



Gestion de Cisco Secure Firewall Threat Defense Virtual avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Ce chapitre décrit comment déployer un périphérique défense contre les menaces virtuelles géré avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

- [Présentation de l'intégration, à la page 1](#)
- [Conditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center \(centre de gestion de pare-feu en nuage\), à la page 2](#)
- [Créer un détenteur CDO, à la page 4](#)
- [Intégrer un périphérique avec une clé d'enregistrement de ligne de commande, à la page 5](#)
- [Configurer une politique de sécurité de base, à la page 7](#)

Présentation de l'intégration

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est pris en charge sur les périphériques Threat Defense Virtual exécutant les versions de Cisco Secure Firewall 7.0.3, 7.2.0 et ultérieures. Pour voir toutes les versions prises en charge et la compatibilité des produits, consultez le [Guide de compatibilité Secure Firewall Threat Defense](#) pour plus d'informations.

Il existe trois types de scénarios différents dans lesquels vous intégrez un périphérique virtuel de défense contre les menaces dans le centre de gestion Cisco Firewall Management Center en nuage :

- Pour intégrer un nouveau périphérique virtuel de défense contre les menaces.
- Pour intégrer un périphérique virtuel de défense contre les menaces qui est actuellement géré par le gestionnaire d'appareils.



Remarque

Si vous intégrez un appareil géré par le gestionnaire d'appareils à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), vous ne pourrez plus gérer le périphérique avec le gestionnaire d'appareils.

- Pour intégrer un périphérique virtuel de défense contre les menaces qui est actuellement géré par un centre de gestion sur site. Consultez la section [Migration de Cisco Secure Firewall Threat Defense vers le nuage](#) pour en savoir plus.



Remarque

Les scénarios suivants se produisent lorsque vous déplacez ou migrez un périphérique vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

- Si vous supprimez un périphérique d'un centre de gestion sur site ou du gestionnaire de périphériques Cisco Secure Firewall Threat Defense pour l'intégrer à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), le changement de gestionnaires efface toutes les politiques configurées au moyen du centre de gestion sur site.
- Toutefois, si vous migrez un périphérique d'un centre de gestion sur site vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), le périphérique conserve la majorité de vos politiques précédemment configurées.

Si vous ne savez pas si votre périphérique est déjà géré par un autre gestionnaire, utilisez la commande **show managers** dans la l'interface de ligne de commande du périphérique.

Ce guide fournit des informations sur les bases de la gestion de Threat Defense Virtual à l'aide de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Pour de plus amples renseignements sur CDO, consultez [Cisco Defense Orchestrator](#).

Conditions préalables à l'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Limites et exigences de l'intégration

Gardez à l'esprit les limites suivantes lors de l'intégration d'un périphérique sur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) :

- Les périphériques **doivent** exécuter la version 7.0.3, ou la version 7.2, ou une version ultérieure. Nous vous recommandons **fortement** d'utiliser la version 7.2 ou une version ultérieure.
- Vous pouvez migrer une paire à haute accessibilité gérée par un Centre de gestion de pare-feu sur site en suivant le processus [Migration du FTD vers le Firewall Management Center en nuage](#). Confirmez que les deux homologues sont dans un état intègre avant la migration.
- Seuls les périphériques configurés pour la gestion locale et gérés par un gestionnaire d'appareil peuvent être intégrés avec le numéro de série et les méthodes provisionnement sans intervention.
- Si le périphérique est géré par un centre de gestion sur site, vous pouvez soit intégrer le périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), soit le faire

migrer. La migration conserve les politiques et les objets existants, tandis que l'intégration du périphérique supprime la plupart des politiques et tous les objets. Consultez la section [Migration du FTD vers le Firewall Management Center en nuage](#) pour de plus amples renseignements.

- Si votre appareil est actuellement géré par un gestionnaire d'appareil, désenregistrez toutes vos licences Smart avant d'intégrer le périphérique. Même si vous changez de gestion de périphériques, Cisco Smart Software Manager conserve les licences Smart.
- Si vous avez déjà intégré un appareil qui était géré par gestionnaire d'appareil et que vous avez supprimé le périphérique de CDO avec l'intention de le réintégrer pour la gestion dans le nuage, vous **devez** enregistrer gestionnaire d'appareil dans le nuage Security Services Exchange après avoir supprimé le périphérique. Reportez-vous au chapitre « Accès aux services de sécurité Exchange » du *Guide d'intégration de Firepower et Cisco SecureX Threat Response*.



