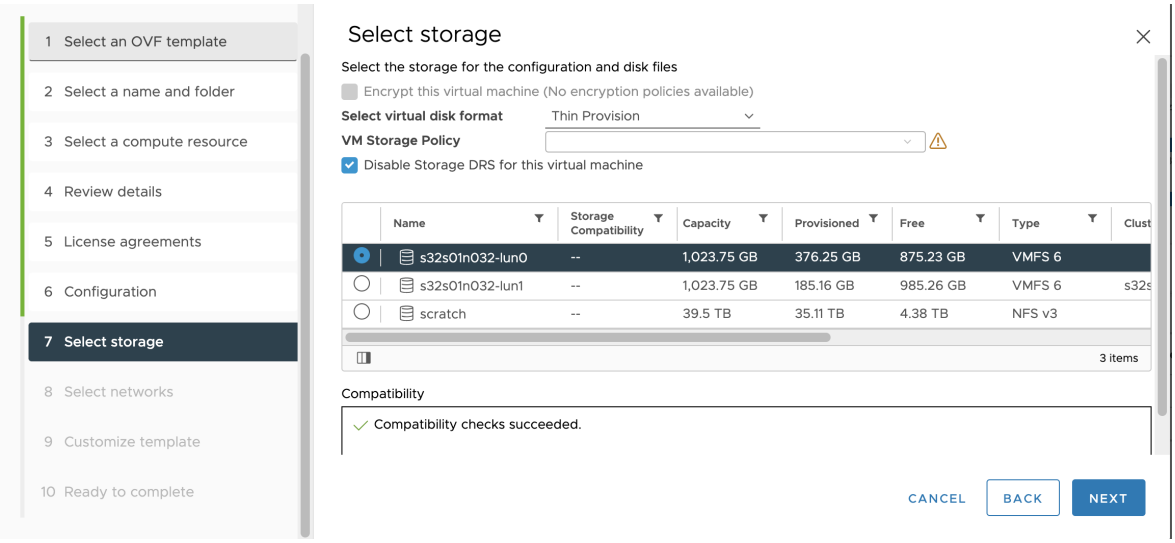
Étape 7 La page **End User License Agreement** (contrat de licence de l'utilisateur final) s'affiche. Passez en revue le contrat de licence groupé avec le modèle OVF (modèles VI uniquement), cliquez sur **Accept** (accepter) pour accepter les conditions des licences et cliquez sur **Next** (suivant).

Étape 8 Dans la page de **Configuration**, choisissez l'une des valeurs de v: CPU/mémoire prises en charge dans les options de **Configuration**, puis cliquez sur **Next** (suivant).



Important
Premiers pas avec la version 6.4 : défense contre les menaces virtuelles se déploie avec des ressources de vCPU et de mémoire ajustables. Avant la version 6.4, défense contre les menaces virtuelles était déployé en tant que périphérique à configuration fixe 4vCPU/8Go; voir Configuration système requise, à la page 3.

Étape 9 Sélectionnez un emplacement de **Storage** (stockage) pour stocker les fichiers de la machine virtuelle.

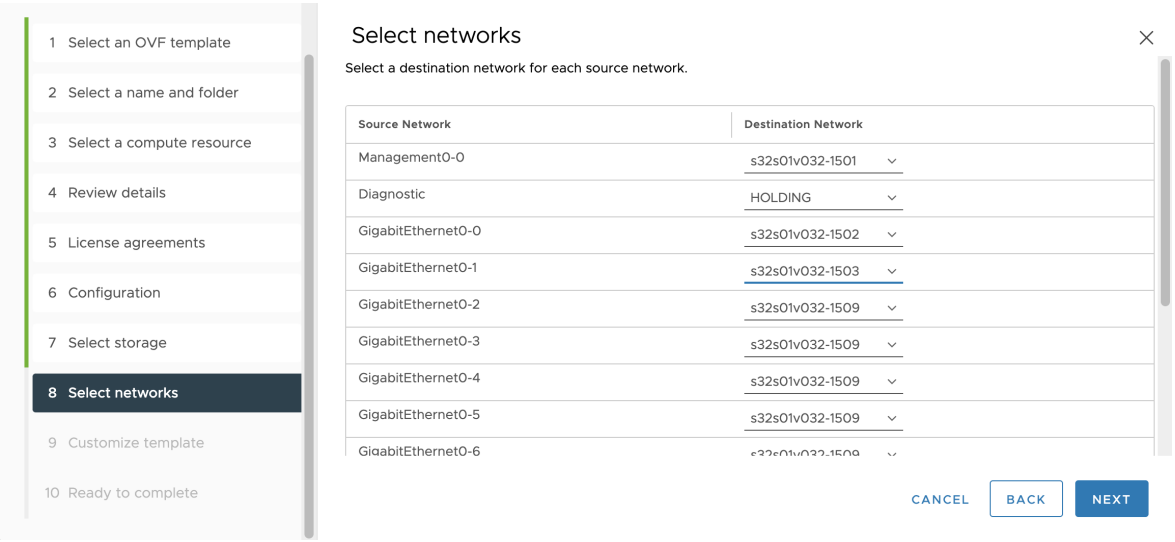


Dans cette page, sélectionnez parmi les banques de données déjà configurées sur la grappe ou l'hôte de destination. Le fichier de configuration de la machine virtuelle et les fichiers de disque virtuel sont stockés dans la banque de données. Sélectionnez une banque de données de taille suffisante pour contenir la machine virtuelle et tous ses fichiers de disque virtuel.

Étape 10 Dans la liste déroulante **Select virtual disk format** (sélectionner le format de disque virtuel), choisissez le **disk format** (format de disque) pour stocker les disques virtuels de la machine virtuelle, puis cliquez sur **Next** (suivant).

Lorsque vous sélectionnez **Thick provisioned** (grand provisionnement), tout le stockage est immédiatement alloué. Lorsque vous sélectionnez **Thin provisioned** (provisionnement léger), le stockage est attribué à la demande, au fur et à mesure que les données sont écrites sur les disques virtuels. Le provisionnement léger peut également réduire le temps nécessaire pour déployer l'appliance virtuelle.

Étape 11 Dans la page **Select networks** (sélectionnez des réseaux), mappez les réseaux précisés dans le modèle OVF aux réseaux de votre inventaire, puis sélectionnez **Next**(suivant).



Assurez-vous que l'interface de gestion 0-0 est ass ociée à un réseau de machine virtuelle accessible à partir d'Internet. Les interfaces qui ne sont pas des interfaces de gestion sont configurables à partir du centre de gestion ou du gestionnaire d'appareil, selon votre mode de gestion.

Important
Défense contre les menaces virtuelles sur VMware utilise maintenant les interfaces vmxnet3 par défaut lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Si vous utilisez des interfaces e1000, nous vous **recommandons fortement** de changer. Les pilotes de périphérique vmxnet3 et le traitement réseau sont intégrés à l'hyperviseur ESXi. Ils utilisent donc moins de ressources et offrent de meilleures performances réseau.

Les réseaux ne peuvent pas être en ordre alphabétique. S'il est trop difficile de trouver vos réseaux, vous pouvez modifier les réseaux plus tard à partir de la boîte de dialogue de modification des paramètres (**Edit Settings**). Après le déploiement, cliquez avec le bouton droit sur l'instance défense contre les menaces virtuelles et choisissez **Edit Settings** (modifier les paramètres). Cependant, cet écran n'affiche pas les ID défense contre les menaces virtuelles (uniquement les ID d'adaptateur réseau).

