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

Ce chapitre décrit la marche à suivre pour déployer défense contre les menaces virtuelles dans un environnement KVM.

Aperçu

KVM est une solution de virtualisation complète pour Linux sur du matériel x86 contenant des extensions de virtualisation (comme Intel VT). Il se compose d'un module de noyau chargeable, kvm.ko, qui fournit l'infrastructure de virtualisation de base et d'un module propre au processeur, tel que kvm-intel.ko.

Vous pouvez exécuter plusieurs machines virtuelles avec des images de système d'exploitation non modifiées. Chaque machine virtuelle dispose d'un matériel virtualisé privé : une carte réseau, un disque, un adaptateur graphique, etc.

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 1 : 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

Niveau de performance	Caractéristiques du périphérique (cœur/RAM)	Limite du débit	Limite de session RA VPN
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 l'octroi de licences pour le système des documents sur le *centre de gestion Secure Firewall Management Center Configuration* et sur la pour obtenir des instructions relatives à la licence de votre périphérique défense contre les menaces virtuelles.

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.

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 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.
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.

Paramètres	Valeur
	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.
Taille provisionnée du disque dur	• 50 Go • Paramètre réglable. Prend en charge les périphériques Virtio Block
Cartes vNIC	Le défense contre les menaces virtuelles sur KVM prend en charge les adaptateurs de réseau virtuels suivants : • **VIRTIO** : Virtio est la principale plateforme de virtualisation des E/S dans KVM et fournit un cadre commun pour les hyperviseurs pour la virtualisation des E/S. L'implémentation de l'hôte se trouve dans l'espace utilisateur - qemu, donc aucun pilote n'est nécessaire dans l'hôte. • **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.

Lignes directrices et limites relatives à la licence

- Nécessite deux interfaces de gestion et deux interfaces de données pour le démarrage.

Remarque La configuration par défaut défense contre les menaces virtuelles place l'interface de gestion, l'interface de diagnostic et l'interface interne sur le même sous-réseau.

  - Prend en charge les pilotes virtIO.
  - Prend en charge les pilotes ixgbe-vf pour SR-IOV.
  - Prend en charge un total de 11 interfaces.

- La configuration par défaut de défense contre les menaces virtuelles suppose que vous placiez les interfaces de gestion (gestion et diagnostic) et les interfaces internes sur le **même sous-réseau** et que l'adresse de gestion utilise l'adresse interne comme passerelle vers Internet (en passant par l'interface externe).

- Le défense contre les menaces virtuelles doit être sous tension sur Firstboot avec au moins quatre interfaces. Votre système ne sera pas déployé sans quatre interfaces
- Le défense contre les menaces virtuelles prend en charge un total de 11 interfaces : une interface de gestion, une interface de diagnostic et un maximum de 9 interfaces réseau pour le trafic de données. Les affectations interface-réseau doivent être ordonnées comme suit :
  - Interface de gestion (1) (obligatoire)

Remarque Dans la version 6.7 et 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 à centre de gestion, consultez la commande **configure network management-data-interface** dans la référence de commande FTD.

  - Interface de diagnostic (2) (obligatoire)
  - Interface externe (3) (obligatoire)
  - Interface interne (4) (obligatoire)
  - Interfaces de données (5-11) (facultatif)

Consultez la concordance suivante concernant l'adaptateur réseau, les réseaux sources et les réseaux de destination pour les interfaces défense contre les menaces virtuelles :

Tableau 3 : Mappage du réseau source au réseau de destination

Adaptateur réseau	Réseau source	Réseau de destination	Fonction
vnic0*	Gestion 0-0	Gestion 0/0	Gestion
vnic1*	Diagnostic 0-0	Diagnostic 0/0	Diagnostic
vnic2	GigabitEthernet 0-0	GigabitEthernet 0/0	Externe
vnic3*	GigabitEthernet 0-1	GigabitEthernet 0/1	Interne
* important. * Attaché au même sous-réseau.			

- Le clonage d'une machine virtuelle n'est pas pris en charge.
- Pour l'accès depuis la console, le serveur de terminaux est pris en charge par Telnet.

