

Déployer le Firewall Management Center Virtual sur GCP

Google Cloud Platform (GCP) est un service en nuage public fourni par Google qui vous permet de créer et d'héberger des applications de l'infrastructure évolutive de Google. Le nuage privé virtuel (VPC) de Google vous offre la possibilité d'évoluer et de contrôler la façon dont les charges de travail se connectent à l'échelle régionale et mondiale. GCP vous permet de créer vos propres VPC en plus de l'infrastructure publique de Google.

Vous pouvez déployer le Firewall Management Center Virtual sur le GCP.

- Aperçu, à la page 1
- Prérequis, à la page 2
- Lignes directrices et limites relatives à la licence, à la page 3
- Exemple de topologie de réseau, à la page 3
- Déployer Firewall Management Center Virtual, à la page 4
- Accéder à l'instance Firewall Management Center Virtual sur GCP, à la page 7

Aperçu

Firewall Management Center Virtual exécute le même logiciel que les On-Prem Firewall Management Center physiques afin d'offrir des fonctionnalités de sécurité éprouvées dans un format virtuel. Firewall Management Center Virtual peut être déployé dans le GCP public. Il peut ensuite être configuré pour gérer les périphériques virtuels et physiques.

Prise en charge des types de machines GCP

Firewall Management Center Virtual prend en charge les machines de calcul optimisé et les machines à usage général (types de machines standard, à mémoire élevée et à processeur élevé). Firewall Management Center Virtual prend en charge les types de machines GCP suivants :

Remarque Les types de machines pris en charge peuvent changer sans préavis.

Tableau 1 : Types de machines optimisées pour le calcul prises en charge

Types de machines optimisées pour le calcul	Attributs	
	vCPU	RAM (Go)
c2-standard-8	8	32 Go
c2-standard-16	16	64 Go

Tableau 2 : Types de machines générales prises en charge

Types de machines à usage général	Attributs	
	vCPU	RAM (Go)
n1-standard-8	8	30 Go
n1-standard-16	16	60 Go
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-32	32	28.8
n2-highcpu-32	32	32
n1-highmem-8	8	52
n1-highmem-16	16	104
n2-highmem-4	4	32
n2-highmem-8	8	64

Prérequis

- Créez un compte GCP à l'adresse https : //cloud.google.com.
- Un compte Cisco Smart. Vous pouvez en créer un sur le Centre des logiciels Cisco (https://software.cisco.com/).
  - Configurez tous les droits de licence pour les services de sécurité à partir de la On-Prem Firewall Management Center.
  - Consultez la section « Licence du système » dans le Guide de configuration On-Prem Firewall Management Center pour en savoir plus sur la gestion des licences.

- Exigences d'interface :
  - Interface de gestion : une interface utilisée pour connecter le périphérique au Firewall Threat Defense au On-Prem Firewall Management Center.
- Chemins de communication :
  - Adresse IP publique permettant l'accès administratif au On-Prem Firewall Management Center.
- Pour la compatibilité de Firewall Management Center Virtual et du système, consultez le guide de compatibilité de Cisco Secure Firewall Threat Defense.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

- Déploiement dans le moteur de traitement de GCP
- Maximum de 32 vCPU par instance (selon le type de machine GCP)
- Licences : Seul le protocole BYOL est pris en charge

