Déployer Défense contre les menaces virtuelles sur la plateforme Google Cloud Platform

Vous pouvez déployer défense contre les menaces virtuelles sur Google Cloud Platform (GCP), un service informatique en nuage public qui vous permet d'exécuter vos applications dans un environnement hébergé hautement disponible offert par Google.

Vous voyez les informations sur le projet GCP dans le tableau de bord (**Dashboard**) de la console GCP.

- Assurez-vous de sélectionner votre projet GCP dans le tableau de bord (**Dashboard**) s'il n'est pas déjà sélectionné.
- Pour accéder au tableau de bord, cliquez sur le menu **Navigation** > **Home (accueil)** > **Dashboard (tableau de bord)**.

Vous vous connectez à la console GCP, recherchez dans le Marché GCP l'offre de pare-feu virtuel Cisco Firepower NGFWv (NGFWv) et lancez l'instance défense contre les menaces virtuelles. Les procédures suivantes décrivent comment préparer votre environnement GCP et lancer l'instance défense contre les menaces virtuelles pour déployer défense contre les menaces virtuelles.

Aperçu

défense contre les menaces virtuelles exécute le même logiciel que Cisco Secure Firewall Threat Defense physique (anciennement Firepower Threat Defense) pour offrir des fonctionnalités de sécurité éprouvées dans un format virtuel. défense contre les menaces virtuelles peut être déployé dans le GCP public. Il peut ensuite être configuré pour protéger les charges de travail des centres de données virtuels et physiques qui se développent, se contractent ou changent d'emplacement au fil du temps.

Configuration système requise

Sélectionnez le type et la taille de machine virtuelle Google qui répondent à vos besoins défense contre les menaces virtuelles. Actuellement, défense contre les menaces virtuelles 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).

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)	Cartes vNIC
c2-standard-4	4	16 Go	4
c2-standard-8	8	32 Go	8
c2-standard-16	16	64 Go	8

Tableau 2 : Types de machines générales prises en charge

Types de machines à usage général	Attributs		
	vCPU	RAM (Go)	Cartes vNIC
n1-standard-4	4	15	4
n1-standard-8	8	30	8
n1-standard-16	16	60	8
n2-standard-4	4	16	4
n2-standard-8	8	32	8

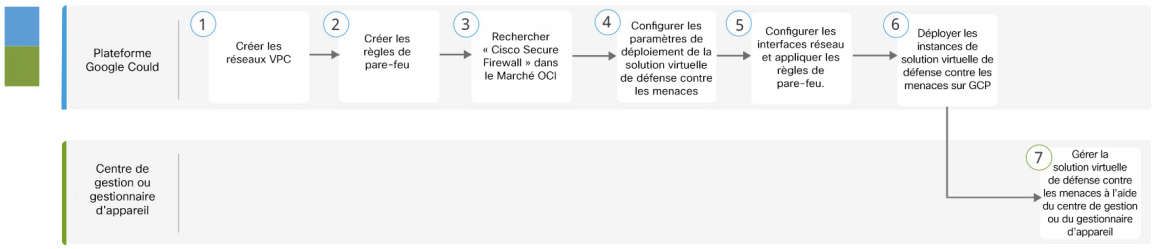
Types de machines à usage général	Attributs		
	vCPU	RAM (Go)	Cartes vNIC
n2-standard-16	16	64	8
n2-highmem-4	4	32	4
n2-highmem-8	8	64	8

- Le défense contre les menaces virtuelles nécessite un minimum de 4 interfaces.
- Le maximum de vCPU pris en charge est de 16.

Vous créez un compte sur GCP, lancez une instance de VM à l'aide de l'offre de pare-feu virtuel Cisco Firepower NGFW (NGFWv) sur GCP Marketplace et choisissez un type de machine GCP.

Procédure de bout en bout

Le diagramme suivant illustre le flux de travail pour le déploiement de Threat Defense Virtual sur la plateforme Google Cloud.



	Espace de travail	Étapes
1	GCP	Déployer Threat Defense Virtual sur GCP : Créez le réseau VPC (**VPC Networks (réseaux)** > **Subnet (sous-réseau)** > **Region (région)** > **IP address range (plage d'adresses IP)**).
2	GCP	Déployer Threat Defense Virtual sur GCP : Créez les règles de pare-feu (**Networking (réseaux)** > **VPC networks (réseaux VPC)** > **Firewall (pare-feu)** > **Create Firewall Rule (créer une règle de pare-feu)**).
3	GCP	Déployer Threat Defense Virtual sur GCP : Recherchez « Cisco Secure Firewall » dans le Marché GCP.
4	GCP	Déployer Threat Defense Virtual sur GCP : Configurez les paramètres de déploiement virtuel de la défense contre les menaces.
5	GCP	Déployer Threat Defense Virtual sur GCP : Configurez les interfaces réseau et appliquer les règles de pare-feu.
6	GCP	Déployer le Threat Defense Virtual sur Nutanix : Déployez Threat Defense Virtual sur GCP.

	Espace de travail	Étapes
7	Centre de gestion ou gestionnaire d'appareil	Gérer défense contre les menaces virtuelles : • Gestion de Défense contre les menaces virtuelles avec Centre de gestion • Gestion de Défense contre les menaces virtuelles avec Gestionnaire d'appareil

Conditions préalables

- Créez un compte GCP à l'adresse https : //cloud.google.com.
- Créez votre projet GCP. Consultez la documentation de Google, Création de votre projet.
- Un compte Cisco Smart. Vous pouvez en créer un sur le Centre des logiciels Cisco (https://software.cisco.com/).
- Obtenez une licence pour défense contre les menaces virtuelles.
  - Configurez tous les droits de licence pour les services de sécurité à partir de la centre de gestion.
  - Consultez la section sur les *licences* dans le Guide d'administration Cisco Secure Firewall Management Center pour plus d'informations sur la gestion des licences.
- Pour les configurations système de défense contre les menaces virtuelles, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense.

Exigences d'interface

- Interfaces de gestion (2) : une utilisée pour connecter défense contre les menaces virtuelles avec centre de gestion, la seconde utilisée pour les diagnostics; ne peut pas être utilisé pour le trafic de transit.
- Interfaces de trafic (2) : utilisées pour connecter défense contre les menaces virtuelles aux hôtes internes et au réseau public.

Chemins de communication

- Adresses IP publiques pour l'accès à défense contre les menaces virtuelles.

Lignes directrices et limites relatives à Défense contre les menaces virtuelles et à GCP

Fonctionnalités prises en charge

- Déploiement dans le moteur de traitement de GCP
- Maximum de 16 vCPU par instance

- Mode avec routage (par défaut)
- Licences : Seul le protocole BYOL est pris en charge
- Mise en grappe (7.2 ou ultérieure). Pour en savoir plus, consultez l'information sur la mise en grappes pour Threat Defense Virtual dans un nuage public.
- Sur Cisco Secure Firewall 7.1 et les versions antérieures, seul Centre de gestion est pris en charge. À partir de la version 7.2 de Cisco Secure Firewall, Gestionnaire d'appareil est également pris en charge.

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

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

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

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

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

Remarque Pour modifier les valeurs de vCPU/mémoire, vous devez d'abord éteindre le périphérique défense contre les menaces virtuelles.

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 GCP 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.

Attribution des files d'attente de réception et de transmission

Un nombre précis de files d'attente de réception (RX) et de transmission (TX) est attribué à chaque vNIC pour traiter les paquets réseau. Selon le type d'interface réseau utilisé (VertIO ou gVNIC), Google Cloud utilise un algorithme pour attribuer un nombre par défaut de files d'attente RX et TX par vNIC.

La méthode utilisée par GCP pour attribuer des files d'attente aux vNIC est la suivante :

- VirtIO : nombre de vCPU divisés par le nombre de vNIC; ignorez toute valeur restante.

  Par exemple, si la machine virtuelle a 16 vCPU et 4 vNIC, le nombre de files d'attente attribuées par vNIC est de [16/4] = 4.

- gVNIC – nombre de vCPU divisés par le nombre de vNIC; divisez ensuite le résultat par 2

  Par exemple, si la machine virtuelle comporte 128 vCPU et 2 vNIC, le nombre de files d'attente attribuées est de [128/2]/2 = 32.

Vous pouvez également personnaliser le nombre de files d'attente allouées à chaque vNIC lorsque vous créez une nouvelle machine virtuelle en utilisant l'API de moteur de traitement informatique. Cependant, vous devez respecter les règles suivantes si vous souhaitez le faire -

- Nombre minimal de files d'attente : une par vNIC.
- Nombre maximal de files d'attente : ce nombre est le plus bas entre le nombre de vCPU ou le nombre maximal de files d'attente par vNIC, en fonction du type de pilote :
  - Le nombre maximal de files d'attente est de 32 si vous utilisez VirtIO ou un pilote personnalisé
  - Le nombre maximal de files d'attente est de 16 si vous utilisez gVNIC
- Si vous personnalisez le nombre de files d'attente attribuées à tous les vNIC de la machine virtuelle, le nombre total d'affectations de files d'attente doit être inférieur ou égal au nombre de vCPU attribuées à l'instance de machine virtuelle.

Pour plus d'informations et des exemples sur l'allocation de file d'attente par défaut et personnalisée, consultez l'information sur l'attribution de files d'attente par défaut et l'attribution de files d'attente personnalisées.

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.

Mise à jour

La mise à niveau de défense contre les menaces virtuelles dans GCP de la version 7.1 de Cisco Secure Firewall à la version 7.2 n'est pas prise en charge. Effectuez une recréation d'image si vous effectuez une mise à niveau de la version 7.1 de Cisco Secure Firewall à la version 7.2.

Fonctionnalités non prises en charge

- IPv6
- Haute accessibilité en natif Défense contre les menaces virtuelles
- Modes transparent/en ligne/passif
- Cadres jumbo

Mappage de la carte NIC avec les interfaces de données

Dans Cisco Secure Firewall version 7.1 et les versions antérieures, le mappage des cartes d'interface réseau (NIC) aux interfaces de données est indiqué ci-dessous :

- nic0 – interface de gestion
- nic1 – interface de diagnostic
- nic2 – Gigabit Ethernet 0/0
- nic3 – Gigabit Ethernet 0/1

À partir de la version 7.2 de Cisco Secure Firewall, une interface de données est requise sur nic0 pour faciliter le mouvement du trafic nord-sud, car l'équilibreur de charges externe (ELB) transfère les paquets uniquement à nic0.