Mode CPU

KVM peut émuler différents types de processeur (ou CPU). Pour votre machine virtuelle (ou VM), vous devez généralement sélectionner un type de processeur qui correspond étroitement au CPU du système hôte, car

cela signifie que les fonctionnalités du processeur de l'hôte (également appelées indicateurs du CPU) seront disponibles dans vos machines virtuelles. Vous devez définir le type de CPU selon l'hôte (**host**), afin que la machine virtuelle présente exactement les mêmes indicateurs d'unité centrale que votre système hôte.

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 KVM. Pour en savoir plus, consultez l'information sur la mise en grappes pour Threat Defense Virtual dans un nuage privé.

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 KVM 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.

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.

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

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 Intel pour serveur Ethernet X710
  - Adaptateur pour serveur Ethernet Intel X520, DA2
  - Adaptateur de réseau Ethernet Intel E810-CQDA2
    - Le micrologiciel (image NVM) et le pilote réseau sont mis à jour sur l'adaptateur réseau Intel® E810 à l'aide d'un outil utilitaire NVM. L'image et le pilote réseau de mémoire non volatile (NVM) sont un ensemble de composants compatibles que vous mettez à jour en tant que combinaison sur l'adaptateur réseau Intel® E810. Pour en savoir plus sur la matrice de compatibilité de NVM et de logiciel, consultez la fiche technique du contrôleur Ethernet Intel® E810 pour mettre à jour les pilotes de micrologiciel appropriés sur l'adaptateur réseau Intel® E810.
- 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.
  - Les 8 cœurs doivent se trouver sur 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. Pour KVM, vous pouvez vérifier la compatibilité du processeur pour la prise en charge de SR-IOV support. Notez que pour le défense contre les menaces virtuelles sur KVM, nous prenons uniquement en charge le matériel x86.

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) jumelée, 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.

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.

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.

Conditions préalables

- Téléchargez le fichier qcow2 défense contre les menaces virtuelles à partir de Cisco.com et placez-le sur votre hôte Linux :

  https://software.cisco.com/download/navigator.html

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

- Aux fins de l'exemple de déploiement présenté dans ce document, nous supposons que vous utilisez Ubuntu 18.04 LTS. Installez les paquets suivants sur l'hôte Ubuntu 18.04 LTS :
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- L'hôte et sa configuration influent sur les performances. Vous pouvez maximiser le débit de défense contre les menaces virtuelles sur KVM en réglant votre hôte. Pour les concepts génériques de réglage d'hôte, consultez l'information sur la virtualisation de la fonction réseau : qualité de service dans des serveurs d'accès à distance à large bande avec l'architecture Linux et Intel.
- Voici des optimisations utiles pour Ubuntu 18.04 LTS :
  - macvtap : pont Linux à haute performance; vous pouvez utiliser macvtap au lieu d'un pont Linux. Notez que vous devez configurer des paramètres précis pour utiliser macvtap au lieu du pont Linux.
  - Transparent Huge Pages : augmente la taille des pages de mémoire et est activé par défaut dans Ubuntu 18.04.
  - Hyperthread désactivé : réduit deux vCPU en un seul cœur.
  - txqueuelength : augmente la longueur de la file d'attente par défaut à 4 000 paquets et réduit le taux d'abandon.
  - épinglage : applique des processus qemu et vhost à des cœurs de CPU spécifiques; dans certaines conditions, l'épinglage augmente considérablement les performances.