Consultez la concordance suivante concernant l'adaptateur réseau, les réseaux sources et les réseaux de destination pour les interfaces défense contre les menaces virtuelles (il s'agit des interfaces vmxnet3 par défaut) :

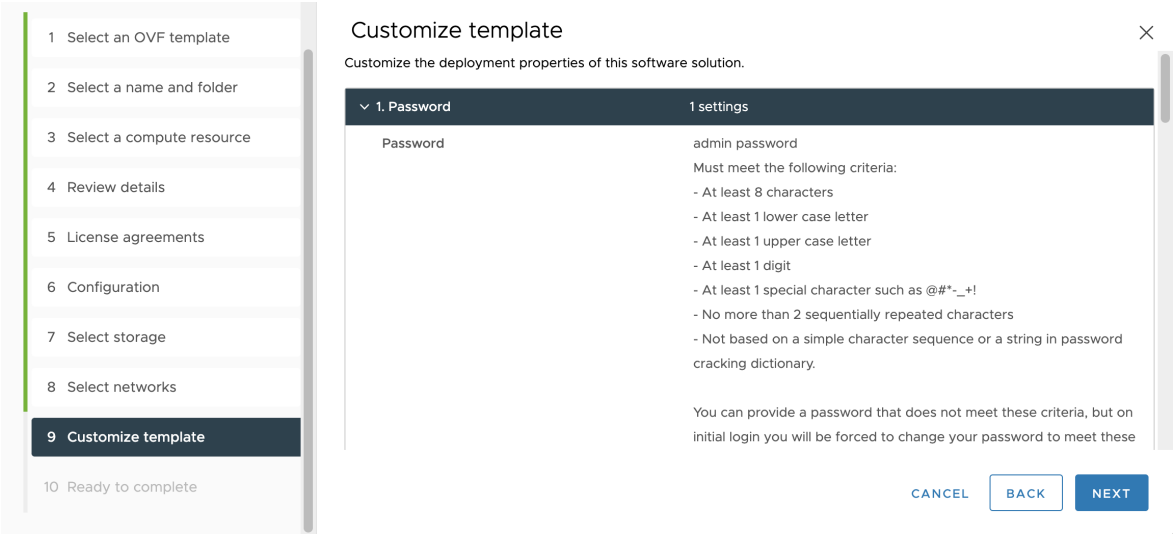
Tableau 7 : Mappage du réseau source au réseau de destination : VMXNET3

Adaptateur réseau	Réseaux sources	Réseaux de destination	Fonction
Adaptateur réseau 1	Gestion 0-0	Gestion 0/0	Gestion
Adaptateur réseau 2	Diagnostic 0-0	Diagnostic 0/0	Diagnostic
Adaptateur réseau 3	GigabitEthernet 0-0	GigabitEthernet 0/0	Données externes
Adaptateur réseau 4	GigabitEthernet 0-1	GigabitEthernet 0/1	Données internes
Adaptateur réseau 5	GigabitEthernet 0-2	GigabitEthernet 0/2	Trafic de données (facultatif)
Adaptateur réseau 6	GigabitEthernet 0-3	GigabitEthernet 0/3	Trafic de données (facultatif)
Adaptateur réseau 7	GigabitEthernet 0-4	GigabitEthernet 0/4	Trafic de données (facultatif)
Adaptateur réseau 8	GigabitEthernet 0-5	GigabitEthernet 0/5	Trafic de données (facultatif)
Adaptateur réseau 9	GigabitEthernet 0-6	GigabitEthernet 0/6	Trafic de données (facultatif)
Adaptateur réseau 10	GigabitEthernet 0-7	GigabitEthernet 0/7	Trafic de données (facultatif)

Vous pouvez avoir un total de 10 interfaces lorsque vous déployez le défense contre les menaces virtuelles. Pour les interfaces de données, assurez-vous que les réseaux sources correspondent aux réseaux de destination appropriés et que chaque interface de données est mappée à un sous-réseau ou à un VLAN unique. Vous n'avez pas besoin d'utiliser toutes les interfaces défense contre les menaces virtuelles; pour les interfaces que vous n'avez pas l'intention d'utiliser, vous pouvez simplement laisser l'interface désactivée dans la configuration défense contre les menaces virtuelles.

Étape 12 Dans la page de propriétés de la personnalisation des modèles (**Customize templates** properties), définissez les propriétés configurables par l'utilisateur groupées avec le modèle OVF (modèles VI uniquement) :

a) **Mot de passe**

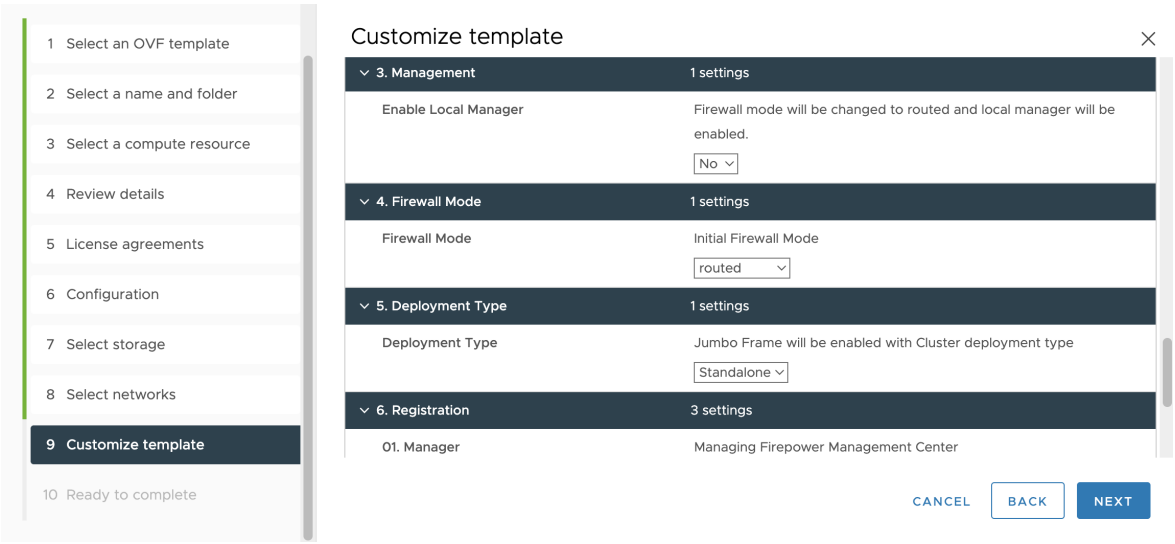


Définissez le mot de passe pour l'accès admin défense contre les menaces virtuelles.

b) **Réseau**

Définissez les renseignements sur le réseau, notamment le nom de domaine complet (FQDN), le DNS, le domaine de recherche et le protocole de réseau (IPv4).

c) **Gestion**



Définissez le mode gestion. Cliquez sur la flèche de la liste déroulante pour **Enable Local Manager** (activer le gestionnaire local) et sélectionnez **Yes** (oui) pour utiliser l'outil de configuration Web intégré gestionnaire d'appareil. Sélectionnez **No** (non) pour utiliser centre de gestion pour gérer cet appareil. Consultez Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual pour savoir comment choisir votre option de gestion.

d) **Mode pare-feu**

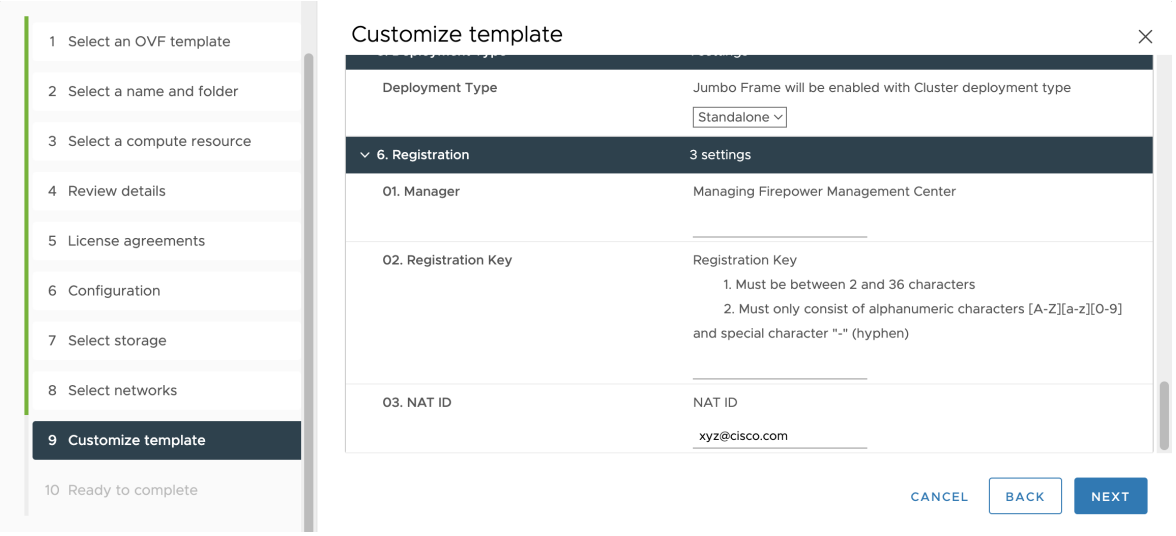
Définissez le mode pare-feu initial. Cliquez sur la flèche de la liste déroulante **Firewall Mode** (mode pare-feu) et choisissez l'un des deux modes pris en charge, **Routed** (routage) ou **Transparent**.