Astuces

L'intégration d'un périphérique à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) supprime toutes les politiques et la plupart des objets configurés par le gestionnaire précédent. Si votre périphérique est actuellement géré par un centre de gestion sur site, il est possible de migrer le périphérique et de conserver vos politiques et vos objets. Consultez la section [Migration du FTD vers le Firewall Management Center en nuage](#) pour de plus amples renseignements.

Exigences en matière de réseau

Avant d'intégrer un périphérique, assurez-vous que les ports suivants ont un accès externe et sortant. Confirmez que les ports suivants du périphérique sont autorisés. Si les ports de communication sont bloqués derrière un pare-feu, l'intégration du périphérique peut échouer.



Remarque

Vous ne pouvez pas configurer ces ports dans l'interface utilisateur CDO. Vous devez activer ces ports via le protocole SSH du périphérique.

Tableau 1 : Configuration de ports requise pour l'appareil

Port	Protocole/Fonctionnalité	Détails
443/tcp	HTTPS	Envoyez et recevez des données d'Internet
443	HTTPS	Communiquez avec le nuage AMP (public ou privé)
8305/tcp	Communications concernant les périphériques	Communiquez en toute sécurité entre les périphériques d'un déploiement

Interfaces de gestion et de données

Assurez-vous que votre périphérique est correctement configuré avec une interface de gestion ou de données.

Créer un détenteur CDO

Vous pouvez provisionner un nouveau détenteur CDO pour intégrer et gérer vos périphériques. Si vous utilisez un Centre de gestion de pare-feu sur site version 7.2 ou ultérieure et que vous souhaitez l'intégrer au nuage de sécurité Cisco, vous pouvez également créer un détenteur CDO dans le cadre du flux de travail d'intégration.

Procédure

1. Accédez à <https://us.manage.security.cisco.com/provision>.
2. Sélectionnez la région dans laquelle vous souhaitez provisionner votre détenteur CDO et cliquez sur **Sign Up** (s'inscrire).
3. Dans la page **Security Cloud Sign On** (connexion au nuage de sécurité), donnez vos informations d'authentification.
4. Si vous n'avez pas de compte Connexion à Cisco Security Cloud et que vous souhaitez en créer un, cliquez sur **Sign up now** (s'inscrire maintenant).
 1. Présentez des informations sur le compte.

Account Sign Up

Provide following information to create enterprise account.

[Back to login page](#)

Email *

First name *

Last name *

Country *

Please select *

Password *

Confirm Password *

I agree to the [End User License Agreement and Privacy Statement](#).

[Cancel](#)

Voici quelques conseils :

- **Adresse courriel** : saisissez l'adresse courriel que vous utiliserez éventuellement pour vous connecter à CDO.
 - **Mot de passe** : saisissez un mot de passe fort.
2. Cliquez sur **Sign in** (connexion). Cisco vous envoie un courriel de vérification à l'adresse avec laquelle vous vous êtes inscrit.
 3. Ouvrez le courriel et cliquez sur **Activate Account** (activer le compte) dans le courriel et sur la page **Security Cloud Sign On** (signature de nuage de sécurité).
 4. Configurez l'authentification à facteurs multiples à l'aide de Duo sur un périphérique de votre choix et cliquez sur **Log in with Duo** (connecter avec Duo) et sur **Finish** (terminer).

**Remarque**

Nous vous recommandons d'installer l'application Duo Security sur un téléphone mobile. Consultez le guide Duo d'authentification à deux facteurs (guide d'inscription) ([Duo Guide to Two Factor Authentication: Enrollment Guide](#)) si vous avez des questions sur l'installation de Duo.

5. Attribuez un nom à votre détenteur et cliquez sur **Create New Account** (créer un nouveau compte).
6. Un nouveau détenteur CDO est créé dans la région que vous avez choisie; vous recevrez également un courriel concernant la création de votre détenteur CDO, avec les détails. Si vous êtes déjà associé à plusieurs détenteurs CDO, sur la page **Choose a tenant** (choisissez un détenteur), sélectionnez le détenteur que vous venez de créer pour vous y connecter. Si vous avez créé un nouveau détenteur CDO pour la première fois, vous êtes directement connecté à votre détenteur.