Le mappage des cartes réseau et des interfaces de données sur la version 7.2 de Cisco Secure Firewall est comme indiqué ci-dessous :

- nic0 – Gigabit Ethernet 0/0
- nic1 – Gigabit Ethernet 0/1
- nic2 – interface de gestion
- nic3 – interface de diagnostic
- nic4 – Gigabit Ethernet 0/2

  .

  .

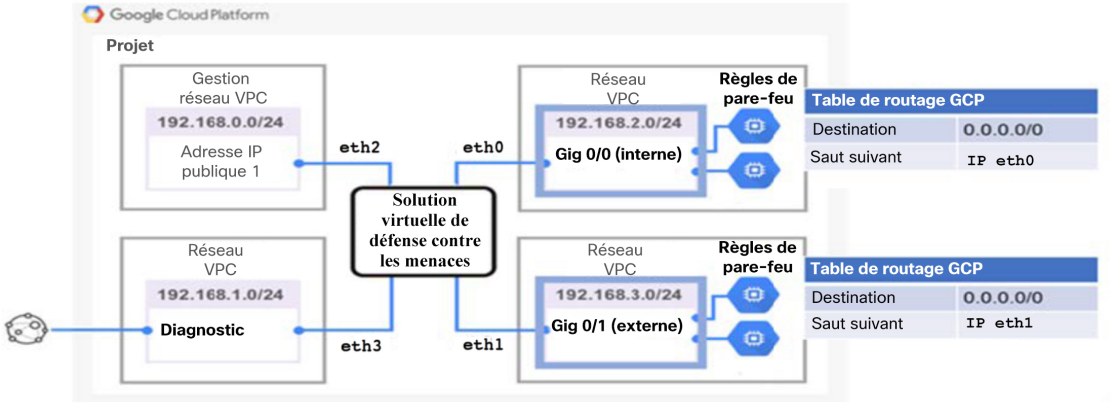
  .

- nic(N-2) – Gigabit Ethernet 0/N-4
- nic(N-1) – Gigabit Ethernet 0/N-3

Exemple de topologie de réseau

La figure suivante montre la topologie recommandée pour défense contre les menaces virtuelles en mode pare-feu avec routage et avec quatre sous-réseaux configurés dans GCP pour défense contre les menaces virtuelles (gestion, diagnostic, interne et externe).

Illustration 1 : Exemple Défense contre les menaces virtuelles sur le déploiement GCP



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.

Configurer l'environnement GCP

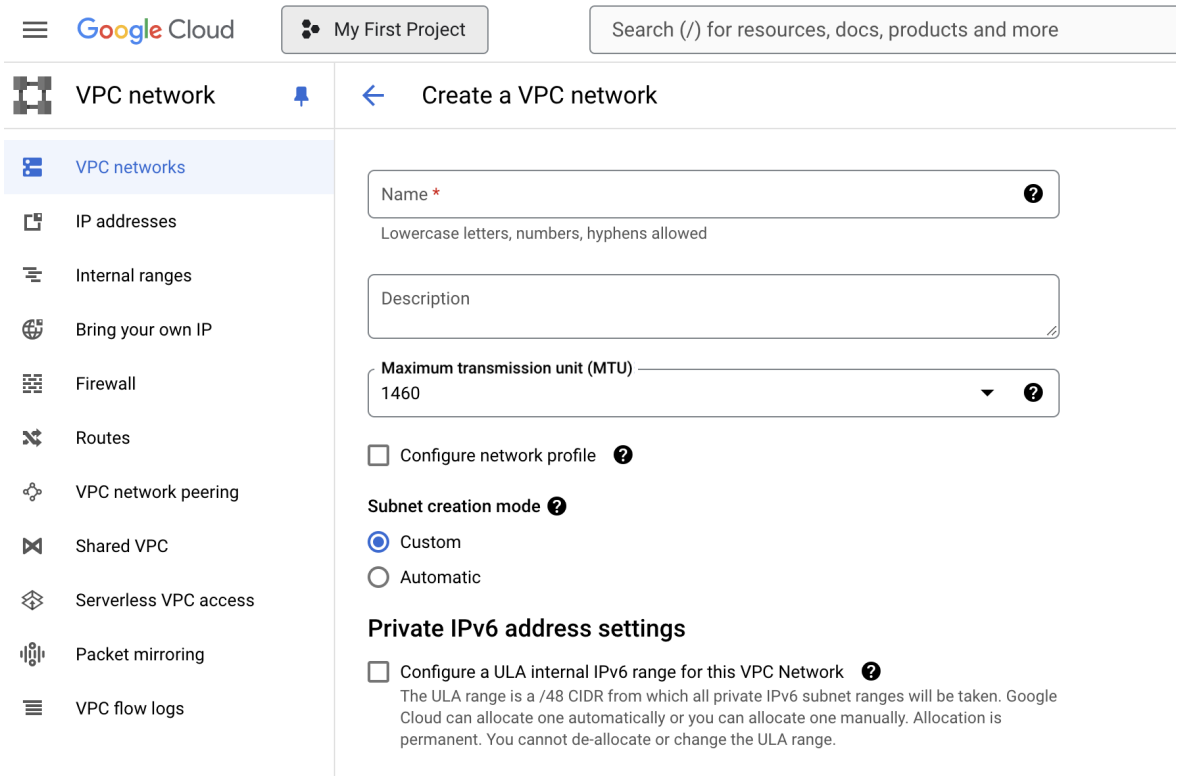
Le déploiement de défense contre les menaces virtuelles nécessite quatre réseaux que vous devez créer avant de déployer défense contre les menaces virtuelles. Les réseaux sont les suivants :

- VPC de gestion pour le sous-réseau de gestion.
- VPC de dépistage ou sous-réseau de dépistage.
- VPC interne pour le sous-réseau interne.
- VPC externe pour le sous-réseau externe.

En outre, vous configurez des tableaux de routage et des règles de pare-feu de GCP pour permettre au trafic de circuler dans défense contre les menaces virtuelles. Les tableaux de routage et les règles de pare-feu sont distincts de ceux configurés sur l'défense contre les menaces virtuelles lui-même. Nommez les tableaux de routage et les règles de pare-feu de GCP en fonction du réseau et des fonctionnalités associés. Consultez la section de la topologie de réseau pour FTDv sur GCP comme guide.

Procédure

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

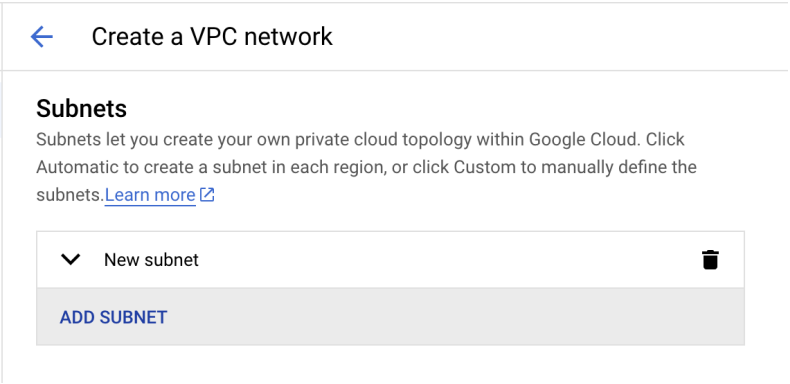


Étape 2 Dans le champ **Name** (nom), saisissez le nom souhaité.

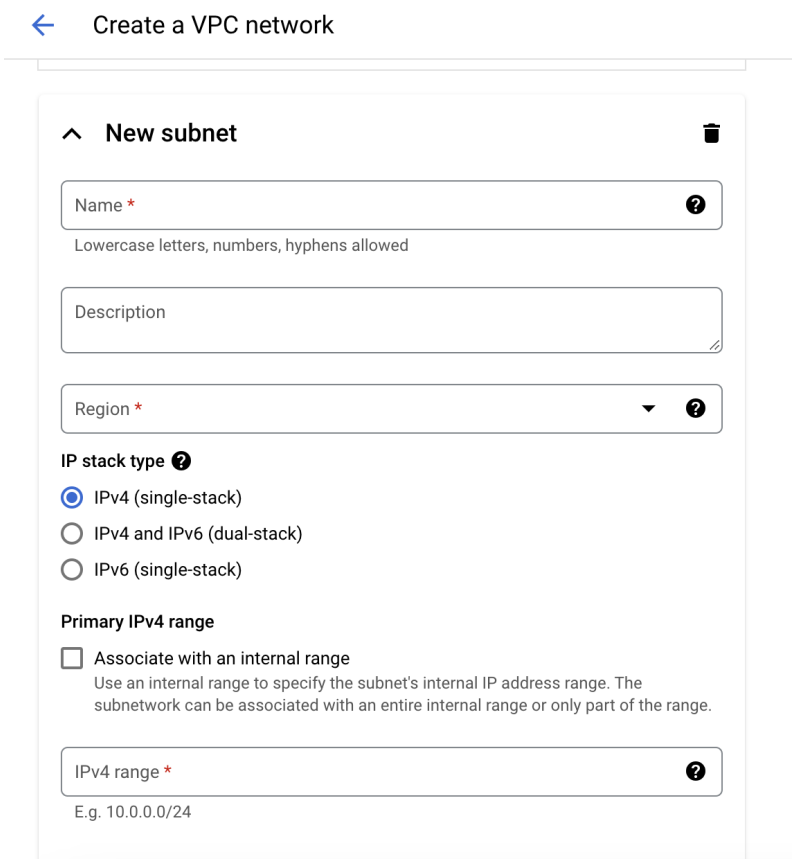
Étape 3 Dans le menu déroulant **Maximum transmission unit (MTU)** (unité de transmission maximale; MTU), choisissez une valeur appropriée.

Étape 4 Dans l'option **Subnet creation mode** (mode de création de sous-réseau), cliquez sur **Custom** (personnalisé).

Étape 5 Dans la section **Subnet** (sous-réseau), cliquez sur **ADD SUBNET** pour créer un nouveau sous-réseau.



Étape 6 Dans le champ **Name** (Nom) sous **New subnet** (nouveau sous-réseau), saisissez le nom souhaité.



Étape 7 Dans la liste déroulante **Region** (région), sélectionnez la région appropriée pour votre déploiement. Les quatre réseaux doivent se trouver dans la même région.

Étape 8 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 9 Acceptez les valeurs par défaut de tous les autres paramètres, puis cliquez sur **Create** (Créer).