Si vous avez choisi **Yes** (oui) pour **Enable Local Manager** (activer le gestionnaire local), vous ne pouvez sélectionner que le mode de pare-feu avec routage (**Routed**). Vous ne pouvez pas configurer des interfaces en mode pare-feu transparent à l'aide du gestionnaire d'appareil local.

e) **Type de déploiement**

Définissez le type de déploiement **Standalone** (autonome) ou **Cluster** (en grappe). Choisissez **Cluster**(grappe) pour activer la réservation de trame étendue, qui est requise pour la liaison de commande de grappe. Choisissez **Standalone** pour un déploiement autonome ou haute accessibilité. Notez que si vous déployez en tant que périphérique autonome, vous pouvez toujours l'utiliser dans une grappe; cependant, l'activation des trames étendues pour la mise en grappe après le déploiement signifie que vous devrez redémarrer.

f) **Renseignements**

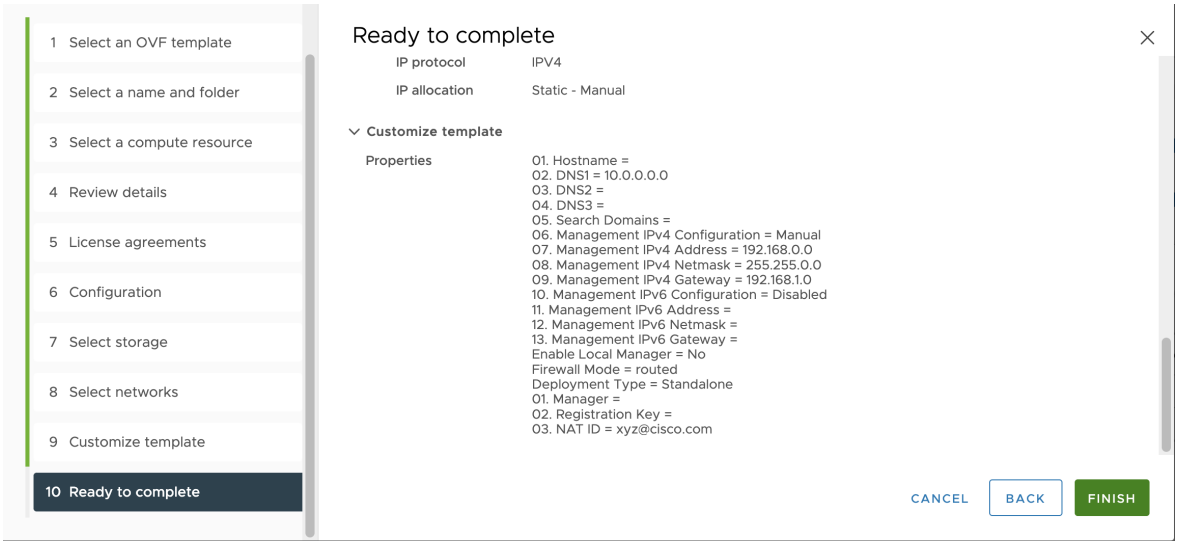


Si vous avez choisi **No** (non) pour **Enable Local Manager** (activer le gestionnaire local), vous devez fournir les informations d'authentification requises pour enregistrer ce périphérique sur le centre de gestion Secure Firewall Management Center. Précisez les éléments suivants :

- **Managing Defense Center** (gestion du centre de défense) : saisissez le nom d'hôte ou l'adresse IP de centre de gestion.
- **Registration Key** (clé d'enregistrement) : la clé d'enregistrement est une clé à usage unique générée par l'utilisateur qui ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-). Vous devez vous souvenir de cette clé d'enregistrement lorsque vous ajoutez le périphérique à centre de gestion.
- **NAT ID** (ID de NAT) : si défense contre les menaces virtuelles et centre de gestion sont séparés par un périphérique de traduction d'adresses réseau (NAT), et que centre de gestion se trouve derrière un périphérique NAT, saisissez un Identifiant NAT unique. Il s'agit d'une clé à usage unique générée par l'utilisateur qui ne doit pas dépasser 37 caractères. Les caractères valides comprennent les caractères alphanumériques (A à Z, a à z, 0 à 9) et le tiret (-).

g) Cliquez sur **Next** (suivant).

Étape 13 Dans la page **Ready to complete** (prêt à terminer), passez en revue et vérifiez les renseignements affichés. Pour commencer le déploiement avec ces paramètres, cliquez sur **Finish** (terminer). Pour apporter des modifications, cliquez sur **Back** (retour) pour accéder aux écrans précédents.



Facultativement, cochez l'option **Power on after deployment** (mise sous tension après le déploiement) pour démarrer défense contre les menaces virtuelles, puis cliquez sur **Finish** (terminer).

Après avoir terminé la démarche guidée par l'assistant, le client Web vSphere gère la machine virtuelle; vous pouvez voir l'état « Initalize OVF Deployment » (initier le déploiement OVF) dans le volet des tâches récentes (**Recent Tasks**) de la zone d'information globale (**Global Information**).

Lorsqu'il a terminé, vous voyez l'état d'achèvement du déploiement du modèle OVF.

L'instance défense contre les menaces virtuelles apparaît dans le centre de données spécifié dans l'inventaire. Le démarrage de la nouvelle machine virtuelle peut prendre jusqu'à 30 minutes.

Remarque
Pour enregistrer avec succès défense contre les menaces virtuelles auprès de l'autorité de licence de Cisco, défense contre les menaces virtuelles nécessite un accès Internet. Vous devrez peut-être effectuer une configuration supplémentaire après le déploiement pour obtenir un accès Internet et un enregistrement de licence réussi.

Prochaine étape

Vos prochaines étapes dépendent du mode de gestion que vous avez choisi.

- Si vous avez sélectionné **No** (non) pour **Enable Local Manager** (activer le gestionnaire local), vous utiliserez centre de gestion pour gérer défense contre les menaces virtuelles; à ce sujet, consultez Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Management Center.

Consultez Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual pour savoir comment choisir votre option de gestion.

Préparer le fichier de configuration Day 0 (Jour 0) pour le déploiement de la grappe

Vous pouvez préparer un fichier de configuration de Day 0 (jour 0) avant de lancerdéfense contre les menaces virtuelles. Ce fichier est un fichier texte qui contient les données de configuration initiale appliquées lors du déploiement d'une machine virtuelle. Cette configuration initiale est placée dans un fichier texte nommé « day0-config » dans un répertoire de travail que vous avez choisi, puis manipulée dans un fichier day0.iso qui est monté et lu lors du premier démarrage.

Important Le fichier day0.so doit être disponible lors du premier démarrage.

Si vous effectuez le déploiement avec un fichier de configuration Day0 (Jour0), le processus vous permet d'effectuer la configuration initiale complète de l'appareil défense contre les menaces virtuelles. Vous pouvez préciser :

- L'adhésion au Contrat de licence de l'utilisateur final (CLUF).
- Un nom d'hôte pour le système.
- Un nouveau mot de passe d'administrateur pour le compte admin.
- Le mode de gestion; voir Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual.