Intégrer un périphérique avec une clé d'enregistrement de ligne de commande

Utilisez la procédure ci-dessous pour intégrer un appareil à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) avec une clé d'enregistrement d'interface de ligne de commande.

**Remarque**


Si votre appareil est actuellement géré par un centre de gestion sur site, l'intégration du périphérique échouera. Vous pouvez soit supprimer le périphérique de centre de gestion sur site et l'intégrer en tant que nouveau périphérique sans politique ni objet, ou vous pouvez migrer le périphérique et conserver les politiques et les objets existants. Consultez la section [Migration de FTD vers le centre de gestion de pare-feu en nuage](#) pour de plus amples renseignements.

Avant de commencer

Avant d'intégrer un appareil, assurez-vous d'effectuer les tâches suivantes :

- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est activé pour votre détenteur.
- Le périphérique doit exécuter la version 7.0.3, ou 7.2.0, ou une version ultérieure.

Procédure

-
- Étape 1** Connectez-vous à CDO.
- Étape 2** Dans le volet gauche, cliquez sur (périphériques de sécurité).
- Étape 3** Dans le coin supérieur droit, cliquez sur **Onboard** (intégrer) ().
- Étape 4** Cliquez sur la fenêtre **FTD**.
- Étape 5** Sous **Management Mode** (mode de gestion), sélectionnez **FTD**. En sélectionnant **FTD** sous **Management Mode**, vous ne pourrez pas gérer le périphérique à l'aide de la plateforme de gestion précédente. Toutes les configurations de politiques existantes, à l'exception des configurations d'interface, seront réinitialisées. Vous devez reconfigurer les politiques après avoir intégré le périphérique.
- Étape 6** Sélectionnez **Use CLI Registration Key (Utiliser la clé d'enregistrement de l'interface de ligne de commande)** comme méthode de préparation.
- Étape 7** Saisissez un nom pour le périphérique dans le champ **Nom du périphérique** et cliquez sur **Suivant**.
- Étape 8** À l'étape d'affectation de politique (**Policy Assignment**), utilisez le menu déroulant pour sélectionner une politique de contrôle d'accès à déployer une fois que le périphérique est intégré. Si vous n'avez pas configuré de politique, sélectionnez la **politique de contrôle d'accès par défaut**.
- Étape 9** Précisez si le périphérique que vous intégrez est un périphérique physique ou virtuel. Si vous intégrez un appareil virtuel, vous devez sélectionner le niveau de performance du périphérique dans le menu déroulant.
- Étape 10** Sélectionnez les licences d'abonnement que vous souhaitez appliquer au périphérique. Cliquez sur **Next** (suivant).
- Étape 11** CDO génère une commande avec la clé d'enregistrement. Connectez-vous au périphérique que vous êtes en train d'intégrer à l'aide de SSH. Connectez-vous en tant qu'« admin » ou en tant qu'utilisateur doté de privilèges d'administrateur équivalents et collez la clé d'enregistrement complète telle quelle dans l'interface de ligne de commande du périphérique.
- Remarque :** Pour les périphériques Firepower 1000, Firepower 2100, ISA 3000 et défense contre les menaces virtuelles, ouvrez une connexion SSH avec le périphérique et connectez-vous en tant qu'administrateur. Copiez la commande d'enregistrement complète et collez-la dans l'interface CLI du périphérique à l'invite. Dans l'interface de ligne de commande, saisissez **Y** (Oui) pour terminer l'enregistrement. Si votre périphérique était auparavant géré par gestionnaire d'appareil, saisissez **Yes** (oui) pour confirmer la soumission.
- Étape 12** Cliquez sur **Next** (suivant) dans l'assistant d'intégration CDO.
- Étape 13** (Facultatif) Ajoutez des étiquettes à votre appareil pour trier et filtrer la page **Security Devices** (appareils de sécurité). Saisissez une étiquette et sélectionnez le bouton bleu Plus. Les étiquettes sont appliquées au périphérique après son intégration à CDO.

Prochaine étape

Une fois le périphérique synchronisé, dans la page des appareils de sécurité (**Security Devices**) sélectionnez le périphérique que vous venez d'intégrer et sélectionnez l'une des options répertoriées dans le volet **Device Management** (gestion des périphériques) situé à droite. Nous vous recommandons fortement d'effectuer les actions suivantes :

- Si vous ne l'avez pas encore fait, créez une politique de contrôle d'accès personnalisée pour adapter la sécurité à votre environnement. Consultez [le survol du contrôle d'accès](#) dans le document *Gestion de*

Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator pour obtenir de plus amples renseignements.

