Déployer Défense contre les menaces virtuelles sur Cisco HyperFlex

Ce chapitre décrit les procédures pour déployer défense contre les menaces virtuelles sur Cisco HyperFlex sur un serveur vCenter ou un hôte ESXi autonome.

Aperçu

Cisco Cisco Secure Firewall Threat Defense Virtual (anciennement Firepower Threat Defense Virtual) apporte la fonctionnalité de pare-feu sécurisé de Cisco à des environnements virtualisés, ce qui permet à des politiques de sécurité cohérentes de faire le suivi des charges de travail dans vos environnements physiques, virtuels et en nuage, et entre les nuages.

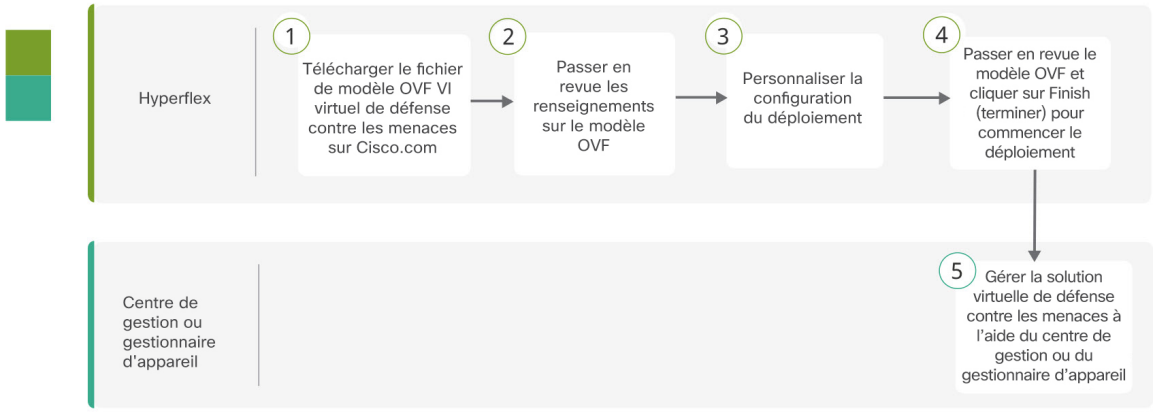
Les systèmes HyperFlex offrent une hyperconvergence pour toutes les applications et partout. Hyperflex, associé à la technologie Cisco Unified Computing System (Cisco UCS) gérée par la plateforme d'exploitation du nuage Cisco Intersight, peut propulser les applications et les données n'importe où, optimiser les opérations d'un centre de données central vers la périphérie et dans les nuages publics, et augmenter ainsi l'agilité en accélérant les pratiques DevOps.

Ce chapitre décrit le fonctionnement de défense contre les menaces virtuelles dans un environnement Cisco HyperFlex, y compris la prise en charge des fonctionnalités, les exigences du système, les lignes directrices et les limites. Ce chapitre décrit également vos options pour la gestion de défense contre les menaces virtuelles. Il est important que vous compreniez vos options de gestion avant de commencer votre déploiement. Vous pouvez gérer et surveiller défense contre les menaces virtuelles à l'aide de Cisco Secure Firewall Management

Center (anciennement Cisco Firepower Management Center) ou de Cisco Secure Firewall Device Manager (anciennement Firepower Device Manager). D'autres options de gestion peuvent être disponibles.

Procédure de bout en bout

Le diagramme suivant illustre le flux de travail pour le déploiement de Threat Defense Virtual sur Cisco HyperFlex.



	Espace de travail	Étapes
1	Hyperflex	Déployer Threat Defense Virtual sur Hyperflex : Téléchargez le fichier de modèle OVF VI virtuel de défense contre les menaces sur Cisco.com.
2	Hyperflex	Déployer Threat Defense Virtual sur Hyperflex : Passez en revue les informations sur le modèle OVF.
3	Hyperflex	Déployer Threat Defense Virtual sur Hyperflex : Personnalisez la configuration de déploiement.
4	Hyperflex	Déployer Threat Defense Virtual sur Hyperflex : Examinez et vérifiez les informations affichées. Cliquez sur Finish (terminer) pour commencer le déploiement du modèle OVF.
5	Centre de gestion ou gestionnaire d'appareil	Gérer Threat Defense Virtual : • À l'aide du centre de gestion • À l'aide du gestionnaire d'appareil

Configuration système requise

Versions

Version du gestionnaire	Version de l'appareil
Gestionnaire d'appareil 7.0	Défense contre les menaces 7.0
Centre de gestion 7.0	

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.