- Pour en savoir plus sur l'optimisation d'une distribution basée sur RHEL, consultez le Guide de réglage et d'optimisation de la virtualisation Red Hat Enterprise Linux6.
- Pour la compatibilité de KVM et du système, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense.
- Vous pouvez utiliser les méthodes suivantes pour vérifier si votre machine virtuelle exécute KVM :
  - Exécutez la commande **lsmod** pour répertorier les modules dans le noyau Linux. Si le KVM est en cours d'exécution, il est indiqué par l'affichage de la sortie suivante :

    root@kvm-host:~$ lsmod | grep kvm

    kvm_intel 123675 0

    kvm 257361 1 kvm_intel

- Si la commande **ls -l /dev/kvm** n'existe pas sur la machine virtuelle cible, vous exécutez probablement **qemu**, et ne tirez pas parti des fonctionnalités d'assistance matérielle de KVM.

  root@kvm-host: ~$ ls -l /dev/kvm

  crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm

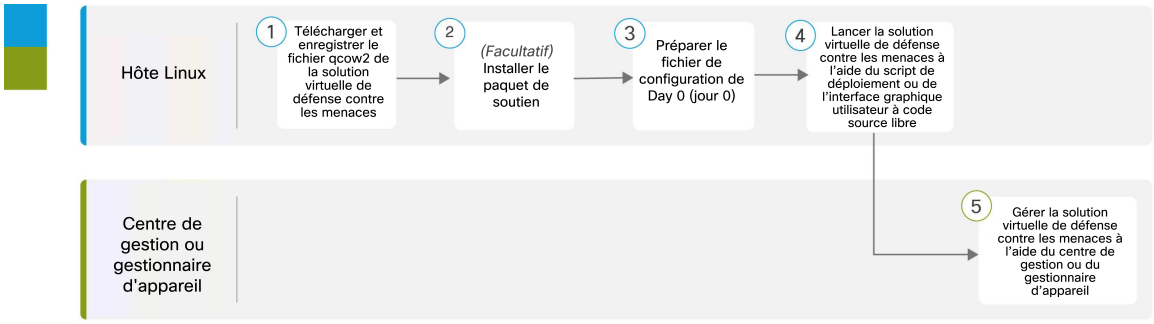
- Exécutez la commande suivante pour vérifier également si la machine hôte prend en charge KVM :

  root@kvm-host:~$ sudo kvm-ok

- Vous pouvez également utiliser l'accélération KVM.

Procédure de bout en bout

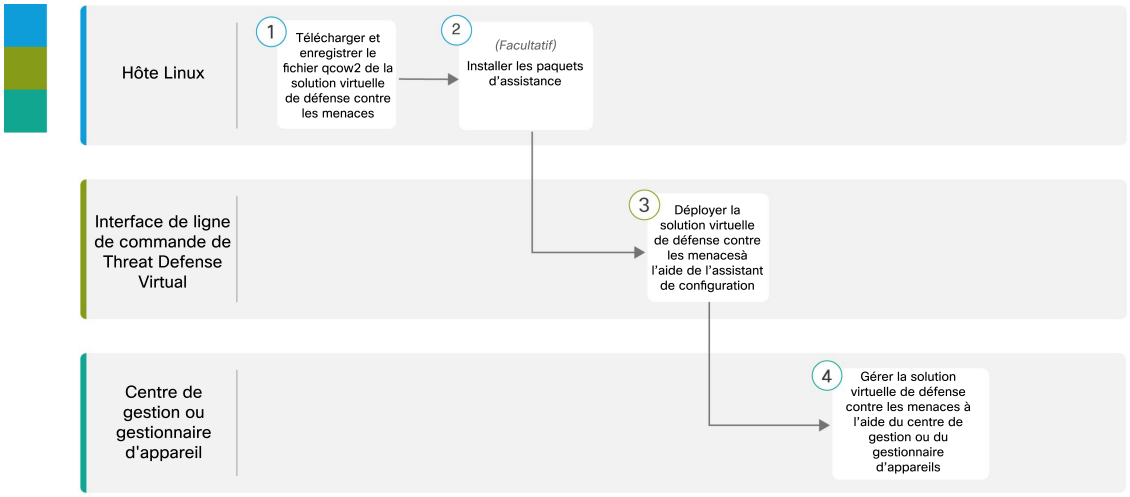
Le diagramme suivant illustre le flux de travail pour le déploiement de défense contre les menaces virtuelles sur une instance KVM à l'aide d'un fichier de configuration de Jour 0.