- Activez Cisco Security Analytics and Logging (SAL) pour afficher les événements dans le tableau de bord CDO **ou** enregistrez le périphérique sur un Cisco Secure Firewall Management Center pour des analyses de sécurité. Pour obtenir de plus amples renseignements sur [Cisco Security Analytics and Logging](#), consultez le guide *Gestion de Firewall Threat Defense avec Cisco Firewall Management Center en nuage dans Cisco Defense Orchestrator*.

Configurer une politique de sécurité de base

Cette section décrit comment configurer la politique de sécurité de base au moyen des paramètres importants suivants :

- Inside and outside interfaces (interfaces internes et externes) : Attribuez une adresse IP statique à l'interface interne et utilisez DHCP pour l'interface externe.
- DHCP server (serveur DHCP) : Utilisez un serveur DHCP sur l'interface interne pour les clients.
- Default route (voie de routage par défaut) : Ajoutez une voie de routage par défaut via l'interface externe.
- NAT : Utilisez l'interface PAT sur l'interface externe.
- Access control (contrôle d'accès) : Autorisez le trafic de l'intérieur vers l'extérieur.

Procédure

-
- Étape 1 [Interfaces de configuration](#)
 - Étape 2 [Configurer le serveur DHCP](#)
 - Étape 3 [Ajouter la voie de routage par défaut](#)
 - Étape 4 [Configurer la traduction d'adresses réseau \(NAT\)](#)
 - Étape 5 [Configurer le contrôle d'accès](#)
 - Étape 6 [Déployer la configuration](#)
-

Interfaces de configuration

Activez les interfaces défense contre les menaces virtuelles, affectez-les aux zones de sécurité et définissez les adresses IP. En règle générale, vous devez configurer au moins deux interfaces pour que le système transmette un trafic significatif. Normalement, vous auriez une interface externe qui fait face à Internet ou au routeur en amont, et une ou plusieurs interfaces internes pour les réseaux de votre entreprise. Certaines de ces interfaces peuvent être des «zones démilitarisées» (DMZ), où vous placez des ressources accessibles au public, comme votre serveur Web.

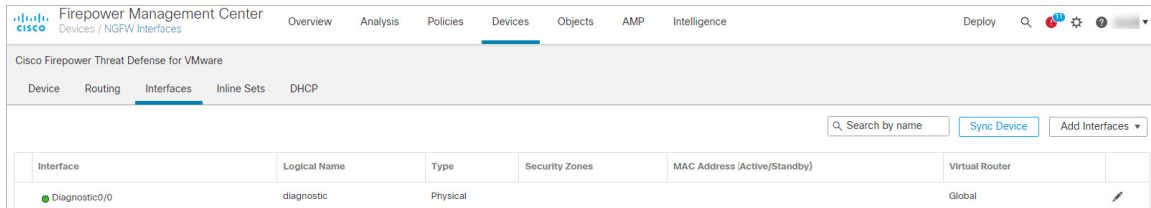
Une situation typique de routage de périphérie consiste à obtenir l'adresse de l'interface externe via DHCP auprès de votre fournisseur de services Internet, pendant que vous définissez des adresses statiques sur les interfaces internes.

Dans l'exemple suivant, une interface interne est configurée en mode routage avec une adresse statique et une interface externe est configurée en mode routage à l'aide de DHCP.

Procédure

Étape 1 Choisissez **Devices (périphériques) > Device Management (gestion de périphériques)**, puis cliquez sur **Modifier** (✎) pour le périphérique.

Étape 2 Cliquez sur **Interfaces**.



Étape 3 Cliquez sur **Modifier** (✎) pour l'interface que vous souhaitez utiliser à l'intérieur. L'onglet **General** (général) s'affiche.

Edit Physical Interface

General | IPV4 | IPV6 | Advanced | Hardware Configuration | FMC Access

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:
(64 - 9000)

Priority:
(0 - 65535)

Propagate Security Group Tag:

- a) Entrez un nom (**Name** (nom) renfermant au maximum 48 caractères.
Par exemple, nommez l'interface **interne**.
- b) Cochez la case **Enabled** (activer).
- c) Laissez le **Mode** défini sur **None** (aucun).