Mémoire, taille du disque et vCPU 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.

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 l'octroi de licences pour le système des documents *Configuration du centre de gestion Secure Firewall Management Center Configuration* et pour obtenir des instructions relatives à la licence de 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.
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	défense contre les menaces virtuelles prend en charge les adaptateurs de réseau virtuel suivants : • **VMXNET3** : le 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. (version 7.1 ou ultérieure) Le pilote vmxnet3 utilise le premier adaptateur Ethernet pour la gestion. Le deuxième adaptateur est inutilisé. (version 7.0 ou antérieure) 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.

Licences Défense contre les menaces virtuelles

- Configurez tous les droits de licence pour les services de sécurité à partir de la Centre de gestion.
- Pour en savoir plus sur la gestion des licences, consultez la section sur *les licences pour le système* du Guide de configuration du centre de gestion Cisco Secure Firewall Management Center.

Configurations et grappes pour les systèmes Hyperflex de série HX

Configurations	Grappes
Nœuds convergés HX220c	• Grappe de flash • Au moins une grappe de 3 nœuds (bases de données, VDI, VSI)
Nœuds convergés HX240c	• Grappe de flash • Au moins une grappe de 3 nœuds (VSI : applications informatiques/informatiques, test/développement)
HX220C et Edge (VDI, VSI, ROBO) HX240C (VDI, VSI, test/développement	• Grappe hybride • Grappe de 3 nœuds au moins
B200 + C240/C220	Applications liées à l'informatique/VDI

Options de déploiement pour le périphérique Hyperflex de série HX :

- Grappe hybride
- Grappe flash
- HyperFlex Edge
- Lecteurs SED

- Cache NVME
- GPU

Pour l'option de gestion en nuage HyperFlex HX, consultez la section sur le *déploiement des grappes reliées à l'interconnexion* de la trame HyperFlex dans le Guide d'installation de Cisco HyperFlex Systems.

Composants et versions d'HyperFlex

Composant	Version
VMware vSphere/VMware ESXI	7.0 Pour en savoir plus sur la compatibilité de Threat Defense Virtual avec VMware vSphere/VMware ESXI, consultez Compatibilité de Threat Defense Virtual : VMware.
Plateforme de données HyperFlex	4.5.1a-39020 et versions ultérieures .

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

- Modes de déploiement : routage (autonome), routage (HA), dérivateur en ligne, En ligne, passif et transparent
- BYOL avec licence uniquement
- IPv6
- Haute accessibilité en natif Défense contre les menaces virtuelles
- Bâtis grand format
- Grappes de centre de données Hyperflex (à l'exception des grappes étendues)
- Grappes de HyperFlex Edge
- Nœuds convergés HyperFlex All NVMe, All Flash et Hybrid
- Nœuds de traitement informatique Hyperflex uniquement

Fonctionnalités non prises en charge

Défense contre les menaces virtuelles exécuté avec SR-IOV n'a pas été qualifié avec HyperFlex.

Remarque HyperFlex prend en charge SR-IOV, mais nécessite une carte réseau PCI-e en plus du VIC MLOM

Lignes directrices générales

Pour configurer les vSwitch pour HyperFlex, vous pouvez utiliser l'interface graphique ou l'interface de ligne de commande. Ces configurations sont utiles lorsque vous installez plusieurs serveurs ESX et que vous prévoyez de scripter la configuration de vSwitch. Pour en savoir plus, consultez la section sur la configuration des vSwitch du Guide de gestion du réseau et du stockage externe des systèmes Cisco HyperFlex.