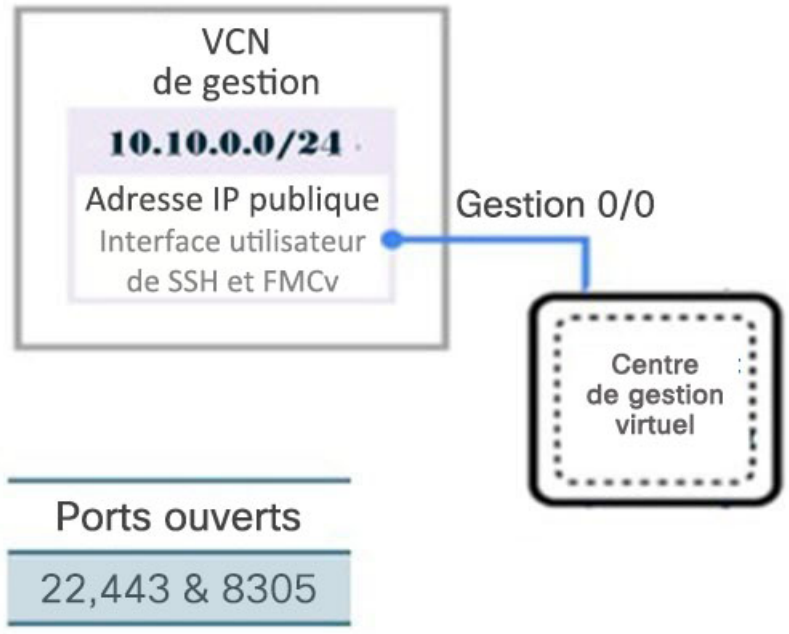
Fonctionnalités non prises en charge

- IPv6
- Haute accessibilité en natif Firewall Management Center Virtual
- Évolutivité automatique
- Modes transparent/en ligne/passif
- Mode multi-contexte

Exemple de topologie de réseau

La figure suivante illustre la topologie typique pour le Firewall Management Center Virtual avec un sous-réseau configuré dans GCP.

Illustration 1 : Exemple de topologie pour le déploiement Firewall Management Center Virtual sur GCP



Déployer Firewall Management Center Virtual

Les procédures suivantes décrivent comment préparer votre environnement GCP et lancer l'instance Firewall Management Center Virtual.

Créer des réseaux vPC

Le déploiement Firewall Management Center Virtual nécessite le Management VPC (VPC de gestion) pour la gestion Firewall Management Center Virtual. Consultez la figure 1 à la page 3 comme guide.

Procédure

Étape 1 Dans la console GCP, choisissez **VPC networking** (réseaux VPC), puis cliquez sur **Create VPC Network** (créer un réseau VPC).

Étape 2 Dans le champ **Name** (nom), saisissez le nom descriptif de votre réseau VPC.

Étape 3 Dans le **Subnet creation mode** (mode de création de sous-réseau), cliquez sur **Custom** (personnalisé).

Étape 4 Dans le champ **Name** (Nom) sous **New subnet** (nouveau sous-réseau), saisissez le nom souhaité.

Étape 5 Dans la liste déroulante **Region** (région), sélectionnez la région appropriée pour votre déploiement.

Étape 6 Dans le champ **IP address range** (plage d'adresses IP), saisissez le sous-réseau du premier réseau au format CIDR, par exemple 10.10.0.0/24.

Étape 7 Acceptez les valeurs par défaut de tous les autres paramètres, puis cliquez sur **Create** (Créer).

Créer les règles de pare-feu

Chacun des réseaux VPC nécessite des règles de pare-feu pour autoriser SSH et le trafic. Créez les règles de pare-feu pour chaque réseau VPC.

Procédure

Étape 1 Dans la console GCP, choisissez **Networking (réseautage)** > **VPC network (réseau VPC)** > **Firewall (pare-feu)**, puis cliquez sur **Create Firewall Rule** (créer une règle de pare-feu).

Étape 2 Dans le champ **Name** (nom), saisissez un nom descriptif pour votre règle de pare-feu, par exemple, *vpc-asiasouth-mgmt-ssh*.

Étape 3 Dans la liste déroulante **Network** (réseau), sélectionnez le nom du réseau VPC pour lequel vous créez la règle de pare-feu, par exemple, *fmcv-south-mgmt*.

Étape 4 Dans la liste déroulante **Targets (** (cibles), sélectionnez l'option applicable à votre règle de pare-feu, par exemple, **All instances in the network** (toutes les instances du réseau).

Étape 5 Dans le champ **Source IP ranges** (plages IP sources), saisissez les plages d'adresses IP sources au format CIDR, par exemple, 0.0.0.0/0.

Le trafic n'est autorisé que par des sources comprises dans ces plages d'adresses IP.

Étape 6 Sous **Protocols and ports** (protocoles et ports), sélectionnez **Specified protocols and ports** (protocoles et ports spécifiés).

Étape 7 Ajoutez vos règles de sécurité :

a) Ajouter une règle pour autoriser SSH (TCP/22).

b) Ajoutez une règle pour autoriser le port TCP 443.