	Espace de travail	Étapes
1	Hôte Linux	Conditions préalables, à la page 9 : Téléchargez et enregistrez le fichier défense contre les menaces virtuelles qcow2 sur l'hôte Linux.
2	Hôte Linux	Conditions préalables, à la page 9 : Installez les paquets de soutien.

	Espace de travail	Étapes
3	Hôte Linux	Préparer le fichier de configuration Day 0 (jour 0)
4	Hôte Linux	Lancez défense contre les menaces virtuelles : • Utiliser un script de déploiement • Utiliser une interface graphique
5	Centre de gestion	Gérez défense contre les menaces virtuelles à l'aide du centre de gestion.

Le diagramme suivant illustre le flux de travail pour le déploiement de défense contre les menaces virtuelles sur une instance KVM à l'aide d'un fichier de configuration de Jour 0.



	Espace de travail	Étapes
1	Hôte Linux	Conditions préalables, à la page 9 : Téléchargez et enregistrez le fichier défense contre les menaces virtuelles qcow2 sur l'hôte Linux.
2	Hôte Linux	Conditions préalables, à la page 9 : Installez les paquets de soutien.
3	CLI Défense contre les menaces virtuelles	Lancement sans le fichier de configuration de jour 0 : déployez défense contre les menaces virtuelles à l'aide de l'assistant de configuration.
4	Centre de gestion	Gérez défense contre les menaces virtuelles à l'aide du centre de gestion

Préparer le fichier de configuration Day 0 (jour 0)

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.

  Vous pouvez soit définir **ManageLocally (gestion locale)** sur **Yes (oui)**, soit saisir des 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.
- Le mode de pare-feu initial; définit le mode de pare-feu initial, **routed** (avec routage) ou **transparent**.

  Si vous prévoyez de gérer votre déploiement à l'aide du gestionnaire d'appareil local, vous ne pouvez entrer que **routed** (avec routage) pour le mode de pare-feu. Vous ne pouvez pas configurer des interfaces en mode pare-feu transparent à l'aide du gestionnaire d'appareil.
- 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 mode grappes ou en mode autonome.

Si vous déployez sans fichier de configuration de jour 0, vous devez configurer les paramètres requis par le système après le lancement; consultez Lancement sans le fichier de configuration Day 0 (jour 0), à la page 19 pour de plus amples renseignements.

Remarque Nous utilisons Linux dans cet exemple, mais il existe des utilitaires similaires pour Windows.

SUMMARY STEPS

1. Saisissez la configuration CLI pour le défense contre les menaces virtuelles dans un fichier texte appelé « day0-config ». Ajoutez des paramètres réseau et des informations sur la gestion du centre de gestion.
2. Générez le CD-ROM virtuel en convertissant le fichier texte en fichier ISO :

3. Répétez les étapes pour créer des fichiers de configuration par défaut uniques pour chaque gestionnaire d'appareil que vous souhaitez déployer.

DETAILED STEPS

Procédure

Étape 1 Saisissez la configuration CLI pour le défense contre les menaces virtuelles dans un fichier texte appelé « day0-config ». Ajoutez des paramètres réseau et des informations sur la gestion du centre de gestion.

Exemple :

```
#Firepower Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "r2M$9^Uk69##",
    "FirewallMode": "routed",
    "DNS1": "1.1.1.1",
    "DNS2": "1.1.1.2",
    "DNS3": "",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.44",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"No"
}
```

Entrez **Yes** (oui) pour **ManageLocally** dans votre fichier de configuration de la journée 0 (Day 0) pour utiliser le gestionnaire d'appareil local; ou renseignez les champs du centre de gestion (**FmcIp**, **FmcRegKey**et **FmcNatId**). Pour l'option de gestion que vous n'utilisez pas, laissez ces champs vides.

Étape 2 Générez le CD-ROM virtuel en convertissant le fichier texte en fichier ISO :

Exemple :

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

ou

Exemple :

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

Étape 3 Répétez les étapes pour créer des fichiers de configuration par défaut uniques pour chaque gestionnaire d'appareil que vous souhaitez déployer.