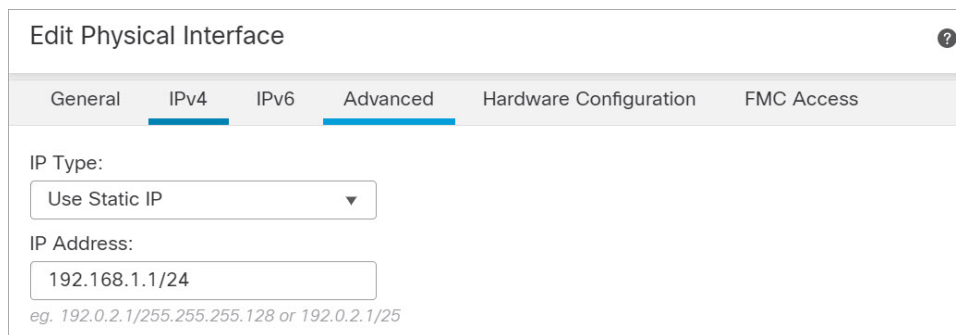
- d) Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité interne existante ou ajoutez-en une en cliquant sur **New** (nouveau).

Par exemple, ajoutez une zone appelée **inside_zone** (zone interne). Chaque interface doit être affectée à une zone de sécurité ou à un groupe d'interfaces. Une interface ne peut appartenir qu'à une seule zone de sécurité, mais peut également appartenir à plusieurs groupes d'interfaces. Vous appliquez votre politique de sécurité en fonction des zones ou des groupes. Par exemple, vous pouvez affecter l'interface interne à la zone interne; et l'interface externe avec la zone externe. Ensuite, vous pouvez configurer votre politique de contrôle d'accès pour permettre au trafic d'être acheminé de l'intérieur vers l'extérieur, mais pas de l'extérieur vers l'intérieur. La plupart des politiques ne prennent en charge que les zones de sécurité; vous pouvez utiliser des zones ou des groupes d'interface dans les politiques NAT, les politiques de préfiltre et les politiques QOS.

- e) Cliquez sur l'onglet **IPv4** ou .

- **IPv4** : Sélectionnez **Use Static IP** (utiliser une adresse IP statique) dans la liste déroulante et saisissez une adresse IP et un filtre d'adresse locale en notation oblique ou selon l'option DHCP.

Par exemple, entrez **192.168.1.1/24**.



The screenshot shows the 'Edit Physical Interface' configuration window. The 'IPv4' tab is selected. Under 'IP Type', 'Use Static IP' is chosen. The 'IP Address' field contains '192.168.1.1/24'. Below the field, a note reads: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

- f) Cliquez sur **OK**.

Étape 4

Cliquez sur **Modifier** (✎) pour l'interface que vous souhaitez utiliser à l'extérieur.

L'onglet **General** (général) s'affiche.

Edit Physical Interface

General IPv4 IPv6 Advanced Hardware Configuration FMC Access

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:

(0 - 65535)

Propagate Security Group Tag:

Cancel OK

- Entrez un nom (**Name** (nom)) renfermant au maximum 48 caractères.
 Par exemple, nommez l'interface **externe**.
- Cochez la case **Enabled** (activer).
- Laissez le **Mode** défini sur **None** (aucun).
- Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité externe existante ou ajoutez-en une en cliquant sur **New** (nouveau).
 Par exemple, ajoutez une zone appelée **outside_zone**.
- Cliquez sur l'onglet **IPv4** ou .
 - **IPv4** : Choisissez **Use DHCP** (utiliser DHCP) et configurez les paramètres facultatifs suivants :
 - **Obtain Default Route Using DHCP** (obtenir la voie de routage par défaut en utilisant DHCP) : Obtenir la voie de routage par défaut à partir du serveur DHCP.
 - **DHCP route metric** (mesure de la voie de routage DHCP) : Attribue une distance administrative à la voie de routage apprise (entre 1 et 255). La distance administrative par défaut pour les routes apprises est de 1.

Edit Physical Interface

General IPv4 IPv6 Advanced Hardware Configuration FMC Access

IP Type:
Use DHCP

Obtain default route using DHCP:

DHCP route metric:
1
(1 - 255)

f) Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (enregistrer).