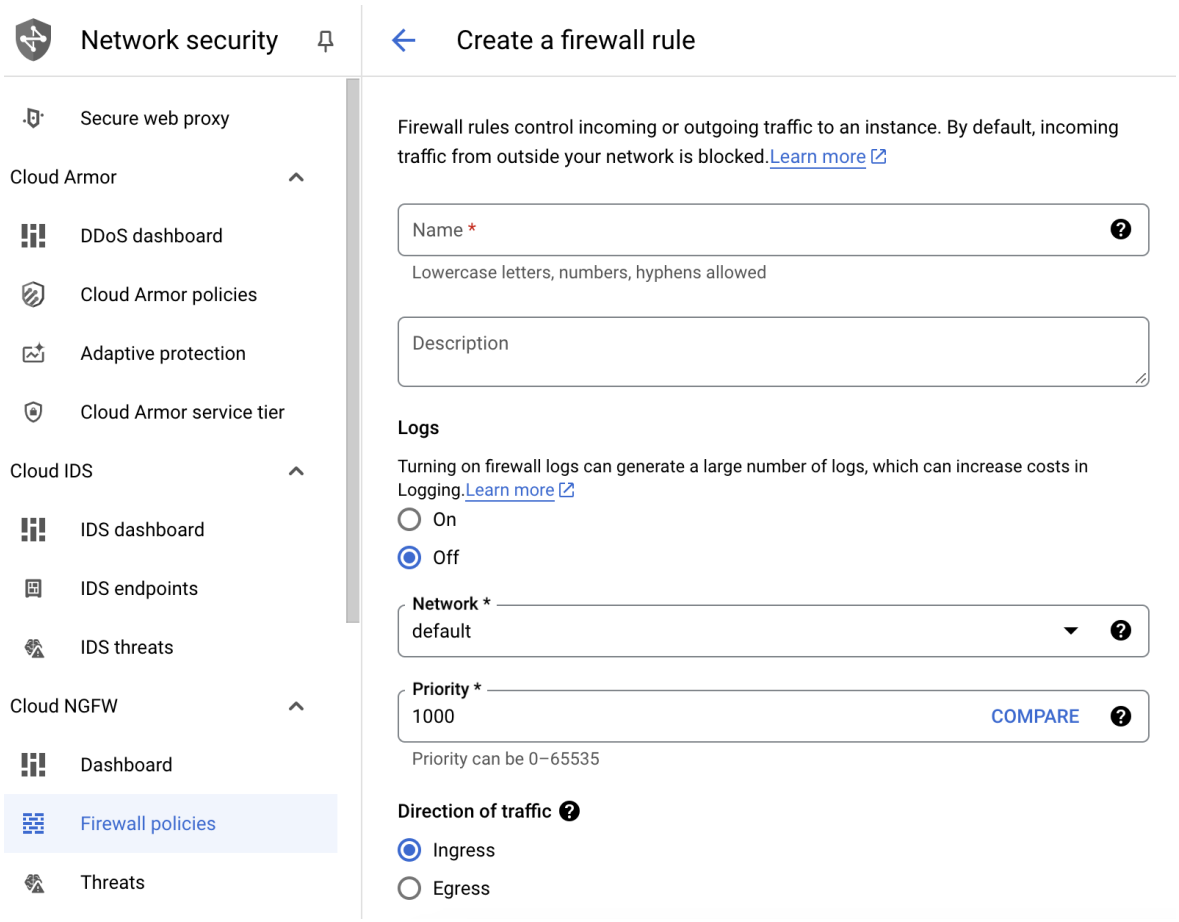
Étape 10 Répétez les étapes 1 à 7 pour créer les trois autres réseaux VPC.

Créer les règles de pare-feu

Vous appliquez les règles de pare-feu de l'interface de gestion (pour permettre la communication de SSH et SFTunnel avec le centre de gestion) lors du déploiement de l'instance défense contre les menaces virtuelles; consultez Déployer Défense contre les menaces virtuelles, à la page 14. Selon vos besoins, vous pouvez également créer des règles de pare-feu pour les interfaces interne, externe et de diagnostic.

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).

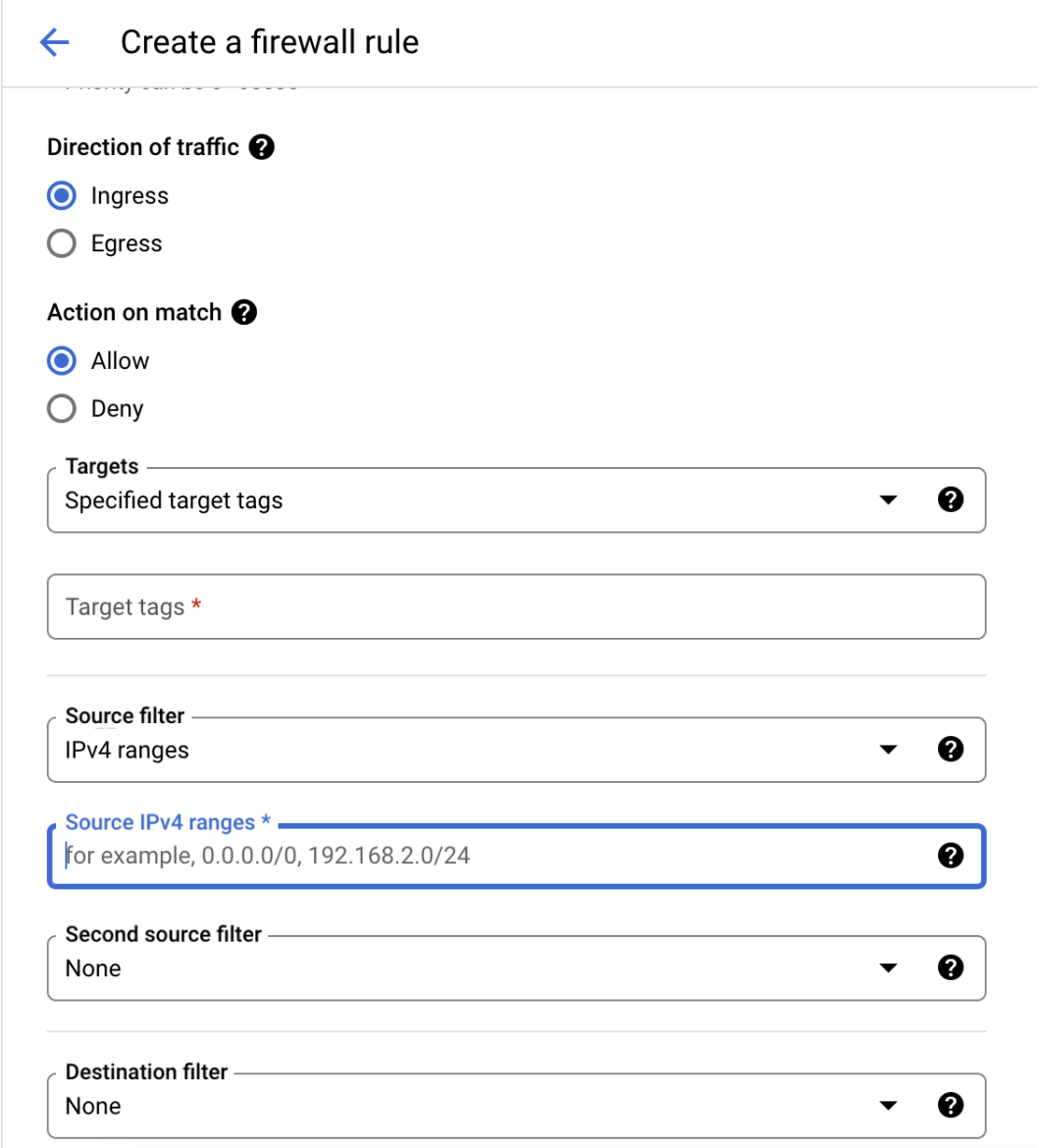


Étape 2 Dans le champ **Name** (nom), saisissez un nom descriptif pour votre règle de pare-feu, par exemple, *vpc-asiasouth-inside-fwrule*.

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, *ftdv-south-inside*.

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 la liste déroulante **Source filter** (filtre de source), sélectionnez le type d'adresse IP pris en charge, par exemple, **IPv4 ranges** pour les plages IPv4.



Étape 6 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 7 Sous **Protocols and ports** (protocoles et ports), sélectionnez **Specified protocols and ports** (protocoles et ports spécifiés).

Étape 8 Ajoutez vos règles de sécurité.

Étape 9 Cliquez sur **Create** (créer).

Déployer Défense contre les menaces virtuelles

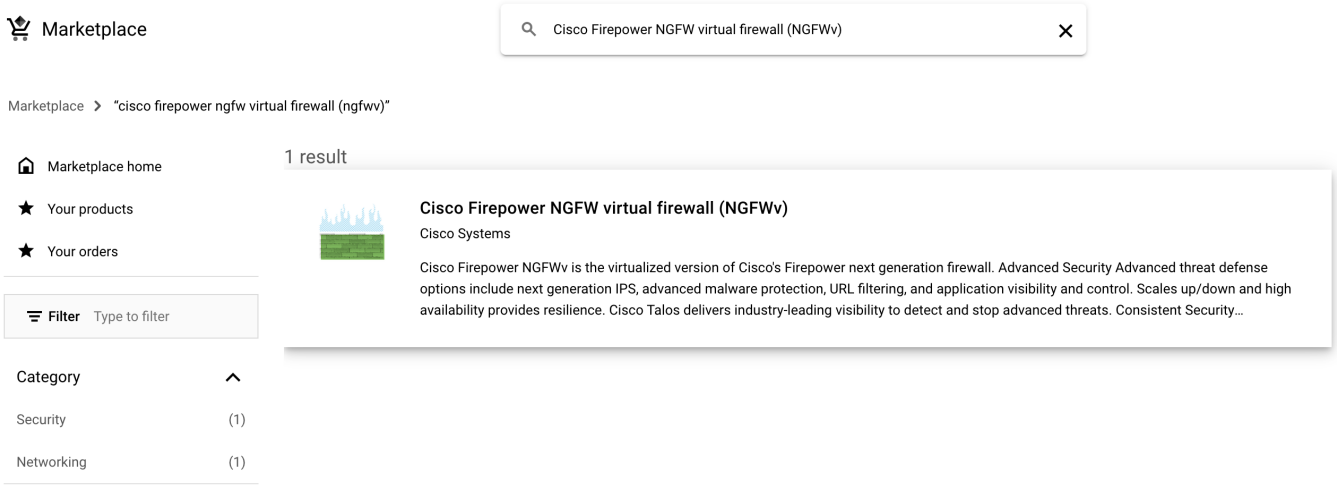
Vous pouvez suivre les étapes ci-dessous pour déployer une instance défense contre les menaces virtuelles à l'aide de l'offre de pare-feu virtuel Cisco Firepower NGFWv (NGFWv) du Marché GCP.