Prochaine étape

- Si vous utilisez virt-install, ajoutez la ligne suivante à la commande virt-install :

```
--disk path=/home/user/day0.iso,format=iso,device=cdrom \
```

- Si vous utilisez virt-manager, vous pouvez créer un CD-ROM virtuel à l'aide de l'interface graphique utilisateur virt-manager; voir Lancement avec une interface utilisateur graphique (GUI), à la page 16.

Lancez le Défense contre les menaces virtuelles

Lancer à l'aide d'un script de déploiement

Utilisez un script de déploiement basé sur virt-install pour lancer défense contre les menaces virtuelles.

Sachez que vous pouvez optimiser les performances en sélectionnant le meilleur mode de mise en cache des invités pour votre environnement. Le mode de mise en cache utilisé aura une incidence sur la perte de données; il peut également influer sur les performances du disque.

Chaque interface de disque invité KVM peut avoir l'un des modes de mise en cache suivants : *writethrough*, *writeback*, *none* (aucun), *directsync* (synchronisation directe) et *unsafe* (non sécurisé). *writethrough* fournit une mise en cache de lecture. *writeback* fournit une mise en cache de lecture et d'écriture. *directsync* contourne le mise en cache de la page hôte. *unsafe* peut mettre en cache tout le contenu et ignorer les demandes de purge de l'invité.

- Le mode *cache=writethrough* réduira la corruption de fichiers sur les machines invitées KVM lorsque l'hôte subit des pertes de puissance subites. Nous vous recommandons d'utiliser le mode *writethrough*.
- Cependant, *cache=writethrough* peut également influer sur les performances du disque en raison de plus grand nombre d'écritures d'E/S sur le disque que *cache=none*.
- Si vous supprimez le paramètre de mise en cache sur l'option *--disk*, la valeur par défaut est *writethrough*.
- Ne pas préciser d'option de mise en cache peut également réduire considérablement le temps nécessaire à la création de la machine virtuelle. Cela est causé par le fait que certains contrôleurs RAID plus anciens ont une mauvaise capacité de mise en cache de disque. Par conséquent, la désactivation de la mise en cache du disque (*cache=none*) et l'utilisation par défaut de l'écriture *writethrough* contribuent à l'intégrité des données.
- À compter de 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. Consultez le tableau suivant pour connaître les niveaux de performance et les valeurs pris en charge pour les paramètres vcpus et ram pour chaque taille de plateforme défense contre les menaces virtuelles.

Tableau 4 : Paramètres de vCPU et de mémoire pris en charge pour virt-install

--vcpus	--ram	Taille de la plateforme Défense contre les menaces virtuelles
4	8192	4vCPU/8 Go (par défaut)
8	16384	8vCPU/16 Go
12	24576	12vCPU/24 Go

Procédure

Étape 1 Créez un script virt-install appelé « virt_install_ftdv.sh ».

Le nom de la machine virtuelle défense contre les menaces virtuelles doit être unique pour toutes les autres machines virtuelles (VM) sur cet hôte KVM. défense contre les menaces virtuelles peut prendre en charge jusqu'à 10 interfaces réseau. Cet exemple utilise quatre interfaces. La carte réseau virtuelle doit être VirtIO.

Remarque
La configuration par défaut défense contre les menaces virtuelles place l'interface de gestion, l'interface de diagnostic et l'interface interne sur le même **sous-réseau**. Le système nécessite au moins quatre interfaces pour démarrer avec succès. Les affectations interface-réseau doivent être ordonnées comme suit :

- (1) Interface de gestion (obligatoire)
- (2) interface de diagnostic (obligatoire)
- (3) Interface externe (obligatoire)
- (4) Interface interne (obligatoire)
- (5) (Facultatif) Interfaces de données, jusqu'à 6

Exemple :