La concordance décrite ci-après concerne l'adaptateur réseau, les réseaux sources et les réseaux de destination pour les interfaces défense contre les menaces virtuelles :

Adaptateur réseau	Réseau source	Réseau de destination	Fonction
Adaptateur réseau 1	Gestion 0-0	Gestion 0/0	Gestion
Adaptateur réseau 2	Diagnostic 0-0	Diagnostic	Diagnostic
Adaptateur réseau 3	GigabitEthernet 0-0	GigabitEthernet 0/0	Externe
Adaptateur réseau 4	GigabitEthernet 0-1	GigabitEthernet 0/1	Interne
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)
...jusqu'à l'adaptateur réseau 10			

Optimisation des performances

Pour obtenir les meilleures performances avec défense contre les menaces virtuelles, vous pouvez apporter des ajustements à la machine virtuelle et à l'hôte. Consultez la section sur le réglage et l'optimisation de la virtualisation sur HyperFlex pour en savoir plus.

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. 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.

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

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. Le défense contre les menaces virtuelles utilise le mode de proximité pour fonctionner, et la haute accessibilité du défense contre les menaces virtuelles dépend du changement d'adresses MAC entre l'appareil actif et l'appareil en veille pour fonctionner correctement.

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

Tableau 1 : Options de politique de sécurité du commutateur standard vSphere

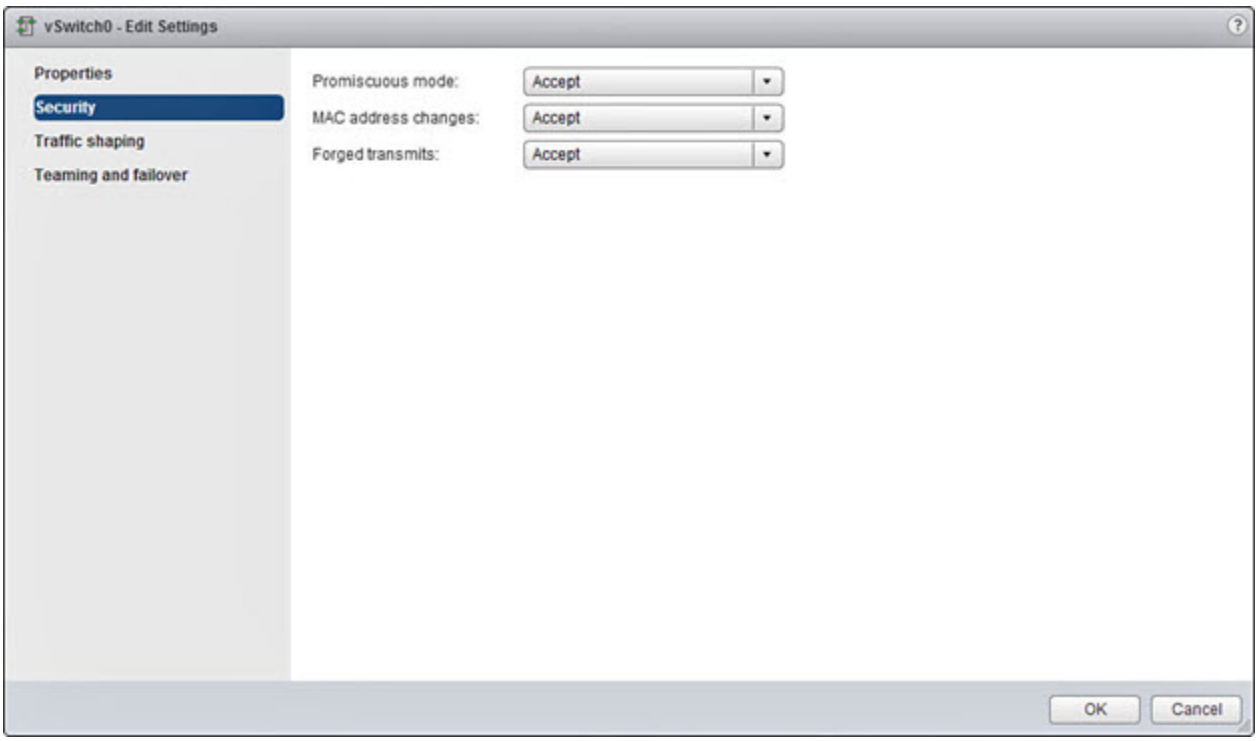
Option	Paramètre requis	Action
Mode de proximité	Accepter	Vous devez modifier la politique de sécurité d'un commutateur standard vSphere dans le client Web vSphere et définir l'option du mode de proximité (Promiscuous mode) sur Accept pour l'accepter. Les pare-feu, les analyses de ports, les systèmes 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.