  Saisissez les informations pour les champs centre de gestion (**FmcIp**, **FmcRegKey**et **FmcNatId**). Ne remplissez pas les champs pour le mode de gestion que vous n'utilisez pas.
- Paramètres réseau qui permettent à l'appareil de communiquer sur votre réseau de gestion.
- Le type de déploiement; vous pouvez préciser si vous déployez défense contre les menaces virtuelles en grappes ou en déploiement autonome.

Remarque La machine Linux est utilisée dans cet exemple, mais il existe des utilitaires similaires pour Windows.

Procédure

Étape 1 Connectez-vous à l'hôte Linux sur lequel vous souhaitez déployer défense contre les menaces virtuelles.

Étape 2 Créez un fichier texte appelé « day0-config » pour défense contre les menaces virtuelles. Dans ce fichier texte, vous devez ajouter les paramètres de déploiement en grappe, les paramètres réseau et les informations sur la gestion de centre de gestion.

Exemple :

```
#Firepower Threat Defense
{

     "DeploymentType": "Cluster"
```

```
}
```

Saisissez les informations pour les champs centre de gestion (**FmcIp**, **FmcRegKey**et **FmcNatId**). Pour l'option de gestion que vous n'utilisez pas, laissez ces champs vides.

Étape 3 Générez le CD-ROM virtuel en convertissant le fichier texte en fichier ISO :

Exemple :

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

Étape 4 Connectez-vous à l'hôte ESXi cible.

Étape 5 Ouvrez l'instance de machine virtuelle sur laquelle vous souhaitez déployer défense contre les menaces virtuelles en mode grappe.

Étape 6 Parcourez et associez le fichier image ISO day0 que vous avez créé dans le champ **CD/DVD drive 1** sous les paramètres de configuration du matériel (**Hardware Configuration**) avant de démarrer la machine virtuelle.

Étape 7 Mettez la machine virtuelle sous tension pour déployer défense contre les menaces virtuelles en mode grappe.

Déployer Défense contre les menaces virtuelles sur un hôte ESXi vSphere

Utilisez cette procédure pour déployer l'appareil défense contre les menaces virtuelles sur un seul hôte ESXi. Vous pouvez utiliser le client d'hôte VMware (ou client vSphere) pour gérer des hôtes ESXi uniques et effectuer des tâches administratives telles que des opérations de virtualisation de base, comme le déploiement et la configuration de machines défense contre les menaces virtuelles.

Remarque Il est important de savoir que même si leurs interfaces utilisateur sont sembables, le client hôte VMware est différent du client Web vSphere. On utilise le client Web vSphere pour se connecter au serveur vCenter et gérer plusieurs hôtes ESXi, tandis qu'on utilise le client hôte VMware pour gérer un seul hôte ESXi.

Pour des instructions sur le déploiement de l'appareil défense contre les menaces virtuelles dans un environnement vCenter, consultez Déployer Défense contre les menaces virtuelles dans vSphere vCenter, à la page 22.

Avant de commencer

- Vous devez avoir au moins un réseau configuré dans vSphere (pour la gestion) avant de déployer le défense contre les menaces virtuelles.

Procédure

Étape 1 Téléchargez le paquet d'installation défense contre les menaces virtuelles pour VMware ESXi à partir de Cisco.com et enregistrez-le sur votre ordinateur de gestion local :

https://www.cisco.com/go/ftd-software

Une connexion à Cisco.com et un contrat de service Cisco sont requis.

Étape 2 Décompressez le fichier TAR dans un répertoire de travail. Ne supprimez aucun fichier du répertoire. Les fichiers suivants sont inclus :

- Cisco_Firepower_Threat_Defense_Virtual-VI-*X.X.X-xx*.ovf — pour les déploiements de vCenter
- Cisco_Firepower_Threat_Defense_Virtual-ESXi-*X.X.X-xx*.ovf — pour les déploiements de vCenter
- Cisco_Firepower_Threat_Defense_Virtual-*X.X.X-xx*.vmdk— fichier de disque virtuel de VMware.
- Cisco_Firepower_Threat_Defense_Virtual-VI-*X.X.X-xx*.mf— fichier de manifeste pour les déploiements vCenter.
- Cisco_Firepower_Threat_Defense_Virtual-ESXi-*X.X.X-xx*.mf — fichier de manifeste pour les déploiements ESXi.

où *X.X.X-xx* est la version et le numéro de version du fichier d'archive que vous avez téléchargé.

Étape 3 Dans un navigateur, saisissez le nom d'hôte ou l'adresse IP cible ESXi au format *http://host-name/ui* ou *http://host-IP-address/ui*.

Une fenêtre de connexion s'affiche.

Étape 4 Saisissez le nom d'utilisateur administrateur et le mot de passe.

Étape 5 Cliquez sur **Login** pour ouvrir une session.

Vous êtes maintenant connecté à votre hôte ESXi cible.

Étape 6 Faites un clic droit sur **Host** (hôte) dans l'inventaire VMware Host Client (client d'hôte VMware) et sélectionnez **Create/Register VM** pour créer et enregistrer une machine virtuelle.

L'assistant de nouvelle machine virtuelle s'ouvre.

Étape 7 Dans la page **Select creation type** (sélectionner le type de création) de l'assistant, sélectionnez **Deploy a virtual machine from an OVF or OVA file** (déployer une machine virtuelle à partir d'un fichier OVF ou OVA) et cliquez sur **Next** (suivant).

Étape 8 Sur la page **de sélection des fichiers OVF et VMDK** de l'assistant :

a) Saisissez un nom pour votre machine défense contre les menaces virtuelles.

Les noms de machine virtuelle peuvent contenir jusqu'à 80 caractères et doivent être uniques dans chaque instance ESXi.

b) Cliquez sur le volet bleu, accédez au répertoire où vous avez décompressé le fichier tar défense contre les menaces virtuelles, puis choisissez le modèle OVF ESXi et le fichier VMDK qui l'accompagne :

Cisco_Firepower_Threat_Defense_Virtual-ESXi-*X.X.X-xx*.ovf

Cisco_Firepower_Threat_Defense_Virtual-*X.X.X-xx*.vmdk

où *X.X.X-xx* est la version et le numéro de version du fichier d'archive que vous avez téléchargé.

Attention
Assurez-vous de sélectionner le protocole OVF ESXi.

Étape 9 Cliquez sur **Next** (suivant).

Le stockage de votre système local s'ouvre.

Étape 10 Choisissez une banque de données dans la liste des banques de données accessibles sur la page **Select storage** (sélectionner le stockage) de l'assistant.

Une banque de données stocke les fichiers de configuration de la machine virtuelle et tous les disques virtuels. Chaque banque de données peut avoir une taille, une vitesse, une disponibilité et d'autres propriétés différentes.

Étape 11 Cliquez sur **Next** (suivant).

Étape 12 Configurez les **options de déploiement** du protocole OVF ESXi pour le défense contre les menaces virtuelles :

a) **Network Mapping** (mappage du réseau) : mappez les réseaux spécifiés dans le modèle OVF aux réseaux de votre inventaire, puis sélectionnez **Next** (suivant).

Assurez-vous que l'interface de gestion 0-0 est ass ociée à un réseau de machine virtuelle accessible à partir d'Internet. Les interfaces qui ne sont pas des interfaces de gestion sont configurables à partir du centre de gestion ou du gestionnaire d'appareil, selon votre mode de gestion.

Important
Défense contre les menaces virtuelles sur VMware utilise maintenant les interfaces vmxnet3 par défaut lorsque vous créez un périphérique virtuel. Auparavant, la valeur par défaut était e1000. Si vous utilisez des interfaces e1000, nous vous **recommandons fortement** de changer. Les pilotes de périphérique vmxnet3 et le traitement réseau sont intégrés à l'hyperviseur ESXi. Ils utilisent donc moins de ressources et offrent de meilleures performances réseau.