Procédure

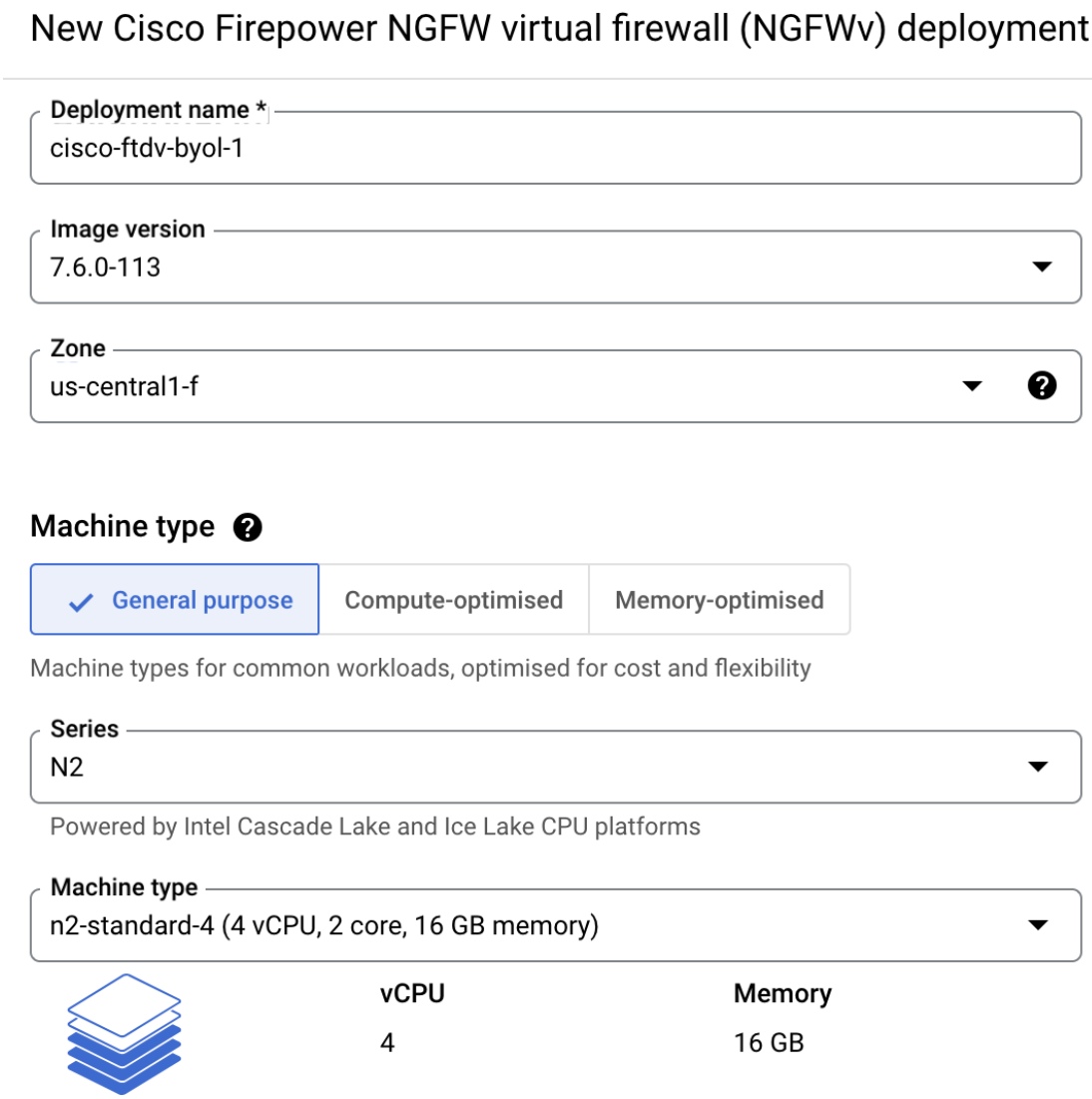
Étape 1 Connectez-vous à la console GCP.

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

Étape 3 Effectuez une recherche sur le Marché pour l'offre « Cisco Firepower NGFW virtual firewall (NGFWv) ».



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



a) **Deployment name** (nom de déploiement) : Précisez un nom unique pour l'instance.
b) **Zone** : Sélectionnez la zone dans laquelle vous souhaitez déployer défense contre les menaces virtuelles.
c) **Type de machine** : Choisissez le bon type de machine en fonction de Configuration système requise, à la page 2.
d) **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.

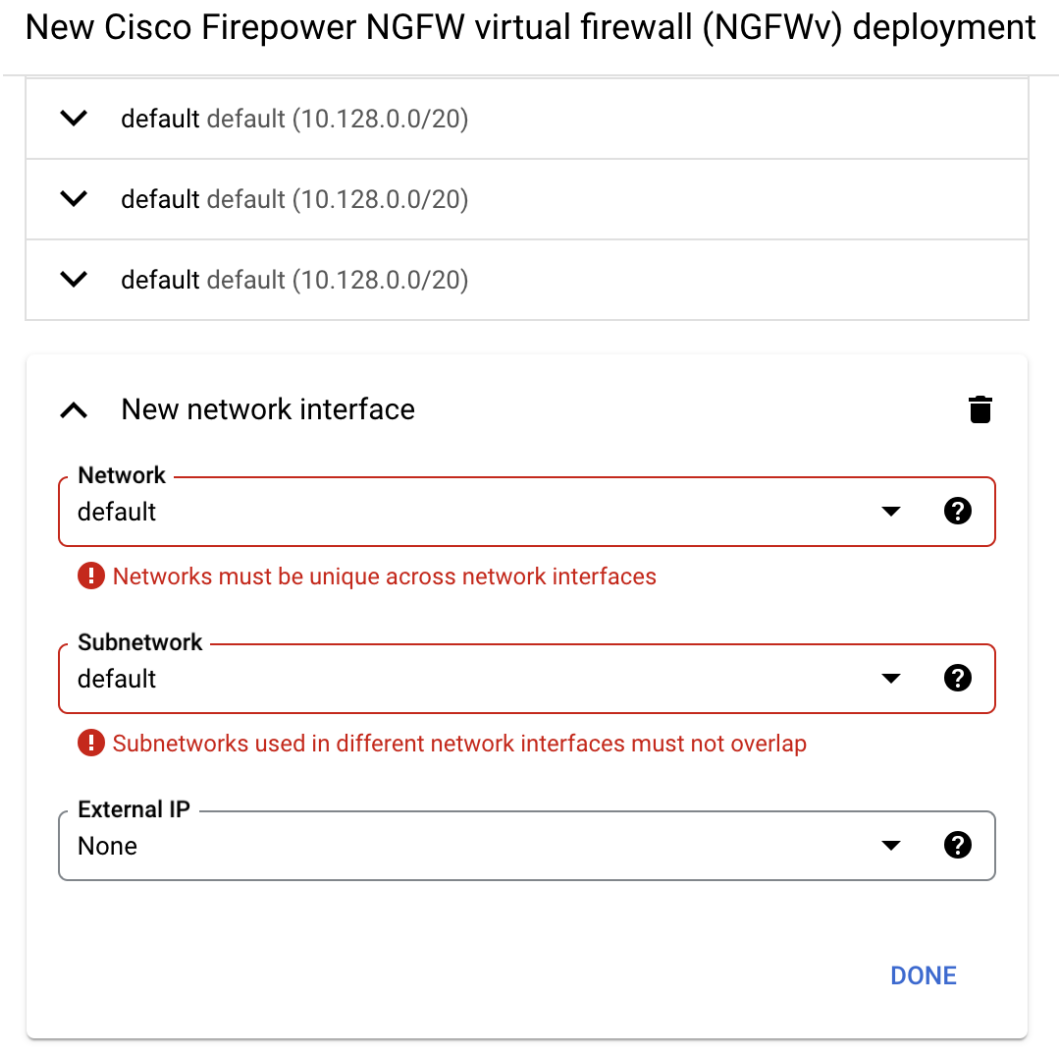
e) Choisissez d'autoriser ou de bloquer les clés SSH à l'échelle du projet pour l'accès à cette instance. Consultez la documentation de Google Autoriser ou bloquer les clés SSH publiques à l'échelle du projet à partir d'une instance Linux.
f) **Script de démarrage** : Vous pouvez créer un script de démarrage pour votre instance défense contre les menaces virtuelles afin d'effectuer des tâches automatisées à chaque démarrage de votre instance.

L'exemple suivant montre une configuration Day0 (jour 0) que vous pouvez copier et coller dans le champ **Startup script** (script de démarrage) :

```
{
"AdminPassword": "Cisco@123123",
"Hostname": "ftdv-gcp",
"DNS1": "8.8.8.8",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"ManageLocally": "No"
}
```

Astuces
Pour éviter les erreurs d'exécution, vous devez valider votre configuration de jour 0 à l'aide d'un programme de validation JSON.

g) **Network interfaces** (interfaces réseau) : Configurez les interfaces : 1) gestion, 2) diagnostic, 3) interne, 4) externe.