Utilisez la procédure suivante pour configurer les paramètres par défaut pour le bon fonctionnement de défense contre les menaces virtuelles.

1. Dans le client web vSphere, accédez à la grappe HyperFlex.
2. Dans l'onglet **Manage** (gérer), sélectionnez **Networking** (mise en réseau), puis **Virtual switches** (commutateurs virtuels).
3. Sélectionnez un commutateur standard dans la liste et cliquez sur **Edit settings** (modifier les paramètres).
4. Sélectionnez **Security** (sécurité) et affichez les paramètres actuels.

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



6. Cliquez sur **OK**.

Remarque 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.

Documents connexes

Notes de version pour la plateforme de données Cisco HX

Guides de configuration de la plateforme de données Cisco HX

Cisco HyperFlex 4.0 pour l'infrastructure de serveur virtuel avec VMware ESXi

Aperçu des solutions des systèmes HyperFlex de Cisco

La feuille de route de la documentation des systèmes Cisco HyperFlex

Gestion du périphérique Cisco Secure Firewall Threat Defense Virtual

Vous avez deux options pour gérer votre Cisco Secure Firewall Threat Defense Virtual.

Cisco Secure Firewall Management Center

Si vous gérez un grand nombre d'appareils, ou si vous voulez utiliser les fonctions et configurations plus complexes que permet défense contre les menaces, utilisez centre de gestion pour configurer vos appareils au lieu du gestionnaire d'appareil intégré.

Important Vous ne pouvez pas utiliser à la fois gestionnaire d'appareil et centre de gestion pour gérer l'appareil défense contre les menaces. Une fois que la gestion intégrée gestionnaire d'appareil est activée, il ne sera plus possible d'utiliser centre de gestion pour gérer le périphérique défense contre les menaces, à moins de désactiver la gestion locale et de reconfigurer la gestion pour utiliser centre de gestion. D'un autre côté, lorsque vous enregistrez le périphérique défense contre les menaces sur centre de gestion, le service de gestion intégrée gestionnaire d'appareil est désactivé.

Mise en garde Actuellement, Cisco n'offre pas la possibilité de migrer votre configuration gestionnaire d'appareil vers centre de gestion et vice versa. Tenez-en compte lorsque vous choisissez le type de gestion que vous configurez pour le périphérique défense contre les menaces.

Cisco Secure Firewall device manager

Le gestionnaire d'appareil est un gestionnaire intégré.

Le gestionnaire d'appareil est une interface de configuration Web incluse sur certains des périphériques défense contre les menaces. gestionnaire d'appareil vous permet de configurer les fonctions de base du logiciel qui sont le plus souvent utilisées pour les petits réseaux. Il est spécialement conçu pour les réseaux qui comprennent un seul périphérique ou quelques-uns, pour lesquels vous ne souhaitez pas utiliser un gestionnaire de périphériques multiples de grande puissance qui permet de contrôler un grand réseau contenant un grand nombre des périphériques défense contre les menaces.

Remarque Consultez Guide Cisco Secure Firewall Device Manager Configuration pour obtenir la liste des périphériques défense contre les menaces qui prennent en charge gestionnaire d'appareil.

Aperçu

Vous pouvez déployer défense contre les menaces virtuelles sur Cisco HyperFlex sur un serveur VMware vCenter.

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 Cisco HyperFlex 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 propose plusieurs façons de provisionner les machines virtuelles vSphere. La méthode optimale pour votre environnement dépend de la taille et du type de votre infrastructure et des objectifs que vous souhaitez atteindre.

Vous pouvez utiliser le client Web VMware vSphere pour accéder à votre environnement Cisco HyperFlex.