Les réseaux ne peuvent pas être en ordre alphabétique. S'il est trop difficile de trouver vos réseaux, vous pouvez modifier les réseaux plus tard à partir de la boîte de dialogue de modification des paramètres (**Edit Settings**). Après le déploiement, cliquez avec le bouton droit sur l'instance défense contre les menaces virtuelles et choisissez **Edit Settings** (modifier les paramètres). Cependant, cet écran n'affiche pas les ID défense contre les menaces virtuelles (uniquement les ID d'adaptateur réseau).

Consultez la concordance suivante concernant l'adaptateur réseau, les réseaux sources et les réseaux de destination pour les interfaces défense contre les menaces virtuelles (il s'agit des interfaces vmxnet3 par défaut) :

Tableau 8 : Mappage du réseau source au réseau de destination : VMXNET3

Adaptateur réseau	Réseaux sources	Réseaux de destination	Fonction
Adaptateur réseau 1	Gestion 0-0	Gestion 0/0	Gestion
Adaptateur réseau 2	Diagnostic 0-0	Diagnostic 0/0	Diagnostic
Adaptateur réseau 3	GigabitEthernet 0-0	GigabitEthernet 0/0	Données externes
Adaptateur réseau 4	GigabitEthernet 0-1	GigabitEthernet 0/1	Données internes
Adaptateur réseau 5	GigabitEthernet 0-2	GigabitEthernet 0/2	Trafic de données (facultatif)
Adaptateur réseau 6	GigabitEthernet 0-3	GigabitEthernet 0/3	Trafic de données (facultatif)
Adaptateur réseau 7	GigabitEthernet 0-4	GigabitEthernet 0/4	Trafic de données (facultatif)
Adaptateur réseau 8	GigabitEthernet 0-5	GigabitEthernet 0/5	Trafic de données (facultatif)

Adaptateur réseau	Réseaux sources	Réseaux de destination	Fonction
Adaptateur réseau 9	GigabitEthernet 0-6	GigabitEthernet 0/6	Trafic de données (facultatif)
Adaptateur réseau 10	GigabitEthernet 0-7	GigabitEthernet 0/7	Trafic de données (facultatif)

Vous pouvez avoir un total de 10 interfaces lorsque vous déployez le défense contre les menaces virtuelles. Pour les interfaces de données, assurez-vous que les réseaux sources correspondent aux réseaux de destination appropriés et que chaque interface de données est mappée à un sous-réseau ou à un VLAN unique. Vous n'avez pas besoin d'utiliser toutes les interfaces défense contre les menaces virtuelles; pour les interfaces que vous n'avez pas l'intention d'utiliser, vous pouvez simplement laisser l'interface désactivée dans la configuration défense contre les menaces virtuelles.

b) **Provisionnement de disque** : sélectionnez le format de disque pour stocker les disques virtuels de la machine virtuelle.

Lorsque vous sélectionnez **Thick** provisioned (grand provisionnement), tout le stockage est immédiatement alloué. Lorsque vous sélectionnez**Thin** provisioned (provisionnement léger), le stockage est attribué à la demande, au fur et à mesure que les données sont écrites sur les disques virtuels. Le provisionnement léger peut également réduire le temps nécessaire pour déployer l'appliance virtuelle.

Étape 13 Sur la page **Ready to complete** (prêt à terminer) de l'assistant de nouvelle machine virtuelle, passez en revue les paramètres de configuration de la machine virtuelle.

a) (Facultatif) Cliquez sur **Back** pour revenir en arrière et examiner ou modifier les paramètres de l'assistant.
b) (Facultatif) Cliquez sur **Cancel** pour annuler la tâche de création et fermer l'assistant.
c) Cliquez sur **Finish** pour terminer la tâche de création et fermer l'assistant.

Après avoir terminé e processus de l'assistant, l'hôte ESXi traite la machine virtuelle; vous pouvez voir l'état du déploiement dans le volet des tâches récentes (**Recent Tasks**). Un déploiement réussi affiche *Completed successfully* (terminé avec succès) dans la colonne **Results** (résultats).

La nouvelle instance de machine virtuelle défense contre les menaces virtuelles apparaît alors dans l'inventaire des machines virtuelles de l'hôte ESXi. Le démarrage de la nouvelle machine virtuelle peut prendre jusqu'à 30 minutes.

Remarque
Pour enregistrer avec succès défense contre les menaces virtuelles auprès de l'autorité de licence de Cisco, défense contre les menaces virtuelles nécessite un accès Internet. Vous devrez peut-être effectuer une configuration supplémentaire après le déploiement pour obtenir un accès Internet et un enregistrement de licence réussi.

Prochaine étape

- Terminez la configuration de votre appareil virtuel à l'aide de l'interface de ligne de commande. Il s'agit de l'étape suivante lorsque vous déployez défense contre les menaces virtuelles à l'aide du modèle OVF ESXi; voir Terminer la configuration de Défense contre les menaces virtuelles à l'aide de l'interface de ligne de commande, à la page 36.

Terminer la configuration de Défense contre les menaces virtuelles à l'aide de l'interface de ligne de commande

Si vous avez procédé au déploiement avec un modèle OVF ESXi, vous devez configurer le défense contre les menaces virtuelles à l'aide de l'interface de ligne de commande. Les périphériques Défense contre les menaces virtuelles n'ont pas d'interface Web. Vous pouvez également utiliser l'interface de ligne de commande pour configurer les paramètres requis par le système si vous avez déployé avec un modèle OVF VI et que vous n'avez pas utilisé l'assistant de configuration lors du déploiement.

Remarque Si vous avez déployé un modèle OVF VI et utilisé l'assistant de configuration, votre appareil virtuel est configuré et aucune autre configuration d'appareil n'est requise. Vos prochaines étapes dépendent du mode de gestion que vous avez choisi.

Lorsque vous vous connectez pour la première fois à un appareil nouvellement configuré, vous devez lire et accepter le CLUF. Suivez ensuite les invites de configuration pour modifier le mot de passe administrateur et configurer les paramètres réseau et le mode de pare-feu du périphérique.

Lorsque vous suivez les invites de configuration, pour les questions à choix multiples, vos options sont répertoriées entre parenthèses, par exemple (y/n) pour oui ou non. Les valeurs par défaut sont répertoriées entre parenthèses, telles que [y]. Appuyez sur Enter (entrée) pour confirmer votre choix.

Procédure

Étape 1 Ouvrez la console VMware.

Étape 2 À **l'invite de connexion firepower**, connectez-vous avec le nom d'utilisateur par défaut en tant qu'**admin**. Le mot de passe est **Admin123**.

Étape 3 Lorsque le système défense contre les menaces virtuelles démarre, un assistant de configuration vous demande les informations suivantes pour configurer le système :

- Accepter le CLUF
- Nouveau mot de passe de l'administrateur
- Configuration IPv4
- Paramètres DHCP IPv4
- Adresse IPv4 et filtre d'adresse locale du port de gestion.
- Nom du système
- Passerelle par défaut
- Configuration DNS
- Proxy HTTP
- Mode de gestion (la gestion locale utilise gestionnaire d'appareil).

Étape 4 Passez en revue les paramètres de l'assistant de configuration. Les valeurs par défaut ou les valeurs saisies précédemment apparaissent entre parenthèses. Pour accepter les valeurs saisies précédemment, appuyez sur la touche **Enter** (Entrée).

La console VMware peut afficher des messages lors de la mise en œuvre de vos paramètres.

Étape 5 Terminez la configuration du système en suivant les invites.

Étape 6 Vérifiez que la configuration a réussi lorsque la console revient à l'invite firepower.

Remarque
Pour enregistrer avec succès défense contre les menaces virtuelles auprès de l'autorité de licence de Cisco, défense contre les menaces virtuelles nécessite un accès Internet. Vous devrez peut-être effectuer une configuration supplémentaire après le déploiement pour obtenir un accès Internet et un enregistrement de licence réussi.