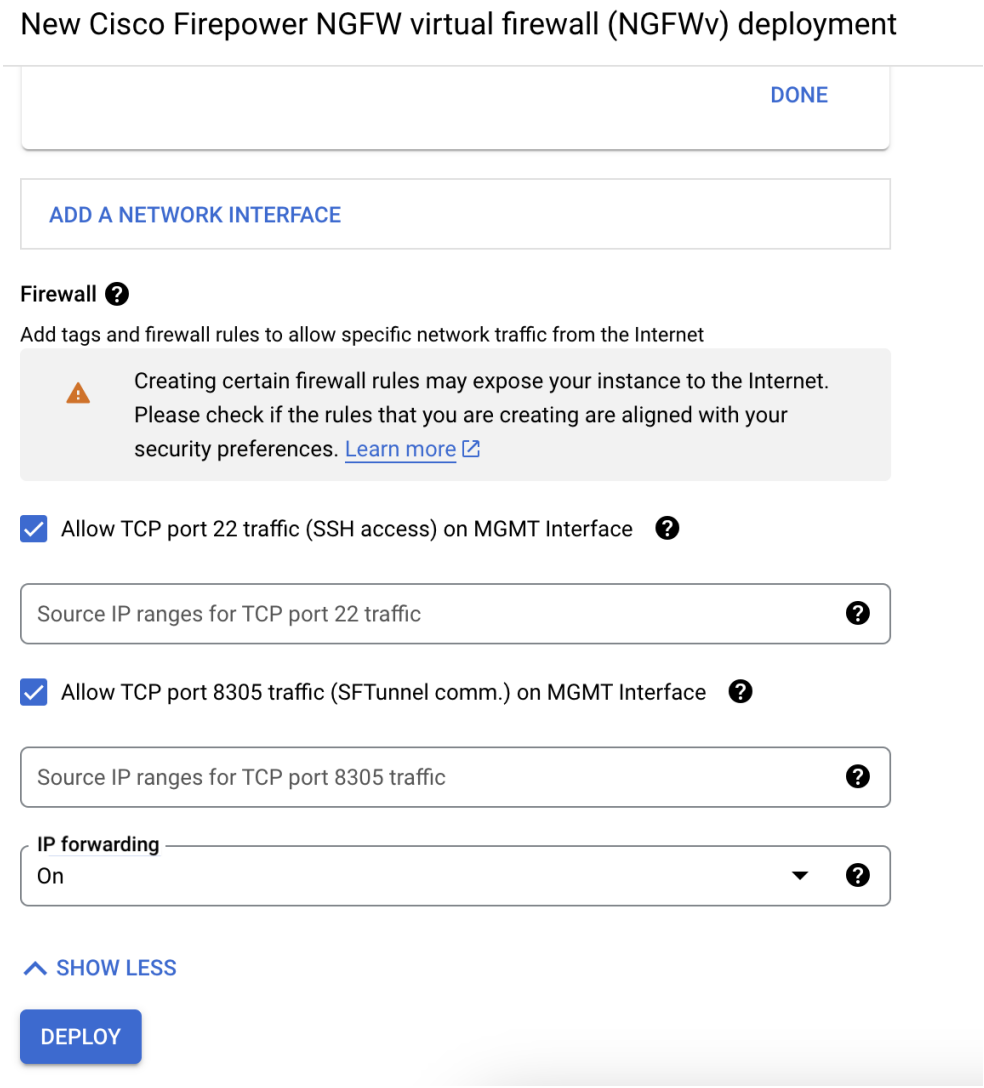
Remarque

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.

1. Dans la liste déroulante **Network** (réseau), sélectionnez un réseau VPC, par exemple, *vpc-asiasouth-mgmt*.
2. Dans la liste déroulante **Subnetwork** (sous-réseau), sélectionnez un sous-réseau.
3. 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). Cette opération est facultative pour les interfaces interne et externe.
4. Cliquez sur **Done (Terminé)**.

h) **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 access) (autoriser le trafic HTTPS de l'Internet (accès FMC)** pour permettre au centre de gestion et aux périphériques gérés de communiquer à l'aide d'un canal de communication chiffré SSL bidirectionnel (SFTunnel).

i) 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 entre sept et huit 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 mesures de contrôle pour arrêter et démarrer l'instance. Vous devez arrêter l'instance si vous devez la modifier.

Se connecter à l'instance Défense contre les menaces virtuelles à l'aide d'une adresse IP externe

L'instance défense contre les menaces virtuelles se voit attribuer une adresse IP interne et une adresse IP externe. Vous pouvez utiliser l'adresse IP externe pour accéder à l'instance défense contre les menaces virtuelles.

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine** > **VM instances** pour accéder aux instances de machine virtuelle du service Compute Engine.

Étape 2 Cliquez sur le nom de l'instance défense contre les menaces virtuelles 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 défense contre les menaces virtuelles 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 Défense contre les menaces virtuelles à l'aide de SSH

Pour vous connecter à l'instance défense contre les menaces virtuelles à partir d'un système de type Unix, connectez-vous à l'instance à l'aide de SSH.

Procédure

Étape 1 Utilisez la commande suivante pour définir les autorisations de fichier afin que seul vous puissiez lire le fichier :

```
$ chmod 400 <private_key>
```

Dans la chaîne ci-haut :

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

Étape 2 Utilisez la commande SSH suivante pour accéder à l'instance :

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

`<nom-utilisateur>` correspond au nom d'utilisateur de l'instance défense contre les menaces virtuelles.

`<public-ip-address>` correspond à l'adresse IP publique de votre instance que vous avez extraite de la console.

Se connecter à l'instance Défense contre les menaces virtuelles à l'aide de la console de série

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine** > **VM instances** pour accéder aux instances de machine virtuelle du service Compute Engine.

Étape 2 Cliquez sur le nom de l'instance défense contre les menaces virtuelles 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 de série).

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

Se connecter à l'instance Défense contre les menaces virtuelles à l'aide de GCloud

Procédure

Étape 1 Dans la console GCP, choisissez **Compute Engine** > **VM instances** pour accéder aux instances de machine virtuelle du service Compute Engine.

Étape 2 Cliquez sur le nom de l'instance défense contre les menaces virtuelles 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.

La solution d'évolutivité automatique

Les sections suivantes décrivent comment les composants de la solution d'évolutivité automatique fonctionnent pour défense contre les menaces virtuelles sur GCP.

Aperçu

L'évolutivité automatique d'Défense contre les menaces virtuelles pour GCP est une implémentation complète sans serveur qui utilise l'infrastructure sans serveur fournie par GCP (fonctions dans le nuage, équilibreurs de charges, publication/abonnement, groupes d'instances, etc.).

Certaines des fonctionnalités clés de l'évolutivité automatique d'Défense contre les menaces virtuelles pour la mise en œuvre de GCP comprennent :

- Déploiement basé sur le modèle de gestionnaire de déploiement GCP.
- Prise en charge des mesures d'évolutivité en fonction du CPU.
- Prise en charge du déploiement d'défense contre les menaces virtuelles et des zones de multi-disponibilité.
- Prise en charge de l'enregistrement et de l'annulation de l'enregistrement automatique de défense contre les menaces virtuelles.
- La configuration entièrement automatisée s'applique automatiquement aux instances défense contre les menaces virtuelles soumise à l'évolutivité à la hausse.
- Prise en charge de l'application automatique de la politique de NAT, de la politique d'accès et des routes, à défense contre les menaces virtuelles.
- Prise en charge des équilibreurs de charges et des zones de multi-disponibilité.

- Prise en charge de centre de gestion virtuel sur d'autres plateformes.
- Cisco fournit un paquet de déploiement de l'évolutivité automatique pour GCP afin de faciliter le déploiement.

Lignes directrices et limites relatives à la licence

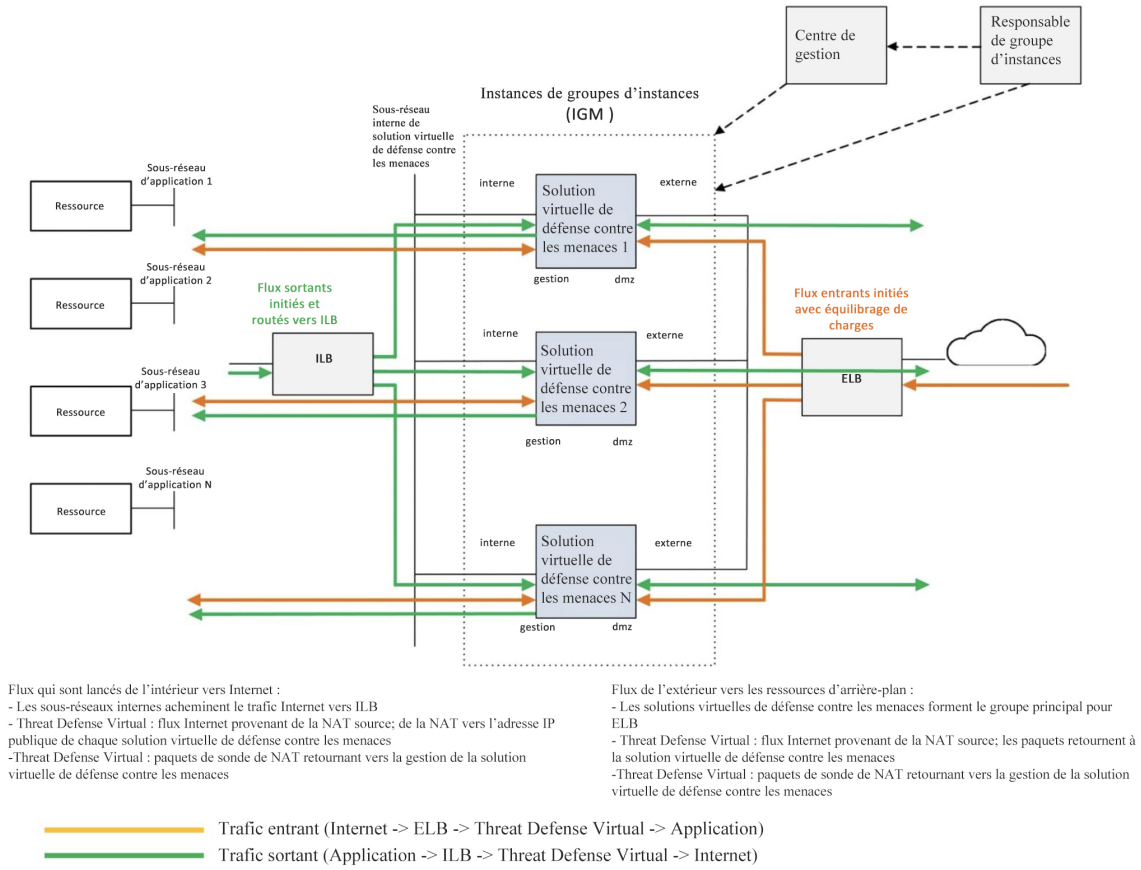
- Seul IPv4 est pris en charge.
- Licences : Seul le protocole BYOL est pris en charge. Les licences PAYG ne sont pas prises en charge.
- Les erreurs de fonctionnalité des périphériques ne s'affichent pas dans les journaux.
- Le nombre maximal d'interfaces prises en charge est de 25. Il s'agit de la limite maximale dans une instance centre de gestion virtuel .
- Sur toutes les versions de Cisco Secure Firewall, vous pouvez utiliser les modèles fournis pour déployer la solution d'évolutivité automatique de Threat Defense Virtual. Les instances de Threat Defense Virtual sont déployées avec un minimum de quatre interfaces : une interface de gestion, une interface de diagnostic et deux interfaces de données.
- Les méthodes de veille à froid ou d'instantané pour réduire le délai d'évolution ne sont pas prises en charge.
- L'évolutivité basée sur une planification n'est pas prise en charge.
- L'évolutivité automatique basée sur l'utilisation moyenne de la mémoire n'est pas prise en charge.
- Les fonctionnalités d'évolutivité à la hausse ou à la baisse peuvent faire augmenter ou diminuer le nombre d'instances de plus d'une instance à la fois. Cependant, les instances défense contre les menaces virtuelles s'annuleront ou s'enregistreront séquentiellement sur centre de gestion virtuel , c'est-à-dire une par une.
- Pendant l'évolutivité à la baisse, il y a une durée de déversement de la connexion de 300 sec. Vous pouvez également configurer manuellement le temps de déversement selon une période requise.
- L'équilibreur de charges externe est créé par le modèle fourni. La personnalisation des exigences DNS de l'adresse IP publique de l'équilibreur de charges n'est pas prise en charge.
- Les utilisateurs doivent intégrer leur infrastructure existante dans le modèle de mise en œuvre en sandwich.
- Pour en savoir plus sur les erreurs rencontrées au cours du processus d'évolutivité à la hausse et à la baisse, analysez les journaux des fonctions du nuage.
- La NAT, les politiques de sécurité associées au groupe d'appareils et les routes statiques sont appliquées au nouveau Défense contre les menaces.
- Si vous déployez la solution sur plus d'un défense contre les menaces virtuelles, le temps de déploiement augmentera, car centre de gestion virtuel ne peut gérer qu'une seule demande d'enregistrement à la fois. Le temps de déploiement augmente également lorsque l'évolutivité à la hausse ajoute plusieurs instances défense contre les menaces virtuelles. Actuellement, tous les enregistrements et toutes les annulations d'enregistrements sont séquentiels.
- Le groupe d'appareils, les règles de NAT et les objets réseau doivent être créés dans centre de gestion virtuel avant que l'évolutivité automatique ne soit lancée. Notez que les adresses IP ILB et ELB ne sont disponibles qu'après le déploiement de la solution. Ainsi, vous pouvez créer des objets fictifs et mettre à jour les objets après l'obtention des adresses IP réelles.