Déployer l'Défense contre les menaces virtuelles

Utilisez cette procédure pour déployer l'appareil défense contre les menaces virtuelles sur Cisco HyperFlex sur un serveur vSphere vCenter Server.

Avant de commencer

- Assurez-vous d'avoir déployé Cisco HyperFlex et effectué toutes les tâches de configuration consécutives à l'installation. Pour en savoir plus, consultez la feuille de route de la documentation des systèmes Cisco HyperFlex.
- Vous devez avoir au moins un réseau configuré dans vSphere (pour la gestion) avant de déployer le défense contre les menaces virtuelles.
- Téléchargez le fichier de modèle VI OVF défense contre les menaces virtuelles à partir de Cisco.com : *Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*, où *X.X.X-xxx* est la version et le numéro de version.

Procédure

Étape 1 Connectez-vous au client Web vSphere.

Étape 2 Sélectionnez la grappe HyperFlex dans laquelle vous souhaitez déployer le défense contre les menaces virtuelles, et cliquez sur **ACTIONS** > **Deploy OVF Template (déployer le modèle OVF)**.

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 Précisez un nom et un emplacement pour le défense contre les menaces virtuelles, et cliquez sur **NEXT** (suivant).

Étape 5 Sélectionnez une ressource de traitement informatique et attendez la vérification de compatibilité.

Si la vérification de compatibilité réussit, cliquez sur **NEXT** (suivant).

Étape 6 Passez en revue 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 Passez en revue et acceptez le contrat de licence qui accompagne le modèle OVF (modèles VI uniquement), puis cliquez sur **NEXT** (suivant).

Étape 8 Sélectionnez une configuration de déploiement (valeurs de vCPU/mémoire) et cliquez sur **NEXT** (suivant).

Étape 9 Sélectionnez un emplacement de stockage et un format de disque virtuel, puis cliquez sur **NEXT** (suivant).

Dans cette fenêtre, sélectionnez parmi les banques de données déjà configurées dans la grappe HyperFlex de destination. Le fichier de configuration de la machine virtuelle et les fichiers de disque virtuel qui sont stockés dans le magasin de données. Sélectionnez une banque de données de taille suffisante pour contenir la machine virtuelle et tous ses fichiers de disque virtuel.

Lorsque vous sélectionnez **Thick Provisioned** (grand provisionnement) comme format de disque virtuel, tout l'espace de stockage est immédiatement attribué. Lorsque vous sélectionnez**Thin Provisioned**(provisionnement léger) comme format de disque virtuel, 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 10 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 associée 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.

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) :

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	Date interne
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	Réseaux sources	Réseaux de destination	Fonction
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 les défense contre les menaces virtuelles interfaces; 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 11 Définissez les propriétés configurables par l'utilisateur fournies avec le modèle OVF :

Remarque
Nous vous recommandons de configurer toutes les personnalisations requises à cette étape. Si vous n'avez pas configuré toutes les personnalisations requises, vous devez terminer la configuration après le déploiement à l'aide de l'interface de ligne de commande. Pour plus d'informations sur les instructions, consultez Terminer la configuration de Défense contre les menaces virtuelles à l'aide de l'interface de ligne de commande, à la page 13

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 ou IPv6).

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 le centre de gestion pour gérer cet appareil.

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) **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 **Firepower Management Center (FMC)**. 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 (-).

f) Cliquez sur **NEXT** (suivant).

Étape 12 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.

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 virtuelle défense contre les menaces virtuelles s'affiche sous le centre de données précisé 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 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.

Remarque Si vous n'avez pas configuré toutes les personnalisations requises lors du déploiement de défense contre les menaces virtuelles, vous devez terminer la configuration à l'aide de l'interface de ligne de commande. Pour plus d'informations sur les instructions, consultez Terminer la configuration de Défense contre les menaces virtuelles à l'aide de l'interface de ligne de commande, à la page 13

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

Si vous n'avez pas configuré toutes les personnalisations requises lors du déploiement de défense contre les menaces virtuelles, vous devez terminer la configuration à l'aide de l'interface de ligne de commande.