Prochaine étape

Vos prochaines étapes dépendent du mode de gestion que vous avez choisi.

- Si vous avez sélectionné **No** (non) pour **Enable Local Manager** (activer le gestionnaire local), vous utiliserez centre de gestion pour gérer défense contre les menaces virtuelles; à ce sujet, consultez Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cisco Secure Firewall Management Center.

Consultez Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual pour savoir comment choisir votre option de gestion.

Amélioration de la performance pour les configurations ESXi

Vous pouvez améliorer la performance de défense contre les menaces virtuelles dans l'environnement ESXi en réglant les paramètres de configuration du CPU de l'hôte ESXi. L'option Scheduling Affinity (planification de l'affinité) vous permet de contrôler la répartition des CPU des machines virtuelles sur les cœurs physiques de l'hôte (et sur les hyperthreads si cette technologie est activée). En utilisant cette fonctionnalité, vous pouvez affecter chaque machine virtuelle aux processeurs de l'ensemble d'affinité spécifié.

Consultez les documents VMware suivants pour plus d'informations :

- Le chapitre sur *l'administration des ressources du CPU* dans Gestion des ressources de vSphere.
- Bonnes pratiques en matière de performances pour VMware vSphere.
- L'aide en ligne du client vSphere.

Lignes directrices NUMA

L'accès mémoire non uniforme (NUMA, Non-Uniform Memory Access) est une architecture de mémoire partagée qui décrit le placement des modules de mémoire principaux en ce qui concerne les processeurs dans un système multiprocesseur. Lorsqu'un processeur accède à la mémoire qui ne se trouve pas dans son propre nœud (mémoire distante), les données doivent être transférées sur la connexion NUMA à un débit plus lent qu'il ne le serait lors de l'accès à la mémoire locale.

L'architecture du serveur x86 est composée de plusieurs connecteurs et de plusieurs cœurs dans un connecteur. Chaque connecteur d'unité centrale, ainsi que sa mémoire et son entrée-sortie, est appelé nœud NUMA. Pour

lire efficacement les paquets à partir de la mémoire, les applications invitées et les périphériques associés (comme la carte d'interface réseau) doivent résider sur le même nœud.

Pour une performance défense contre les menaces virtuelles optimale :

- La machine virtuelle défense contre les menaces virtuelles doit fonctionner sur un seul nœud NUMA. Si un seul défense contre les menaces virtuelles est déployé de sorte qu'il fonctionne sur deux connecteurs, la performance sera considérablement réduite.
- Un défense contre les menaces virtuelles à huit cœurs exige que chaque connecteur de l'unité centrale hôte ait au moins huit cœurs par connecteur. Il faut tenir compte des autres machines virtuelles en cours d'exécution sur le serveur.
- Un défense contre les menaces virtuelles à 16 cœurs exige que chaque connecteur de l'unité centrale hôte ait au moins 16 cœurs par connecteur. Il faut tenir compte des autres machines virtuelles en cours d'exécution sur le serveur.
- La carte réseau (NIC) doit se trouver sur le même nœud NUMA que la machine virtuelle défense contre les menaces virtuelles.

Vous trouverez plus de renseignements sur l'utilisation des systèmes NEMA avec ESXi dans le document VMware *Gestion des ressources de vSphere* pour votre version de VMware ESXi. Pour obtenir les versions les plus récentes de ce document et d'autres documents pertinents, consultez la page http://www.vmware.com/support/pubs.

Provisionnement d'interface SR-IOV

La virtualisation des I/O de racine unique (SR-IOV) permet à plusieurs machines virtuelles exécutant divers systèmes d'exploitation invités de partager un seul adaptateur de réseau PCIe dans un serveur d'hôte. SR-IOV permet à une machine virtuelle de déplacer des données directement vers et à partir de l'adaptateur réseau, en contournant l'hyperviseur pour augmenter le débit du réseau et réduire la charge CPU du serveur. Les processeurs de serveur x86 récents comprennent des améliorations de jetons, comme la technologie Intel VT-d, qui facilitent les transferts directs de mémoire et d'autres opérations requises par SR-IOV.

La spécification SR-IOV définit deux types d'appareils :

- Fonction physique (PF) : essentiellement une carte réseau statique, un appareil de PF est un périphérique PCIe complet qui comprend des fonctionnalités SR-IOV. Les appareils de PF sont détectés, gérés et configurés comme des périphériques PCIe normaux. Un seul appareil de PF peut assurer la gestion et la configuration d'un ensemble de fonctions virtuelles (VF).
- Fonction virtuelle (VF) : comme pour une vNIC dynamique, un appareil de VF est un périphérique PCIe virtuel complet ou allégé qui fournit au moins les ressources nécessaires pour les déplacements de données. Un appareil de VF n'est pas géré directement, mais il est dérivé et géré par un appareil de PF. Un ou plusieurs appareils de VF peuvent être attribués à une machine virtuelle (ou VM).

Les appareils de VF peuvent fournir une connectivité allant jusqu'à 10 Gbit/s aux machines défense contre les menaces virtuelles dans une structure de système d'exploitation virtualisé. Cette section explique comment configurer les appareils de VF dans un environnement VMware.

Bonnes pratiques pour les interfaces SR-IOV

Lignes directrices relatives aux interfaces SR-IOV

VMware vSphere 5.1 et les versions ultérieures prennent en charge SR-IOV dans un environnement avec des configurations spécifiques uniquement. Certaines fonctionnalités de vSphere ne sont pas opérationnelles lorsque SR-IOV est activé.

En plus des exigences système pour défense contre les menaces virtuelles et SR-IOV, vous devez passer en revue les configurations prises en charge pour l'utilisation de SR-IOV dans la documentation de VMware pour en savoir plus sur les exigences, les cartes réseau prises en charge, la disponibilité des fonctionnalités et les exigences de mise à niveau pour VMware et SR-IOV.

Défense contre les menaces virtuelles sur VMware à l'aide de l'interface SR-IOV prend en charge le mélange de types d'interfaces. Vous pouvez utiliser SR-IOV ou VMXNET3 pour l'interface de gestion et SR-IOV pour l'interface de données.

Cette section montre diverses étapes d'installation et de configuration pour le provisionnement des interfaces SR-IOV sur un système VMware. Les renseignements figurant dans cette section ont été créés à partir de périphériques dans un environnement de laboratoire spécifique, en utilisant VMware ESXi 6.0 et le client web vSphere, un serveur Cisco série UCS C et un adaptateur de serveur Ethernet Intel X520 - DA2.

Limites des interfaces SR-IOV

Lorsque défense contre les menaces virtuelles est démarré, sachez que les interfaces SR-IOV peuvent s'afficher dans l'ordre inverse de celui présenté dans ESXi. Cela pourrait entraîner des erreurs de configuration d'interface qui entraîneront un manque de connectivité réseau pour une machine défense contre les menaces virtuelles particulière.

⚠

Mise en garde Il est important de vérifier le mappage de l'interface avant de commencer à configurer les interfaces réseau SR-IOV sur le défense contre les menaces virtuelles. Cela garantit que la configuration de l'interface réseau s'appliquera à la bonne interface d'adresse MAC physique sur l'hôte de machine virtuelle.

Après le démarrage du défense contre les menaces virtuelles, vous pouvez confirmer quelle adresse MAC est mappée à quelle interface. Utilisez la commande **show interface** (afficher l'interface) pour afficher des renseignements détaillés sur l'interface, y compris l'adresse MAC d'une interface. Comparez l'adresse MAC avec les résultats de la commande **show kernel ifconfig** pour confirmer l'affectation d'interface correcte.