Scénario d'évolutivité automatique

L'évolutivité automatique de défense contre les menaces virtuelles pour GCP est une solution d'évolutivité horizontale automatisée qui positionne un groupe d'instances défense contre les menaces virtuelles entre un équilibreur de charges interne (ILB) et un équilibreur de charges externe (ELB) de GCP.

- L'ELB distribue le trafic Internet aux instances défense contre les menaces virtuelles du groupe d'instances; le défense contre les menaces virtuelles transfère ensuite le trafic à l'application.
- L'ILB distribue le trafic Internet sortant d'une application aux instances défense contre les menaces virtuelles du groupe d'instances; le défense contre les menaces virtuelles transfère ensuite le trafic à Internet.
- Un paquet réseau ne traversera jamais les deux équilibreurs de charges (interne et externe) en une seule connexion.
- Le nombre d'instances défense contre les menaces virtuelles dans l'ensemble d'évolutivité se verra évoluer et sera configuré automatiquement en fonction des conditions de charge.

Illustration 2 : Scénario d'évolutivité automatique de Défense contre les menaces virtuelles



Champ d'application

Ce document aborde les procédures détaillées pour déployer les composants sans serveur pour la solution Défense contre les menaces virtuelles d'évolutivité automatique pour GCP.

Important

- Lisez le document entier avant de commencer le déploiement.
- Assurez-vous que les conditions préalables sont remplies avant de commencer le déploiement.
- Assurez-vous de suivre les étapes et l'ordre d'exécution décrits dans le présent document.

Télécharger le paquet de déploiement

La solution d'évolutivité automatique d'Défense contre les menaces virtuelles pour GCP est un déploiement basé sur le modèle de gestionnaire de déploiement GCP qui utilise l'infrastructure sans serveur fournie par GCP (fonctions dans le nuage, équilibreurs de charges, publication/abonnement, groupes d'instances, etc.).

Téléchargez les fichiers requis pour lancer la solution d'évolutivité automatique de défense contre les menaces virtuelles pour GCP. Les scripts et les modèles de déploiement pour votre version défense contre les menaces virtuelles sont disponibles dans le référentiel GitHub.

Attention Remarque : Les scripts et les modèles de déploiement fournis par Cisco pour l'évolutivité automatique sont présentés à titre d'exemples de code source libre et ne font pas l'objet de l'assistance technique du TAC dans sa portée normale.

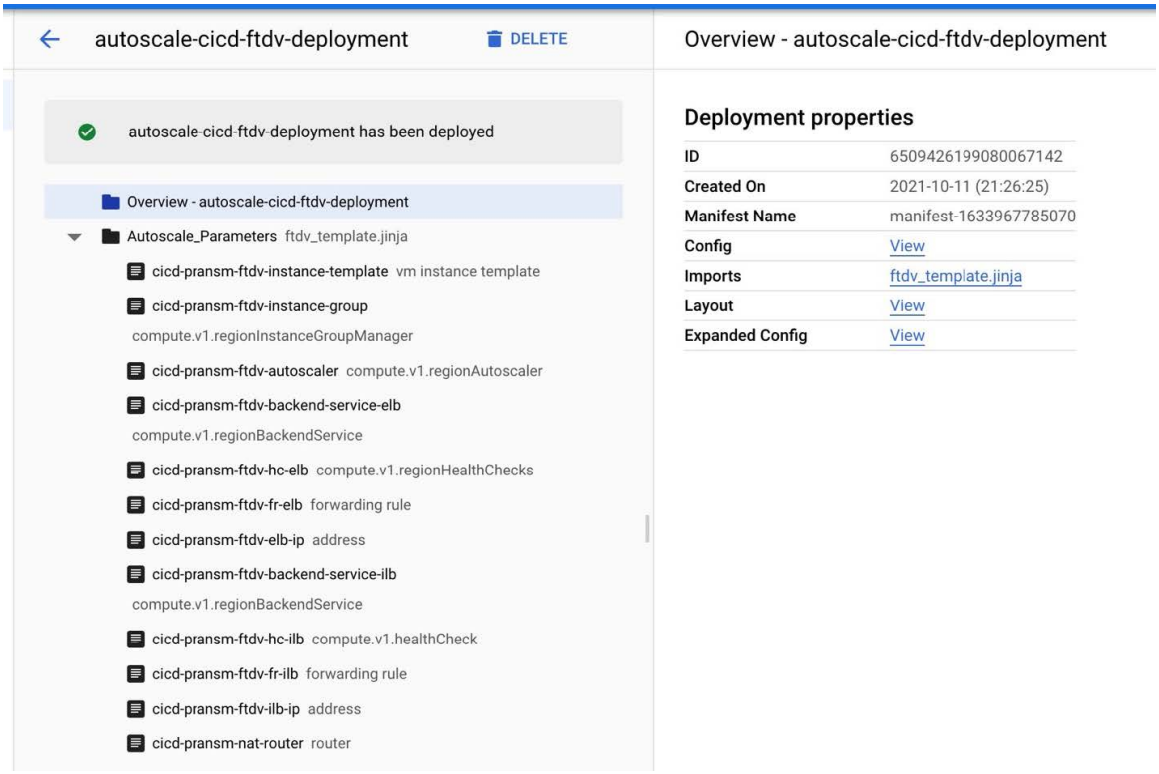
Configuration système requise

Les composants suivants constituent la solution d'évolutivité automatique Défense contre les menaces virtuelles pour GCP.

Gestionnaire de déploiement

- Traitez votre configuration comme du code et effectuez des déploiements reproductibles. Google Cloud Deployment Manager vous permet de spécifier toutes les ressources nécessaires à votre application dans un format explicite à l'aide de YAML. Vous pouvez également utiliser des modèles Jinja2 pour paramétrer la configuration et permettre la réutilisation des schémas de déploiement courants.
- Créez des fichiers de configuration qui définissent les ressources. Le processus de création de ces ressources peut être répété à plusieurs reprises avec des résultats cohérents. Consultez https://cloud.google.com/deployment-manager/docs pour de plus amples renseignements.

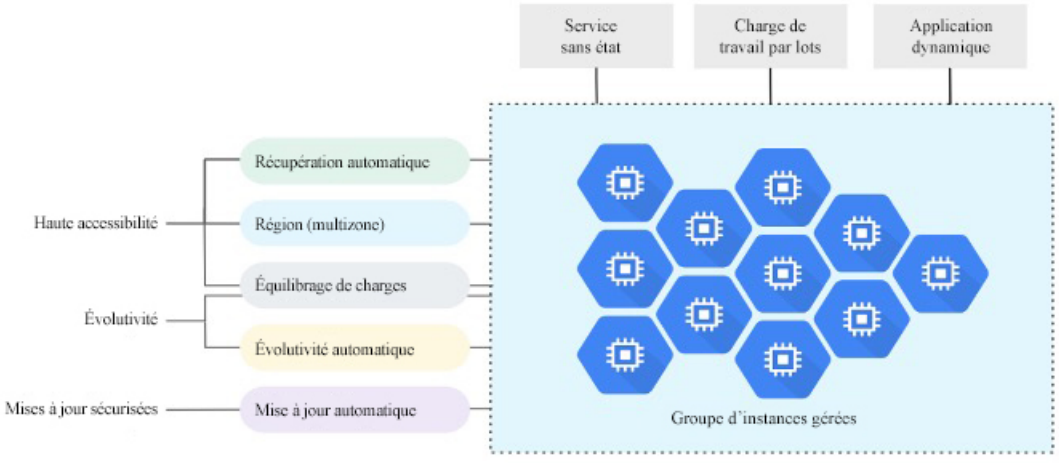
Illustration 3 : Vue du gestionnaire de déploiement



Groupe d'instances gérées dans GCP

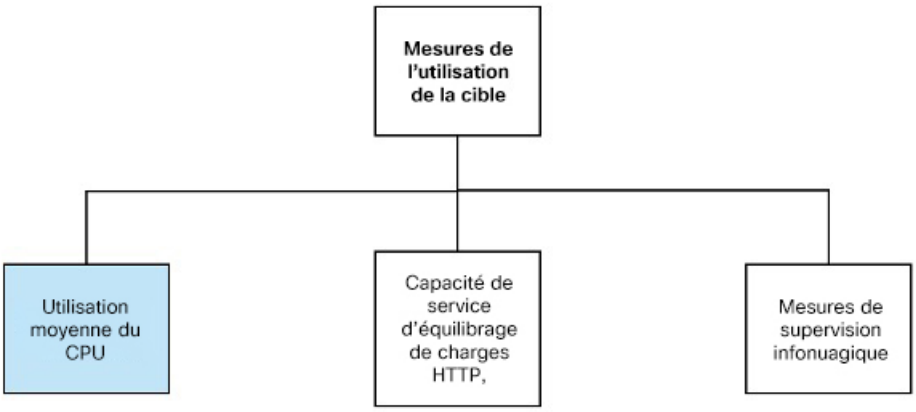
Un groupe d'instances gérées (MIG) crée chacune de ses instances gérées en fonction du modèle d'instance et de la configuration dynamique facultative que vous spécifiez. Consultez https://cloud.google.com/compute/docs/instance-groups pour de plus amples renseignements.