Vous accédez à l'UI Firewall Management Center Virtual qui exige l'ouverture du port 443 pour les connexions HTTPS.

Étape 8 Cliquez sur **Create** (créer).

Créer l'instance Firewall Management Center Virtual sur GCP

Vous pouvez suivre les étapes ci-dessous pour déployer l'instance Firewall Management Center Virtual à partir de la console GCP.

Procédure

Étape 1 Connectez-vous à la console GCP.

Étape 2 Cliquez sur **Navigation menu** > **(menu de navigation)** > **Marketplace** > **(Marché)**.

Étape 3 Effectuez une recherche sur le Marché pour « BYOL On-Prem Firewall Management Center » et choisissez l'offre.

Étape 4 Cliquez sur **Launch** (lancer).

a) **Deployment name** (nom de déploiement) : Précisez un nom unique pour l'instance.

b) **Version de l'image** : sélectionnez la version dans la liste déroulante.

c) **Zone** : Sélectionnez la zone dans laquelle vous souhaitez déployer Firewall Management Center Virtual.

d) **Type de machine** : Choisissez le bon type de machine en fonction de Prise en charge des types de machines GCP, à la page 1.

e) **SSH key (clé SSH, facultatif)** : Collez la clé publique de la paire de clés SSH.

La paire de clés se compose d'une clé publique que GCP stocke et d'un fichier de clé privée que l'utilisateur stocke. Ensemble, ils vous permettent de vous connecter à votre instance en toute sécurité. Assurez-vous d'enregistrer la paire de clés à un emplacement connu, car elle devra se connecter à l'instance.

f) Choisissez d'autoriser ou de **bloquer les clés SSH à l'échelle du projet pour l'accès à cette instance**. Consultez la documentation de Google Autoriser ou bloquer les clés SSH publiques à l'échelle du projet à partir d'une instance Linux.

g) **Startup script** (Script de démarrage) : fournissez la configuration day0 (jour0) pour le Firewall Management Center Virtual.

L'exemple suivant montre une configuration day0 (jour0) que vous pouvez copier et coller dans le champ **Startup script** (Script de démarrage) :

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

Astuces
Pour éviter les erreurs d'exécution, vous devez valider votre configuration day0 à l'aide d'un programme de validation JSON.

h) Sélectionnez le **Boot disk type** (Type de disque de démarrage) dans la liste.

Par défaut, le **Standard Persistent Disk** (Disque persistant standard) est sélectionné. Cisco vous recommande d'utiliser le type de disque de démarrage par défaut.

i) La valeur par défaut **de la taille du disque de démarrage en Go** est de 250 Go. Cisco vous recommande de conserver la taille par défaut du disque de démarrage. Elle ne peut pas être inférieure à 250 Go.

j) Cliquez sur **Add network interface** (ajouter une interface de réseau) pour configurer l'interface de gestion (Management).

Remarque
Vous ne pouvez pas ajouter des interfaces à une instance après l'avoir créée. Si vous créez l'instance avec une configuration d'interface incorrecte, vous devez supprimer l'instance et la recréer avec la configuration d'interface appropriée.

- Dans la liste déroulante **Network** (réseau), sélectionnez un réseau VPC, par exemple, *vpc-branch-mgmt*.
- Dans la liste déroulante **External IP** (adresse IP externe), sélectionnez l'option appropriée.

  Pour l'interface de gestion, sélectionnez **External IP** (Adresse IP externe) à **Ephemeral** (Éphémère).
- Cliquez sur **Done (Terminé)**.

k) **Firewall** (pare-feu) : Appliquez les règles de pare-feu.

- Cochez la case **Allow TCP port 22 traffic from the Internet (SSH access)** (autoriser le trafic du port TCP 22 de l'Internet, accès SSH) pour autoriser SSH.
- Cochez la case **Allow HTTPS traffic from the Internet (FMC GUI)** (Autoriser le trafic HTTPS de l'Internet (interface FMC)) pour autoriser les connexions HTTPS.
- Cochez la case **Allow HTTPS traffic from the Internet** (SFTunnel comm.) (autoriser le trafic HTTPS de l'Internet (comm. SFTunnel) pour permettre au Firewall Management Center Virtual et aux périphériques gérés de communiquer à l'aide d'un canal de communication chiffré SSL bidirectionnel (SFTunnel).

l) Cliquez sur **More** (plus) pour développer l'affichage et assurez-vous que **IP Forwarding** (transfert IP) est défini sur **On** (activé).