REMARQUE :

Limites de l'utilisation des interfaces ixgbe-vf

Gardez à l'esprit des limites suivantes lors de l'utilisation des interfaces ixgbe-vf :

- La machine virtuelle (VM) invitée n'est pas autorisée à définir la VF en mode de proximité. Pour cette raison, le mode transparent n'est pas pris en charge lors de l'utilisation de ixgbe-vf.
- La VM invitée n'est pas autorisée à définir l'adresse MAC sur la VF. C'est pourquoi l'adresse MAC n'est pas transférée pendant la haute accessibilité, comme cela se fait sur d'autres plateformes défense contre les menaces virtuelles et avec d'autres types d'interfaces. Le basculement de la haute accessibilité fonctionne par le transfert de l'adresse IP du mode actif au mode en veille.

Remarque Cette limite s'applique également aux interfaces i40e-vf.

- Le serveur Cisco UCS-B ne prend pas en charge la vNIC ixgbe-vf.
- Dans une configuration de basculement, en cas de défaillance d'une défense contre les menaces virtuelles (unité principale de la paire), l'unité en veille défense contre les menaces virtuelles prend le rôle d'unité principale, et l'adresse IP de son interface est mise à jour avec la nouvelle adresse MAC de l'unité en veille défense contre les menaces virtuelles. Ensuite, défense contre les menaces virtuelles envoie une mise à jour spontanée du protocole ARP (Address Resolution Protocol) pour annoncer le changement d'adresse MAC de l'adresse IP de l'interface aux autres périphériques du même réseau. Cependant, en raison d'une incompatibilité avec ces types d'interfaces, la mise à jour spontanée du protocole ARP n'est pas envoyée à l'adresse IP globale qui est définie dans les instructions NAT ou PAT pour traduire l'adresse IP de l'interface en adresses IP globales.

Vérifier le BIOS de l'hôte ESXi

Avant de commencer

Pour déployer défense contre les menaces virtuelles avec les interfaces SR-IOV sur VMware, la virtualisation doit être prise en charge et activée. VMware propose plusieurs méthodes pour vérifier la prise en charge de la virtualisation, y compris leur Guide de compatibilité en ligne pour la prise en charge de SR-IOV et un programme utilitaire d'identification de CPU téléchargeable qui détecte si la virtualisation est activée ou désactivée.

Vous pouvez également déterminer si la virtualisation est activée dans le BIOS en vous connectant à l'hôte ESXi.

Procédure

Étape 1 Connectez-vous à l'interface Shell ESXi en utilisant l'une des méthodes suivantes :

- Si vous avez un accès direct à l'hôte, appuyez sur Alt+F2 pour ouvrir la page de connexion sur la console physique de la machine.
- Si vous vous connectez à l'hôte à distance, utilisez le protocole SSH ou une autre connexion de console distante pour démarrer une session sur l'hôte.

Étape 2 Saisissez un nom d'utilisateur et un mot de passe reconnus par l'hôte.

Étape 3 Exécutez la commande suivante :

```
esxcfg-info|grep "\----\HV Support"
```

- Le résultat de la commande HV Support indique le type de prise en charge d'hyperviseur disponible. Voici les descriptions des valeurs possibles :
- 0 – VT/AMD-V indique que la prise en charge n'est pas disponible pour ce matériel.
- 1 – VT/AMD-V indique que VT ou AMD-V peut être disponible, mais qu'il n'est pas pris en charge par ce matériel.
- 2 – VT/AMD-V indique que VT ou AMD-V est disponible, mais n'est actuellement pas activé dans le BIOS.

- 3 – VT/AMD-V indique que VT ou AMD-V est activé dans le BIOS et peut être utilisé.

```
~ # esxcfg-info|grep "\----\HV Support"
         |----HV Support.........................3
```

La valeur 3 indique que la virtualisation est prise en charge et activée.

Prochaine étape

Activez SR-IOV sur l'adaptateur physique de l'hôte.

Activer SR-IOV sur l'adaptateur physique de l'hôte

Avant de pouvoir connecter des machines virtuelles à des fonctions virtuelles, utilisez le client web vSphere pour activer SR-IOV et définir le nombre de fonctions virtuelles sur votre hôte.

Avant de commencer

- Assurez-vous d'avoir installé une carte d'interface réseau (NIC) compatible avec SR-IOV; voir Configuration système requise, à la page 3.

Procédure

Étape 1 Dans le client web vSphere, accédez à l'hôte ESXi sur lequel vous souhaitez activer SR-IOV.

Étape 2 Dans l'onglet **Manage** (gérer), cliquez sur **Networking** (mise en réseau) et sélectionnez **Physical Adapters** (adaptateurs physiques).

Vous pouvez consulter la propriété SR-IOV pour voir si un adaptateur physique prend en charge SR-IOV.

Étape 3 Sélectionnez l'adaptateur physique et cliquez sur **Edit Adapter Settings** (modifier les paramètres de l'adaptateur).

Étape 4 Sous SR-IOV, sélectionnez **Enabled** (activé) dans le menu déroulant **Status** (état).

Étape 5 Dans la zone de texte **Number of virtual functions** (nombre de fonctions virtuelles), saisissez le nombre de fonctions virtuelles que vous souhaitez configurer pour l'adaptateur.

Remarque
Nous vous recommandons de **NE PAS** utiliser plus d'une VF par interface. Une dégradation des performances est susceptible de se produire si vous partagez l'interface physique avec plusieurs fonctions virtuelles.

Étape 6 Cliquez sur **OK**.

Étape 7 Redémarrez l'hôte ESXi.

Les fonctions virtuelles deviennent actives sur le port NIC représenté par l'entrée d'adaptateur physique. Elles apparaissent dans la liste PCI Devices (appareils PCI) de l'onglet **Settings** (paramètres) de l'hôte.

Prochaine étape

- Créez un vSwitch standard pour gérer les fonctions et les configurations SR-IOV.

Créer un commutateur vSphere

Créez un commutateur vSphere pour gérer les interfaces SR-IOV.

Procédure

Étape 1 Dans le client web vSphere, accédez à l'hôte ESXi.

Étape 2 Sous **Manage** (gérer), sélectionnez **Networking** (mise en réseau), puis **Virtual switches** (commutateurs virtuels).

Étape 3 Cliquez sur l'icône **Add host networking** (ajouter la mise en réseau des hôtes), qui est l'icône en forme de globe vert avec le signe plus (+).

Étape 4 Sélectionnez un type de connexion **Virtual Machine Port Group for a Standard Switch** (groupe de ports de machines virtuelles pour un commutateur standard) et cliquez sur **Next** (suivant).

Étape 5 Sélectionnez **New standard switch** (nouveau commutateur standard) et cliquez sur **Next** (suivant).