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 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 ou IPv6
- Paramètres DHCP IPv4 ou IPv6
- Adresse IPv4 et filtre d'adresse locale du port de gestion, ou adresse et préfixe IPv6.
- 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 été établie lorsque la console revient à l'invite #.

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.

Activation des trames étendues

Une MTU plus grande vous permet d'envoyer des paquets plus volumineux. Des paquets plus volumineux pourraient être plus efficaces pour votre réseau. Consultez les consignes suivantes :

- Correspondance des MTU sur le chemin de trafic : nous vous recommandons de définir la MTU sur toutes les interfaces d'ASAv et les autres interfaces de périphériques le long du chemin de trafic. La correspondance des MTU empêche les périphériques intermédiaires de fragmenter les paquets.
- Prise en charge des bâtis grand format : vous pouvez définir la MTU à 9 198 octets maximum. Le maximum est de 9 000 pour l'ASAv.

Cette procédure explique comment activer les bâtis grand format dans l'environnement suivant :

HyperFlex Cluster on the vSphere 7.0.1 (grappe HyperFlex sur vSphere 7.0.1) > **VMware vSphere vSwitch**> **Cisco UCS Fabric Interconnects (FI) (interconnexions de trames Cisco UCS).**

Procédure

Étape 1 Modifiez les paramètres MTU de l'hôte ASAv sur lequel vous avez déployé l'ASAv.

1. Connectez-vous au serveur vCenter à l'aide du client web vSphere.
2. Dans les **Advanced System Settings** (paramètres système avancés) de votre hôte HyperFlex, définissez la valeur du paramètre de configuration`Net.Vmxnet3NonTsoPacketGtMtuAllowed` sur `1`.
3. Enregistrez les modifications et redémarrez l'hôte.

Pour en savoir plus, consultez https://kb.vmware.com/s/article/1038578.

Étape 2 Modifiez les paramètres MTU de VMware vSphere vSwitch.

1. Connectez-vous au serveur vCenter à l'aide du client web vSphere.
2. Modifiez les propriétés de VMware vSphere vSwitch et définissez la valeur de la **MTU** à `9 000`.

Étape 3 Modifiez les paramètres MTU de Cisco UCS Fabric Interconnects (FI).

1. Connectez-vous à la console de gestion Cisco UCS.
2. Pour modifier la classe du système QoS, sélectionnez **LAN** > **LAN Cloud (nuage LAN)** > **QoS System Class (classe du système QoS).** Sous l'onglet **General** (général), définissez la valeur de la **MTU** à 9 216.
3. Pour modifier votre vNIC, choisissez **LAN** > **Policies (politiques)** > **racine (racine)** > **Sub-Organisations (sous-organisations)**

   <your-hyperflex-org>**vNIC Templates (modèles vNIC)** <your-vnic>. Sous l'onglet **General (général)**, définissez la valeur de la **MTU** à 9 000.

Dépannage

Cette section décrit des étapes de dépannage de base liées à votre déploiement Hyperflex sur votre machine virtuelle.

Vérifiez si votre machine virtuelle exécute HyperFlex

Si l'appareil défense contre les menaces virtuelles est installé sur HyperFlex avec ESX OS, la politique de haute accessibilité vSphere par défaut créée par le script HX post_install provoque un message d'erreur lorsque défense contre les menaces virtuelles est sous tension. Le message d'erreur est le suivant :

« Power on Failures: Insufficient resources to satisfy configured failover level for vSphere HA », ce qui signifie que les ressources sont insuffisantes pour satisfaire au niveau de basculement configuré pour la haute accessibilité de vSphere.

Solution de rechange

1. Dans VMware vCenter, accédez à **HX cluster (grappe HX)** > **Configure (configurer)** > **vSphere Availability (disponibilité de vSphere)** > **Edit Vsphere HA (modifier la haute accessibilité de Vsphere)** > **Admission Control (contrôle d'admission)** > **Define host failover capacity (définir la capacité de basculement de l'hôte)** > **Override calculated failover capacity (déterminer la capacité de basculement calculée)**.
2. Modifier et régler le CPU de basculement réservé et le pourcentage de capacité de mémoire.
3. Mettez la machine virtuelle défense contre les menaces virtuelles sous tension.

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.