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=ftdv \
   --arch=x86_64 \
   --cpu host \
   --vcpus=8 \
   --ram=16384 \
   --os-type=linux \
   --os-variant=generic26 \
   --virt-type=kvm \
   --import \
   --watchdog i6300esb,action=reset \
   --disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
   --disk path=<day0_filename>.iso,format=iso,device=cdrom \
   --console pty,target_type=serial \
   --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
   --force
```

Étape 2 Exécutez le script virt_install :

Exemple :

```
/usr/bin/virt_install_ftdv.sh

Starting install...
Creating domain...
```

Une fenêtre apparaît, affichant la console de la machine virtuelle. Vous pouvez voir que la machine virtuelle démarre. Le démarrage de la machine virtuelle prend quelques minutes. Une fois que le démarrage prend fin, vous pouvez exécuter des commandes de l'interface de ligne de commande à partir de l'écran de la console.

Prochaine étape

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

- Si vous avez choisi **No** (non) pour **Manage Locally**, vous utiliserez centre de gestion pour gérer votre défense contre les menaces virtuelles; voir 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.

Lancement avec une interface utilisateur graphique (GUI)

Plusieurs options à code source libre sont disponibles pour gérer les machines virtuelles KVM à l'aide d'une interface graphique. La procédure suivante utilise virt-manager, également appelé gestionnaire de machines virtuelles, pour lancer défense contre les menaces virtuelles. Le gestionnaire virt-manager est un outil graphique pour créer et gérer des machines virtuelles d'invités.

Remarque KVM peut émuler différents types de processeur (ou CPU). Pour votre machine virtuelle (ou VM), vous devez généralement sélectionner un type de processeur qui correspond étroitement au CPU du système hôte, car cela signifie que les fonctionnalités du processeur de l'hôte (également appelées indicateurs du CPU) seront disponibles dans vos machines virtuelles. Vous devez définir le type de CPU selon l'hôte (**host**), afin que la machine virtuelle présente exactement les mêmes indicateurs d'unité centrale que votre système hôte.

Procédure

Étape 1 Démarrez virt-manager en accédant à la section du gestionnaire de machines virtuelles dans les outils de système **(Applications** > **System Tools** > **Virtual Machine Manager**).

Il se peut que vous deviez sélectionner l'hyperviseur ou saisir votre mot de passe racine.

Étape 2 Cliquez sur le bouton dans le coin supérieur gauche pour ouvrir l'assistant **New VM** (nouvelle machine virtuelle).

Étape 3 Saisissez les détails de la machine virtuelle :

a) Pour le système d'exploitation, sélectionnez **Import exist disk image** (Importer une image de disque existante).

Cette méthode vous permet d'importer une image de disque (contenant un système d'exploitation préinstallé et amorçable).

b) Cliquez sur **Forward** pour continuer.

Étape 4 Chargez l'image disque :

a) Cliquez sur **Browse...** (parcourir) pour sélectionner le fichier d'image.

b) Choisissez *Generic* (général) pour le type de système d'exploitation (**OS type**).
c) Cliquez sur **Forward** pour continuer.

Étape 5 Configurer les options de mémoire et de CPU :

Important
À compter de la version 7.0 : défense contre les menaces virtuelles prend en charge les licences par niveau de performance qui procurent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement. Avant la version 7.0, défense contre les menaces virtuelles était déployé avec des options de configuration limitées vCPU/ mémoire; voir Configuration système requise, à la page 2.

Consultez le tableau suivant pour connaître les niveaux de performance et les valeurs pris en charge pour les paramètres vcpus et ram pour chaque plateforme défense contre les menaces virtuelles.

Tableau 5 : Paramètres de vCPU et de mémoire pris en charge pour Virtual Machine Manager

CPU	Mémoire	Taille de la plateforme Défense contre les menaces virtuelles
4	8192	4vCPU/8 Go (par défaut)
8	16384	8vCPU/16 Go
12	24576	12vCPU/24 Go