Configurer le serveur DHCP



Remarque Ignorez cette procédure si vous procédez à un déploiement dans un environnement de nuage public tel qu’AWS, Azure, GCP, OCI.

Activez le serveur DHCP si vous souhaitez que les clients utilisent DHCP pour obtenir des adresses IP à partir de défense contre les menaces virtuelles.

Procédure

Étape 1 Choisissez **Devices (périphériques) > Device Management (gestion de périphériques)**, puis cliquez sur **Modifier** (✎) pour le périphérique.

Étape 2 Choisissez **DHCP > DHCP Server**.

Étape 3 Dans la page **Server** (serveur), cliquez sur **Add** (ajouter) puis configurez les options suivantes :

- **Interface** : Choisissez une interface dans la liste déroulante.
- **Address Pool** (ensemble des adresses) : Définissez la plage d'adresses IP (de la plus basse à la plus élevée) qu'utilise le serveur DHCP. La plage d'adresses IP doit se trouver sur le même sous-réseau que l'interface sélectionnée et elle ne peut pas inclure l'adresse IP de l'interface elle-même.
- **Enable DHCP Server** : Activez le serveur DHCP sur l'interface sélectionnée.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Save** (enregistrer).

Ajouter la voie de routage par défaut

La voie de routage par défaut s'oriente normalement vers le routeur en amont accessible de l'interface externe. Si vous utilisez DHCP pour l'interface externe, votre appareil a peut-être déjà reçu une voie de routage par défaut. Si vous devez ajouter la route manuellement, procédez comme suit.

Procédure

Étape 1 Choisissez **Devices (périphériques) > Device Management (gestion de périphériques)**, puis cliquez sur **Modifier** (✎) pour le périphérique.

Étape 2 Choisissez **Routing (routage) > Static Route (routage statique)**, cliquez sur **Add Route** (ajouter une voie de routage), puis définissez les paramètres suivants :

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
 Outside

(Interface starting with this icon signifies it is available for route leak)

Available Network + Selected Network

Q Search any-ipv4

any-ipv4
 any-IPv4-10.0.0.1
 IPv4-Benchmark-Tests
 IPv4-Link-Local
 IPv4-Multicast
 IPv4-Private-10.0.0.0-8

Ensure that egress virtualrouter has route to that destination

Gateway
 any-IPv4-10.0.0.1

Metric:
 1
 (1 - 254)

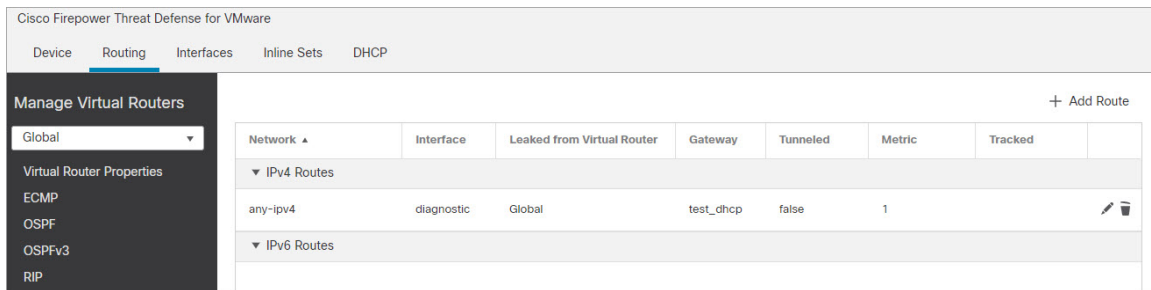
Tunneled: (Used only for default Route)

Route Tracking:

- **Type** : Cliquez sur le bouton radio **IPv4** selon le type de routage statique que vous ajoutez.
- **Interface** : Sélectionnez l'interface de sortie; il s'agit généralement de l'interface externe.
- **Available Network** (réseau disponible) : Choisissez **any-ipv4** pour une voie de routage IPv4 par défaut.
- **Gateway (passerelle)** : Saisissez ou choisissez le routeur de passerelle qui est le prochain saut sur cette voie de routage. Vous pouvez fournir une adresse IP ou un objet réseaux/hôtes.
- **Metric** (nombre) : Saisissez le nombre de sauts sur le réseau de destination. Les valeurs valides vont de 1 à 255; la valeur par défaut est 1.

Étape 3 Cliquez sur **OK**.