Illustration 4 : Fonctionnalités du groupe d'instances



Mesures de l'utilisation de la cible

- Le diagramme suivant présente les mesures d'utilisation de la cible. Seules les mesures d'utilisation moyenne du CPU sont utilisées pour prendre des décisions en matière d'évolutivité automatique.
- Le dispositif d'évolutivité automatique recueille en permanence des renseignements sur l'utilisation en fonction de la mesure d'utilisation sélectionnée, compare l'utilisation réelle à votre utilisation cible souhaitée et utilise ces renseignements pour déterminer si le groupe doit supprimer des instances (évolutivité à la baisse) ou ajouter des instances (évolutivité à la hausse).
- Le niveau d'utilisation cible est le niveau auquel vous souhaitez maintenir vos instances de machine virtuelle (VM). Par exemple, si vous évoluez en fonction de l'utilisation du CPU, vous pouvez définir votre niveau d'utilisation cible à 75 % et le dispositif d'évolutivité automatique maintiendra l'utilisation du CPU du groupe d'instances spécifié à 75 %. Le niveau d'utilisation de chaque mesure est interprété différemment en fonction de la politique d'évolutivité automatique. Consultez https://cloud.google.com/compute/docs/autoscaler pour de plus amples renseignements.



Fonctions de nuage sans serveur

Vous utilisez les fonctions Google Cloud sans serveur pour des tâches telles que la modification du mot de passe SSH, la configuration du gestionnaire, l'enregistrement de défense contre les menaces virtuelles sur centre de gestion virtuel , la désinscription défense contre les menaces virtuelles sur centre de gestion virtuel , etc.

- Lorsqu'une nouvelle instance défense contre les menaces virtuelles apparaît dans le groupe d'instances au cours du processus d'évolutivité à la hausse, vous devez effectuer des tâches telles que la modification du mot de passe SSH, la configuration du gestionnaire, l'enregistrement de défense contre les menaces virtuelles sur centre de gestion virtuel , l'annulation de l'enregistrement de défense contre les menaces virtuelles sur centre de gestion virtuel , etc.
- Les fonctions du nuage sont déclenchées par un sujet de publication ou d'abonnement en nuage pendant le processus d'évolutivité à la hausse. Vous disposez également d'un récepteur de journaux avec un filtre exclusif à l'ajout d'instances lors de l'évolutivité à la hausse.

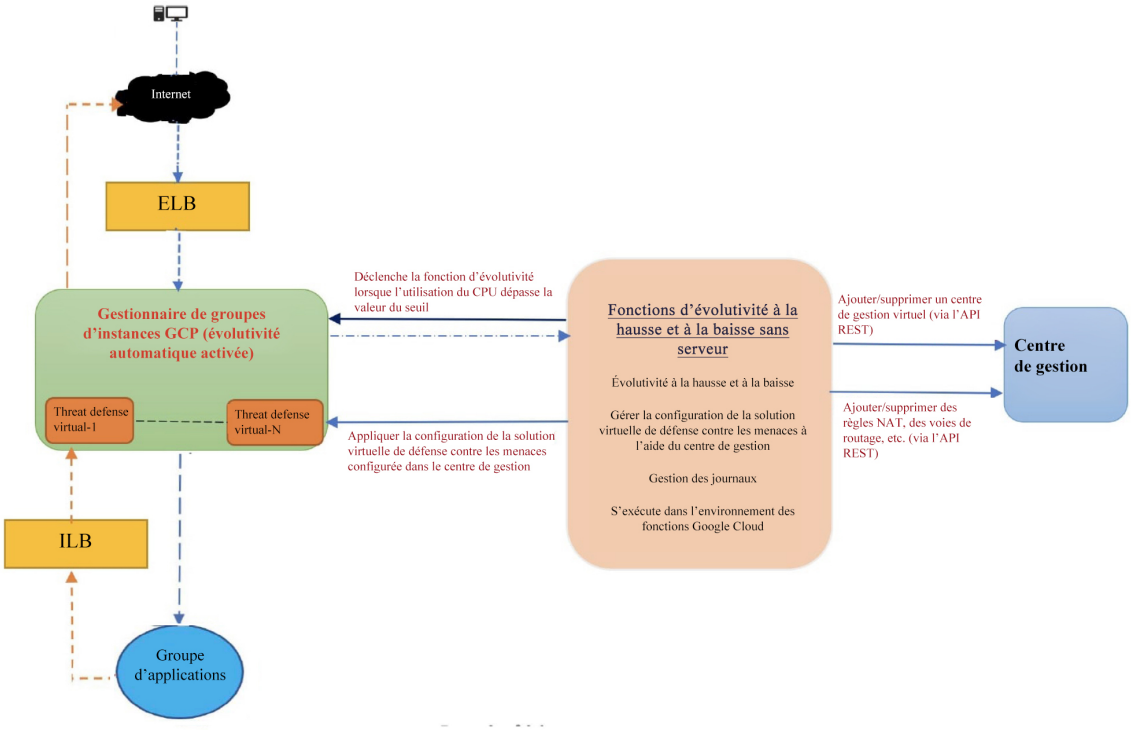
Annulation de l'enregistrement de la licence sans serveur à l'aide des fonctions du nuage

- Pendant que les instances sont supprimées lors de l'évolutivité à la baisse, vous devez annuler l'enregistrement de la licence de l'instance défense contre les menaces virtuelles et annuler l'enregistrement de défense contre les menaces virtuelles sur centre de gestion virtuel .

- Les fonctions du nuage sont déclenchées par un sujet de publication ou d'abonnement en nuage. En particulier pour le processus de suppression, vous disposez d'un récepteur de journaux avec un filtre exclusif à la suppression des instances lors de l'évolutivité à la baisse.
- La fonction du nuage, lorsqu'elle est déclenchée, se connecte en SSH à l'instance défense contre les menaces virtuelles à supprimer et exécute la commande pour annuler l'enregistrement de la licence.

Présentation générale de la solution d'évolutivité automatique

Illustration 5 : Survolde la solution d'évolutivité automatique



Conditions préalables

Ressources GCP

Projet GCP

Un projet existant ou nouvellement créé est requis pour déployer tous les composants de cette solution.

Réseaux VPC

Assurez-vous que quatre VPC sont disponibles ou créés. Un déploiement de l'évolutivité automatique ne créera, ne modifiera ni ne gérera de ressources réseau.

En plus des sous-réseaux existants, créez un nouveau connecteur VPC dans le réseau VPC de gestion avec un sous-réseau /28. La fonction en nuage utilise le connecteur VPC pour accéder au défense contre les menaces virtuelles à l'aide d'adresses IP privées.

défense contre les menaces virtuelles nécessite quatre interfaces réseau. Par conséquent, votre réseau virtuel nécessite quatre sous-réseaux pour :

- Le trafic externe
- Le trafic interne
- Le trafic de gestion
- Le trafic de diagnostic

Pare-feu

Des règles de pare-feu qui permettent la communication inter-VPC et permettent également la création de sondes d'intégrité.

Créez quatre règles de pare-feu pour les interfaces interne, externe, de gestion et de diagnostic. En outre, vous devez créer une règle de pare-feu pour autoriser les sondes de vérification de l'intégrité.

Les adresses IP des sondes de vérification de l'intégrité sont indiquées ci-dessous :

- 35.191.0.0/16
- 130.211.0.0/22
- 209.85.152.0/22
- 209.85.204.0/22

Vous devez noter les balises de pare-feu, qui sont utilisées plus tard dans le modèle de gestionnaire de déploiement.

Les ports suivants doivent être ouverts dans le groupe de sécurité réseau auquel les sous-réseaux sont connectés :

- SSH (TCP/22) : requis pour la sonde d'intégrité entre l'équilibreur de charges et défense contre les menaces virtuelles. Requis pour la communication entre les fonctions sans serveur et défense contre les menaces virtuelles.
- Protocole/ports spécifiques à l'application : requis pour toutes les applications des utilisateurs (par exemple, TCP/80, etc.).

Créer le paquet de fonction en nuage de GCP

La solution d'évolutivité automatique Défense contre les menaces virtuelles vous oblige à créer deux fichiers d'archive qui fournissent les fonctions en nuage sous la forme de paquet ZIP compressé.

- `ftdv_scalein.zip`
- `ftdv_scaleout.zip`

Consultez les instructions de déploiement Auto Scale pour savoir comment créer les paquets `ftdv_scalein.zip` et `ftdv_scaleout.zip`.

Ces fonctions sont aussi distinctes que possible pour effectuer des tâches spécifiques et peuvent être mises à niveau au besoin pour des améliorations et du soutien de nouvelles versions.

Paramètres d'entrée

Le tableau suivant définit les paramètres du modèle et fournit un exemple. Une fois que vous avez choisi ces valeurs, vous pouvez utiliser ces paramètres pour créer le périphérique défense contre les menaces virtuelles lorsque vous déployez le modèle de gestionnaire de déploiement GCP dans votre projet GCP.