a) Définissez le paramètre de mémoire (**Memory (RAM)**) pour la taille de votre plateforme défense contre les menaces virtuelles.
b) Définissez le paramètre **CPU** correspondant à la taille de la plateforme défense contre les menaces virtuelles.
c) Cliquez sur **Forward** pour continuer.

Étape 6 Cochez la case **Customize configuration before install**(personnaliser la configuration avant l'installation), précisez un **nom**, puis cliquez sur **Finish** (terminer).

Cela ouvre un autre assistant qui vous permet d'ajouter, de supprimer et de configurer les paramètres matériels de la machine virtuelle.

Étape 7 Modifier la configuration de CPU

Dans le volet de gauche, sélectionnez **Processor** (processeur), puis sélectionnez **Configuration** > **Copy host CPU configuration** (copier la configuration CPU de l'hôte).

Ainsi, le modèle et la configuration de CPU de l'hôte physique sont appliqués à votre machine virtuelle.

Étape 8 Configurer le disque virtuel :

a) Dans le volet de gauche, sélectionnez **Disk 1** (disque 1).
b) Sélectionnez **Advanced options** (options avancées).
c) Définissez **Disk bus** en choisissant *Virtio*.
d) Définissez le format de stockage (**Storage format**) pour *qcow2*.

Étape 9 Configurer une console série :

a) Dans le volet de gauche, sélectionnez **Console**.
b) Sélectionnez **Remove** pour supprimer la console par défaut.
c) Cliquez sur **Add Hardware** (ajouter du matériel) pour ajouter un périphérique série.
d) Pour **Device Type** (type de périphérique), sélectionnez *TCP net console (tcp)*.

e) Pour **Mode**, sélectionnez *Server mode (bind)*, soit le mode liaison pour le serveur.
f) Pour l'hôte (**Host**), saisissez **0.0.0.0** pour l'adresse IP, puis saisissez un numéro de **Port** unique.
g) Cochez la case **Use Telnet** (utiliser Telnet) .
h) Configurer les paramètres de l'appareil

Étape 10 Configurez un périphérique de surveillance pour déclencher automatiquement une action lorsque l'invité KVM est suspendu ou planté :

a) Cliquez sur **Add Hardware** (ajouter du matériel) pour ajouter un périphérique de surveillance.
b) Pour **Model** (modèle), sélectionnez *default* (par défaut).
c) Pour **Action**, sélectionnez *Forcely reset the guest* (réinitialiser l'invité de manière forcée).

Étape 11 Configurez au moins quatre interfaces de réseau virtuel.

Cliquez sur **Add Hardware** (ajouter du matériel) pour ajouter une interface, puis choisissez **macvtap** ou indiquez un nom de périphérique partagé (utiliser un nom de pont).

Remarque
Le défense contre les menaces virtuelles sur KVM prend en charge un total de 11 interfaces : une interface de gestion, une une interface de diagnostic et un maximum de neuf interfaces réseau pour le trafic de données. Les affectations interface-réseau doivent être ordonnées comme suit :

vnic0 : interface de gestion (obligatoire)

vnic1 : interface de diagnostic (obligatoire)

vnic2 : interface externe (obligatoire)

vnic3 : interface interne (obligatoire)

vNIC4-10 : interfaces de données (facultatif)

Important
Assurez-vous que vnic0, vnic1 et vnic3 sont mappés au même sous-réseau.

Étape 12 Si vous déployez à l'aide d'un fichier de configuration de jour 0, créez un CD-ROM virtuel pour l'ISO :

a) Cliquez sur **Add Hardware** (ajouter du matériel).
b) Sélectionnez **Storage** (stockage).
c) Cliquez sur **Select managed or other existing storage** (sélectionner le stockage géré ou existant) et accédez à l'emplacement du fichier ISO.
d) Pour **Device type** (type d'appareil), sélectionnez *IDE CDROM*.

Étape 13 Après avoir configuré le matériel de la machine virtuelle, cliquez sur **Apply** (appliquer).

Étape 14 Cliquez sur **Begin installation** afin de commencer l'installation de virt-manager pour créer la machine virtuelle avec vos paramètres matériels précisés.

Prochaine étape

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

- Si vous avez choisi **No** (non) pour **ManageLocally**, vous utiliserez le centre de gestion pour gérer votre défense contre les menaces virtuelles; voir 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.

Lancement sans le fichier de configuration Day 0 (jour 0)