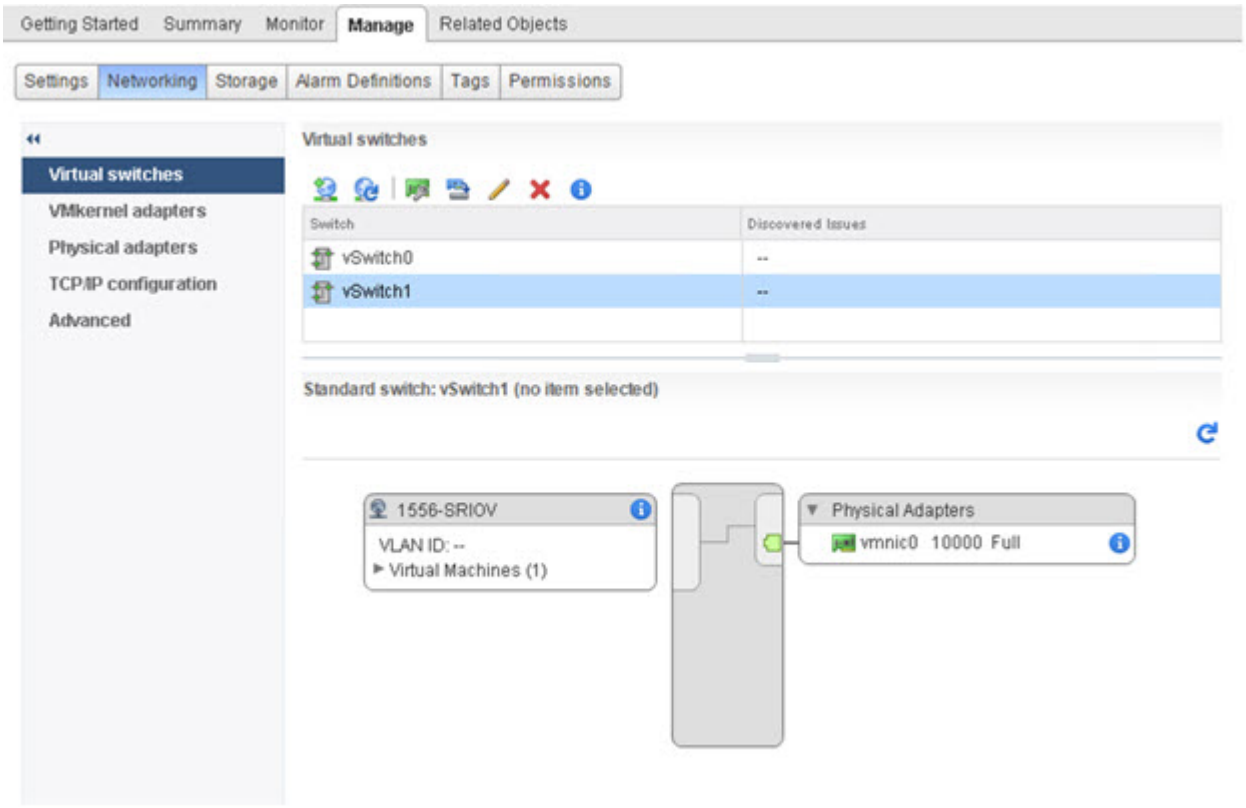
Étape 6 Ajoutez des adaptateurs réseau physiques au nouveau commutateur standard.

a) Sous Affected Adapters (adaptateurs attribués), cliquez sur le signe plus vert (+) pour sélectionner **Add adapters** (ajouter des adaptateurs).
b) Sélectionnez l'interface réseau correspondante pour SR-IOV dans la liste. Par exemple, Intel(R) 82599, 10 Gigabit, connexion réseau à double port.
c) Dans le menu déroulant **Failover order group** (groupe de commandes de basculement), sélectionnez parmi les **Active adapters** (adaptateurs actifs).
d) Cliquez sur **OK**.

Étape 7 Saisissez une **Network label** (étiquette de réseau) pour le vSwitch SR-IOV et cliquez sur **Next** (suivant).

Étape 8 Passez en revue vos sélections sur la page **Ready to complete** (prêt à terminer), puis cliquez sur **Finish** (terminer).

Illustration 2 : Nouveau vSwitch avec une interface SR-IOV associée



Prochaine étape

- Examinez le niveau de compatibilité de votre machine virtuelle.

Mettre à niveau le niveau de compatibilité des machines virtuelles

Le niveau de compatibilité détermine le matériel virtuel disponible pour la machine virtuelle, qui correspond au matériel physique disponible sur la machine hôte. La machine virtuelle défense contre les menaces virtuelles doit être au niveau matériel 10 ou supérieur. Cela exposera la fonctionnalité de transmission directe SR-IOV à défense contre les menaces virtuelles. Cette procédure met immédiatement à niveau défense contre les menaces virtuelles vers la dernière version de matériel virtuel prise en charge.

Pour en savoir plus sur les versions matérielles et la compatibilité des machines virtuelles, consultez la documentation d'administration de la machine virtuelle de vSphere.

Procédure

Étape 1 Connectez-vous au serveur vCenter à partir du client Web vSphere.

Étape 2 Localisez la machine défense contre les menaces virtuelles que vous souhaitez modifier.

a) Sélectionnez un centre de données, un dossier, une grappe, un ensemble de ressources ou un hôte et cliquez sur l'onglet **Related Objects** (objets associés).

b) Cliquez sur **Virtual Machines (machines virtuelles)** et sélectionnez la machine défense contre les menaces virtuelles dans la liste.

Étape 3 Mettez la machine virtuel sélectionnée sous tension.

Étape 4 Faites un clic droit sur défense contre les menaces virtuelles et sélectionnez **Actions** > **All vCenter Actions (toutes les actions de centre virtuel)** > **Compatibility (compatibilité)** > **Upgrade VM Compatibility (mettre à niveau la compatibilité de la machine virtuelle)**.

Étape 5 Cliquez sur **Yes** (Oui) pour confirmer le mise à niveau.

Étape 6 Choisissez l'option **ESXi 5.5 and later** (ESXi 5.5 ou ultérieure) pour la compatibilité des machines virtuelles.

Étape 7 (Facultatif) Sélectionnez **Only upgrade after normal guest OS shutdown** (mettre à niveau seulement après l'arrêt normal du système d'exploitation invité).

La machine virtuelle sélectionnée est mise à niveau vers la version matérielle correspondante pour le paramètre de compatibilité que vous avez choisi, et la nouvelle version matérielle est mise à jour dans l'onglet **Summary** (sommaire) de la machine virtuelle.

Prochaine étape

- Associez défense contre les menaces virtuelles à une fonction virtuelle par l'intermédiaire d'un adaptateur de réseau de transmission directe SR-IOV.

Attribuer la carte réseau (NIC) SR-IOV à Défense contre les menaces virtuelles

Pour vous assurer que la machine défense contre les menaces virtuelles et la carte réseau physique peuvent échanger des données, vous devez associer défense contre les menaces virtuelles à une ou plusieurs fonctions virtuelles en tant qu'adaptateurs réseau de transmission directe SR-IOV. La procédure suivante explique comment affecter la carte réseau SR-IOV à la machine défense contre les menaces virtuelles à l'aide du client web vSphere.

Procédure

Étape 1 Connectez-vous au serveur vCenter à partir du client Web vSphere.

Étape 2 Localisez la machine défense contre les menaces virtuelles que vous souhaitez modifier.

a) Sélectionnez un centre de données, un dossier, une grappe, un ensemble de ressources ou un hôte et cliquez sur l'onglet **Related Objects** (objets associés).

b) Cliquez sur **Virtual Machines (machines virtuelles)** et sélectionnez la machine défense contre les menaces virtuelles dans la liste.

Étape 3 Dans l'onglet **Manage** (gérer) de la machine virtuelle, sélectionnez **Settings (paramètres)** > **VM Hardware (matériel VM)**.

Étape 4 Cliquez sur **Edit** (modifier) et sélectionnez l'onglet **Virtual Hardware** (matériel virtuel).

Étape 5 Dans le menu déroulant **New device** (nouveau périphérique), sélectionnez **Network** (réseau) et cliquez sur **Add** (ajouter).

Une interface **New Network** (nouveau réseau) s'affiche.

Étape 6 Développez la section **New Network** (nouveau réseau) et sélectionnez une option SR-IOV disponible.

Étape 7 Dans le menu déroulant **Adapter Type** (type d'adaptateur), sélectionnez **SR-IOV passthrough** (transmission directe SR-IOV).

Étape 8 Dans le menu déroulant **Physical Function** (fonction physique), sélectionnez l'adaptateur physique qui correspond à l'adaptateur de machine virtuelle de transmission directe.

Étape 9 Mettez l'ordinateur virtuel sous tension.

Lorsque vous mettez la machine virtuelle sous tension, l'hôte ESXi sélectionne une fonction virtuelle libre dans l'adaptateur physique et la mappe à l'adaptateur de transmission directe SR-IOV. L'hôte valide toutes les propriétés de l'adaptateur de machine virtuelle et de la fonction virtuelle sous-jacente.

Remarque L'utilisation d'interfaces SR-IOV en tant qu'interfaces passives sur défense contre les menaces virtuelles n'est pas prise en charge sur certaines cartes réseau Intel (comme les Intel X710 ou 82599) utilisant les pilotes SR-IOV en raison d'une restriction de mode de proximité. Dans ce cas, utilisez une carte réseau qui prend en charge cette fonctionnalité. Consultez la section Produits Ethernet Intel pour plus d'informations sur les cartes réseau Intel.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.