Étape 5 Cliquez sur **Deploy** (déployer).

Remarque
Le délai de démarrage dépend d'un certain nombre de facteurs, notamment la disponibilité des ressources. L'initialisation peut prendre jusqu'à 35 minutes. N'interrompez pas l'initialisation, sinon vous devrez peut-être supprimer l'appareil et recommencer.

Prochaine étape

Affichez les détails de l'instance dans la page d'instance de VM de la console GCP. Vous trouverez l'adresse IP interne, l'adresse IP externe et les contrôles pour arrêter et démarrer l'instance. Vous devez arrêter l'instance si vous devez la modifier.

Accéder à l'instance Firewall Management Center Virtual sur GCP

Assurez-vous d'avoir déjà activé une règle de pare-feu pour autoriser les connexions SSH (TCP par le port 22) pendant le déploiement ; consultez Créer les règles de pare-feu, à la page 5 pour plus d'information.

Cette règle de pare-feu active l'accès à l'instance Firewall Management Center Virtual et vous permet de vous connecter à l'instance en utilisant les méthodes suivantes.

- External IP (IP externe)
  - Fenêtre du navigateur
  - Tout autre outil client SSH ou tiers
- Console de série
  - Ligne de commande Gcloud

Consultez la documentation de Google, Connexion aux instances pour en savoir plus.

Remarque Si vous choisissez de ne pas ajouter de configuration Day0, vous pouvez vous connecter à l'instance Firewall Management Center Virtual en utilisant les informations d'authentification par défaut. Vous êtes invité à définir le mot de passe lors de la première tentative de connexion.

Se connecter à l'instance Firewall Management Center Virtual à l'aide de la console de série

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

Étape 2 Cliquez sur le nom de l'instance Firewall Management Center Virtual pour ouvrir la page des renseignements de l'instance de machine virtuelle (**VM instance details**).

Étape 3 Sous l'onglet **Details** (Détails), cliquez sur **Connect to serial console** (Se connecter à la console série).

Consultez la documentation de Google, Interagir avec la console série pour en savoir plus.

Se connecter à l'instance Firewall Management Center Virtual à l'aide d'une adresse IP externe

L'instance Firewall Management Center Virtual se voit attribuer une adresse IP interne et une adresse IP externe. Vous pouvez utiliser l'adresse IP externe pour accéder à l'instance Firewall Management Center Virtual.

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

Étape 2 Cliquez sur le nom de l'instance Firewall Management Center Virtual pour ouvrir la page des renseignements de l'instance de machine virtuelle (**VM instance details**).

Étape 3 Sous l'onglet **Details** (Détails), cliquez sur le menu déroulant du champ **SSH**.

Étape 4 Sélectionnez l'option souhaitée dans le menu déroulant **SSH**.

Vous pouvez vous connecter à l'instance Firewall Management Center Virtual en utilisant la méthode suivante.

- Tout autre outil client SSH ou tiers : consultez l'information sur la connexion à l'aide d'outils tiers de la documentation de Google pour en savoir plus.

Se connecter à l'instance Firewall Management Center Virtual à l'aide de GCloud

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

Étape 2 Cliquez sur le nom de l'instance Firewall Management Center Virtual pour ouvrir la page des renseignements de l'instance de machine virtuelle (**VM instance details**).

Étape 3 Sous l'onglet **Details** (Détails), cliquez sur le menu déroulant du champ **SSH**.

Étape 4 Cliquez sur **View gcloud command (Voir la commande gcloud)** > **Run in Cloud Shell (Exécuter dans Cloud Shell)**.

La fenêtre de terminal Cloud Shell s'ouvre. Consultez la documentation de Google, Présentation de l'outil de ligne de commande gcloudet Calcul gcloud ssh pour en savoir plus.

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.