La voie est ajoutée à la table de routage statique.



Étape 4 Cliquez sur **Save** (enregistrer).

Configurer la traduction d'adresses réseau (NAT)

Une règle de NAT typique convertit les adresses internes en un port sur l'adresse IP de l'interface externe. Ce type de règle de NAT est appelé *interface Port Address Translation (PAT)*.

Procédure

Étape 1 Choisissez **Devices (périphériques) > NAT** et cliquez sur **New Policy (nouvelle politique) > Threat Defense NAT (NAT de défense contre les menaces)**.

Étape 2 Nommez la politique, sélectionnez le ou les périphériques pour lesquels vous souhaitez utiliser la politique et cliquez sur **Save** (enregistrer).

New Policy

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Q Search by name or value

FTDv 7.1.0 Build 1...

Selected Devices

FTDv 7.1.0 Build 1...

La politique est ajoutée le centre de gestion. Vous devez encore ajouter des règles à la politique.

Étape 3 Cliquez sur **Add Rule** (ajouter une règle).

La boîte de dialogue **Add NAT Rule** (ajouter une règle NAT) apparaît.

Étape 4 Configurez les options des règles de base :

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

- **NAT Rule** (règle NAT) : Choisissez la règle NAT automatique (**Auto NAT Rule**).
- **Type** : Choisissez **Dynamic** (dynamique).

Étape 5 Dans la page **Interface Objects** (objets d'interface), ajoutez la zone externe du champ **Available Interface Objects** (objets d'interface disponibles) dans la zone **Destination Interface Objects** (objets d'interface de destination).

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects Source Interface Objects (0) Destination Interface Objects (1)

Search by name

outside-zone Add to Source

Add to Destination

any

outside-zone

Cancel OK

Étape 6 Dans la page **Translation** (traduction), configurez les options suivantes :

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet Translated Packet

Original Source:*
any-IPv4-10.0.0.1 +

Translated Source:
Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Original Port:
TCP

Translated Port:

Cancel OK

- **Original Source (source d'origine)** : Cliquez sur **Ajoutez (+)** pour ajouter un objet réseau pour l'ensemble du trafic IPv4 (0.0.0.0/0).

New Network Object

Name
all-ipv4

Description

Network
 Host Range Network FQDN

0.0.0.0/0

Allow Overrides

Cancel Save

Remarque

Vous ne pouvez pas utiliser l'objet **any-ipv4** défini par le système, car les règles de NAT automatiques ajoutent la NAT dans la définition de l'objet, et vous ne pouvez pas modifier les objets définis par le système.

- **Translated Source** (source traduite) : Choisissez l'adresse IP de l'interface de destination (**Destination Interface IP**).

Étape 7 Cliquez sur **Save** (enregistrer) pour ajouter la règle.

La règle est enregistrée dans le tableau **Rules** (règles).

The screenshot shows the 'Interface_PAT' configuration page in the Firepower Management Center. The 'Rules' section is active, displaying a table of NAT rules. The table is organized into sections: 'NAT Rules Before', 'Auto NAT Rules', and 'NAT Rules After'. The 'Auto NAT Rules' section contains one rule with the following details:

Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
D...	any	outside-z	any-IPv4-10.0.1							Interface

Étape 8 Cliquez sur **Save** pour enregistrer vos modifications dans la page **NAT**.

Configurer le contrôle d'accès

Si vous avez créé une politique de contrôle d'accès de base de blocage de tout le trafic (**Block all traffic**) lors de votre inscription de défense contre les menaces virtuelles au centre de gestion, vous devez ajouter des règles à la politique pour autoriser le trafic sur l'appareil. La procédure suivante ajoute une règle pour autoriser le trafic de la zone intérieure vers la zone extérieure. Si vous avez d'autres zones, assurez-vous d'ajouter des règles autorisant le trafic vers les réseaux appropriés.

Consultez le [Guide de configuration de Firepower Management Center](#) pour configurer des paramètres et des règles de sécurité plus avancés.

Procédure

Étape 1 Choisissez **Policy (politique) > Access Policy (politique d'accès) > Access Policy (politique d'accès)**, et cliquez sur **Modifier** (✎) pour la politique de contrôle d'accès assignée à défense contre les menaces.