Étant donné que les appareils défense contre les menaces virtuelles n'ont pas d'interface Web , vous devez configurer un périphérique virtuel à l'aide de l'interface de ligne de commande si vous avez effectué un déploiement sans fichier de configuration Day 0 (jour 0).

Lorsque vous vous connectez pour la première fois à un périphérique nouvellement déployé, 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 indiquées entre crochets, par exemple [*y*]. Appuyez sur Enter (entrée) pour confirmer votre choix.

Remarque Pour modifier l'un de ces paramètres d'un appareil virtuel après avoir terminé la configuration initiale, vous devez utiliser l'interface de ligne de commande.

Procédure

Étape 1 Établissez une connexion console avec défense contre les menaces virtuelles.

Étape 2 À l'invite **firepower login** (connexion à Firepower), connectez-vous avec les identifiants par défaut : *admin* comme **username** (nom d'utilisateur) et *Admin123* comme **password** (mot de passe).

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 (gestion locale requise)

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).

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 #.

Étape 7 Fermez l'interface de ligne de commande.

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.

Dépannage

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

Vérifiez si votre machine virtuelle exécute KVM

Vous pouvez utiliser les méthodes suivantes pour vérifier si votre machine virtuelle exécute KVM :

- Exécutez la commande **lsmod** pour répertorier les modules dans le noyau Linux. Si le KVM est en cours d'exécution, il est indiqué par l'affichage de la sortie suivante :

  root@kvm-host:~$ lsmod | grep kvm

  kvm_intel 123675 0

  kvm 257361 1 kvm_intel

- Si la commande **ls -l /dev/kvm** n'existe pas sur la machine virtuelle cible, vous exécutez probablement **QEMU**, et ne tirez pas parti des fonctionnalités d'assistance matérielle de KVM.

  root@kvm-host: ~$ ls -l /dev/kvm

  crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm

- Exécutez la commande suivante pour vérifier également si la machine hôte prend en charge KVM :

  root@kvm-host:~$ sudo kvm-ok

- Vous pouvez également utiliser l'accélération KVM.

Expérimentation de boucles de démarrage lors du déploiement de Défense contre les menaces virtuelles

Vous devez vous assurer des éléments suivants si votre machine virtuelle connaît des boucles de démarrage :

- Assurez-vous de déployer la machine virtuelle avec au moins 8 Go de mémoire.
- Assurez-vous de déployer la machine virtuelle avec au moins quatre interfaces.
- Assurez-vous de déployer la machine virtuelle avec au moins quatre vCPU.

- Vérifiez que le processus de QEMU utilise une unité centrale (ou CPU) de classe de serveur, par exemple, SandyBridge, IvyBridge, Haswell, etc. Utilisez la commande suivante, **ps -edaf | grep qemu** pour inspecter les paramètres de processus.

Expérimentation de boucles de démarrage lors du déploiement de Centre de gestion virtuel

Vous devez vous assurer des éléments suivants si votre machine virtuelle connaît des boucles de démarrage :

- Assurez-vous de déployer la machine virtuelle avec au moins 28 Go de mémoire.
- Assurez-vous de déployer la machine virtuelle avec au moins quatre interfaces.
- Assurez-vous de déployer la machine virtuelle avec au moins quatre vCPU.
- Vérifiez que le processus de QEMU utilise une unité centrale (ou CPU) de classe de serveur, par exemple, SandyBridge, IvyBridge, Haswell, etc. Utilisez la commande suivante, **ps -edaf | grep qemu** pour inspecter les paramètres de processus.

Dépannage après le déploiement

Vous pouvez exécuter la commande suivante sur défense contre les menaces virtuelles pour vérifier les problèmes de capture de journaux pour le débogage, **system generate-troubleshoot <space> ALL**

Vous pouvez également utiliser **system generate-troubleshoot <space>**, suivi d'un point d'interrogation **(?)** ou le bouton **Tab** pour afficher l'option ou la commande possible.

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.