Étape 2 Cliquez sur **Add Rule** (ajouter une règle) et définissez les paramètres suivants :

The screenshot shows the 'Add Rule' configuration interface. The 'Name' field contains 'inside_to_outside' and is checked as 'Enabled'. The 'Insert' dropdown is set to 'into Mandatory'. The 'Action' is 'Allow'. The 'Time Range' is 'None'. Below these fields are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'Dynamic Attributes', 'Inspection', 'Logging', and 'Comments'. The 'Zones' tab is active, showing 'Available Zones' with 'inside-zone' and 'outside-zone'. 'inside-zone' is added to 'Source Zones (1)' and 'outside-zone' is added to 'Destination Zones (1)'.

- **Name** (nom) : Nommez cette règle, par exemple **inside_to_outside**.
- **Source Zones** (zones source) : Sélectionnez la zone intérieure sous **Available Zones (zones disponibles)**, et cliquez sur **Add to Source** pour l'ajouter.
- **Destination Zones** (zones de destination) : Sélectionnez la zone extérieure sous **Available Zones (zones disponibles)**, et cliquez sur **Add to Destination** pour l'ajouter.

Laissez les autres paramètres tels quels.

Étape 3

Cliquez sur **Add** (ajouter).

La règle est ajoutée dans le tableau **Rules** (règles).

The screenshot shows the 'Initial AC Policy' configuration page. The 'Rules' tab is selected. A table lists the rules:

#	Name	Source Zones	Dest Zones	Source Netw...	Dest Netw...	VLAN Tags	Users	Appli...	Source Ports	Dest Ports	URLs	Source Dyna... Attrl...	Desti... Dyna... Attrl...	Act...	Icons
1	inside_to_outside	inside-zone	outside-zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	Icons

Buttons for 'Show Warnings', 'Analyze Hit Counts', 'Save', and 'Cancel' are visible. The 'Default Action' is set to 'Access Control:Block all traffic'.

Étape 4

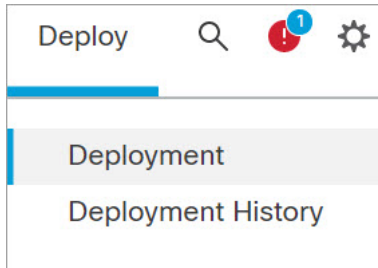
Cliquez sur **Save** (enregistrer).

Déployer la configuration

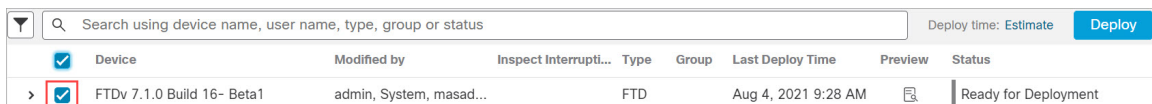
Déployez les modifications de configuration sur défense contre les menaces virtuelles; aucune de vos modifications n'est active sur l'appareil tant que vous ne les avez pas déployées.

Procédure

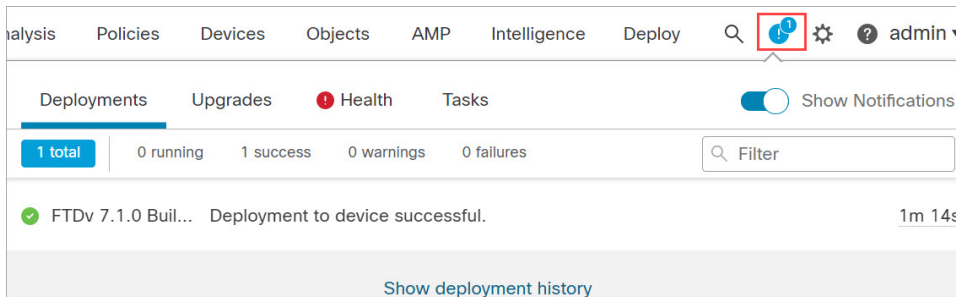
Étape 1 Cliquez sur **Deploy** (déployer) dans le coin supérieur droit.



Étape 2 Sélectionnez le périphérique dans la boîte de dialogue **Deploy Politiques** (déployer des politiques), puis cliquez sur **Deploy** pour exécuter le déploiement.



Étape 3 Assurez-vous que le déploiement réussit. Cliquez sur l'icône à droite du bouton **Deploy** (déployer) dans la barre de menus pour voir l'état des déploiements.



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.