Tableau 4 : Paramètres du modèle

Nom du paramètre	Type/valeurs autorisés	Description
resourceNamePrefix	Chaîne	Toutes les ressources sont créées avec un nom contenant ce préfixe. Exemple : demo-test
region	Régions valides prises en charge par GCP [Chaîne]	Nom de la région où le projet sera déployé. Exemple : us-central1
serviceAccountMailId	Chaîne [ID de courriel]	Adresse courriel qui identifie le compte de service.
vpcConnectorName	Chaîne	Nom du connecteur qui gère le trafic entre votre environnement sans serveur et votre réseau VPC. Exemple : demo-test-vpc-connector
adminPassword	Chaîne	Mot de passe initial pour l'instance virtuelle de défense contre les menaces. Plus tard, ce paramètre est remplacé par « newFtdPasswordSecret ».
bucketName	Chaîne	Nom du compartiment de stockage GCP dans lequel le progiciel ZIP de la fonction en nuage sera chargé. Exemple : demo-test-bkt
coolDownPeriodSec	Nombre entier	Nombre de secondes que l'évolutivité automatique doit attendre avant de commencer à collecter des informations à partir d'une nouvelle instance. Exemple : 30

Nom du paramètre	Type/valeurs autorisés	Description
cpuUtilizationTarget	Décimal (0, 1]	L'utilisation moyenne du CPU des machines virtuelles du groupe d'instances que l'évolutivité automatique doit maintenir. Exemple : 0.5
deployUsingExternalIP	Booléen	Décidez si la gestion de Threat Defense Virtual doit avoir une adresse IP publique. Exemple : « true » (vrai) Si la valeur est True (vrai), le Threat Defense Virtual doit avoir une adresse IP publique. Si la valeur est False (faux), une adresse IP publique n'est pas requise.
diagFirewallRule	Chaîne	Nom de la règle de pare-feu créée pour le VPC de diagnostic. Exemple : cisco-ftdv-diag-firewall-rule
diagSubnetworkName	Chaîne	Nom du sous-réseau VPC utilisé pour l'interface de diagnostic. Exemple : cisco-ftdv-diag-subnet
diagVpcName	Chaîne	Nom du VPC utilisé pour l'interface de diagnostic. Exemple : custom-ftdv-diag-vpc
elbFePorts	Nombre entier	Ports Ethernet du Fast Ethernet. Exemple : 80,22
elbIpProtocol	Chaîne	Protocole IP ELB utilisé. Exemple : TCP
elbPort	Nombre entier	Numéro de port ELB. Exemple : 80
elbPortName	Chaîne	Nom du port ELB. Exemple : tcp
elbPortRange	Nombre entier	Plage de ports ELB. Exemple : 80-80

Nom du paramètre	Type/valeurs autorisés	Description
elbProtocol	Chaîne	Protocole ELB utilisé. Exemple : TCP
elbProtocolName	Chaîne	Nom du protocole ELB. Exemple : TCP
elbTimeoutSec	Nombre entier	Période d'expiration d'ELB en secondes. Exemple : 5
elbUnhealthyThreshold	Nombre entier	Numéro de seuil pour les échecs de vérification de l'intégrité. Exemple : 2
fmcIP	Chaîne	Adresse IP du centre de gestion Exemple : 10.61.1.2
fmcPasswordSecrt et nouveau new FtdPasswordSecret	Chaîne	Noms des secrets créés.
fmcUsername	Chaîne	nom d'utilisateur Centre de gestion virtuel .
ftdvCheckIntervalSec	Nombre entier	Intervalle entre les vérifications d'intégrité. Exemple : 300
ftdvHealthCheckPort	Nombre entier	Numéro de port pour le contrôle d'intégrité Défense contre les menaces virtuelles. Exemple : 22
ftdvHealthCheckProtocolName	Chaîne	Protocole utilisé pour la vérification de l'intégrité. Exemple : TCP
ftdvPassword	Chaîne	mot de passe Défense contre les menaces virtuelles.
ftdvTimeoutSec	Nombre entier	Délai d'expiration pour la connexion Défense contre les menaces virtuelles. Exemple : 300
ftdvUnhealthyThreshold	Nombre entier	Numéro de seuil pour les échecs de vérification de l'intégrité. Exemple : 3

Nom du paramètre	Type/valeurs autorisés	Description
grpID	Chaîne	Nom du groupe d'appareils créé dans centre de gestion. Exemple : auto-group
healthCheckFirewallRule	Chaîne	Nom de la règle de pare-feu qui autorise les paquets des plages d'adresses IP de sonde de vérification de l'intégrité. Exemple : Custom-ftdv-hc-firewall-rule
healthCheckFirewallRuleName	Chaîne	Balise de la règle de pare-feu qui autorise les paquets des plages d'adresses IP de sonde de vérification de l'intégrité. Exemple : demo-test-health-allow-all
ilbCheckIntervalSec	Nombre entier	Intervalle pour vérifier la connexion ILB. Exemple : 10
ilbDrainingTimeoutSec	Nombre entier	Période de vidange de la connexion. Exemple : 60
IlbPort	Nombre entier	Numéro de port ELB. Exemple : 80
ilbProtocol	Chaîne	Protocole ELB utilisé. Exemple : TCP
ilbProtocolName	Chaîne	Nom du protocole ILB. Exemple : TCP
ilbTimeoutSec	Nombre entier	Période d'expiration d'ILB. Exemple : 5
ilbUnhealthyThreshold	Nombre entier	Numéro de seuil pour les échecs de vérification de l'intégrité. Exemple : 3
insideFirewallRule	Chaîne	Nom de la règle de pare-feu interne. Exemple : custom-ftdv-in-firewall-rule

Nom du paramètre	Type/valeurs autorisés	Description
insideFirewallRuleName	Chaîne	Balise des règles de pare-feu qui permet la communication dans le VPC interne. Exemple : demo-test-inside-allowall
insideGwName	Chaîne	Nom de la passerelle interne. Exemple : inside-gateway
insideSecZone	Chaîne	Sélection de la zone de sécurité interne. Exemple : inside-zone
insideSubnetworkName	Chaîne	Nom du sous-réseau interne. Exemple : custom-ftdv-inside-subnet
insideVPCName	Chaîne	Nom du VPC interne. Exemple : demo-test-inside
insideVPCSubnet	Chaîne	Nom du sous-réseau interne. Exemple : demo-test-inside-subnet
licenceCAPS	Chaîne	Noms des licences utilisées. Exemple : BASE, MALWARE, URL Filter, THREAT
machineType	Chaîne	Type de machine pour la machine virtuelle défense contre les menaces virtuelles. Exemple : n1-standard-4
maxFTDCount	Nombre entier	Le nombre maximal d'instances Défense contre les menaces virtuelles autorisées dans le groupe d'instances. Exemple : 3
maxFTDReplicas	Nombre entier	Nombre maximal d'instances Défense contre les menaces virtuelles dans le groupe d'évolutivité automatique. Exemple : 2

Nom du paramètre	Type/valeurs autorisés	Description
mgmtFirewallRule	Chaîne	Nom de la règle de pare-feu de gestion. Exemple : cisco-ftdv-mgmt-firewall-rule
mgmtFirewallRuleName	Chaîne	Balise des règles de pare-feu qui permet la communication dans le VPC de gestion. Exemple : demo-test-mgmt-allowall
mgmtSubnetworkName	Chaîne	Nom des sous-réseaux de gestion. Exemple : custom-ftdv-mgmt-subnet
mgmtVPCName	Chaîne	Nom du VPC de gestion. Exemple : demo-test-mgmt
mgmtVPCSubnet	Chaîne	Nom du sous-réseau de gestion. Exemple : demo-test-mgmt-subnt
minFTDCount	Nombre entier	Le nombre minimal d'instances Défense contre les menaces virtuelles disponibles dans le groupe d'instances à tout moment. Exemple : 1
minFTDReplicas	Nombre entier	Le nombre minimal d'instances Défense contre les menaces virtuelles dans le groupe d'évolutivité automatique. Exemple : 2
natID	Chaîne	Identifiant de NAT unique requis lors de l'enregistrement de centre de gestion sur Défense contre les menaces.
outsideFirewallRule	Chaîne	Nom de la règle de pare-feu externe. Exemple : cisco-ftdv-out-firewall-rule
outsideFirewallRuleName	Chaîne	Balise des règles de pare-feu qui permet la communication dans le VPC externe. Exemple : demo-test-outside-allowall

Nom du paramètre	Type/valeurs autorisés	Description
outsideGwName	Chaîne	Nom de la passerelle externe. Exemple : outside-gateway
outsideSecZone	Chaîne	Sélection de la zone de sécurité externe. Exemple : outside-zone
outsideSubnetworkName	Chaîne	Nom du sous-réseau externe. Exemple : custom-ftdv-outside-subnet
outsideVPCName	Chaîne	Nom du VPC externe. Exemple : demo-test-outside
outsideVPCSubnet	Chaîne	Nom du sous-réseau externe. Exemple : demo-test-outside-subnt
policyID	Chaîne	Nom de la politique d'ACL.
publicKey	Chaîne	Clé SSH de la machine virtuelle Défense contre les menaces virtuelles.
sourceImageURL	Chaîne	URL de l'image Défense contre les menaces virtuelles qui doit être utilisé dans le projet.
sshUsingExternalIP	Booléen	Détermine si les fonctions Google utilisent une adresse IP publique ou une adresse IP privée. Exemple : « true » (vrai) Si la valeur est définie sur « true », les fonctions Google utilisent une adresse IP publique. Si la valeur est définie sur « false », les fonctions Google utilisent une adresse IP privée.

Déployer la solution d'évolutivité automatique

Procédure

Étape 1 Copiez le référentiel Git dans un dossier local.

```
git clone git_url -b branch_name
```

Étape 2 Créez le compartiment dans l'interface de ligne de commande gcloud.

```
gsutil mb -c nearline gs://bucket_name
```

Remarque
Exécutez les commandes **gsutil** ou **gcloud** au cours de cette procédure dans Google Cloud Shell ou le SDK Google Cloud installé sur votre système.

Étape 3 Créez des paquets zip compressés :

a) Créez des paquets zip compressés contenant les fichiers suivants à partir des dossiers `ftdv_scaleout` et `ftdv_scalein`.

- main.py
- basic_functions.py
- fmc_functions.py
- requirements.txt

Remarque
Dans le fichier main.py, utilisez la commande **ssh_ip = response['networkInterfaces'] [2] ['networkIP']** si une adresse IP interne est utilisée. Si une adresse IP externe est utilisée, saisissez la commande **ssh_ip = response['networkInterfaces'] [2] ['accessConfigs'] [0] ['natIP']** . De plus, deux routes statiques sont ajoutées dans cette fonction. Vous pouvez modifier les routes statiques à l'aide des commandes **fmc.create_static_network_route (vm_name, 'outside', 'any_ipv4', os.getenv("OUTSIDE_GW_NAME"), metric=1)** et **fmc.create_static_network_route (vm_name, 'inside', 'any_ipv4', os.getenv("INSIDE_GW_NAME"), metric=2)**.

b) Renommez les paquets zip compressés en `ftdv_scaleout.zip` et `ftdv_scalein.zip`.

Remarque
Naviguez dans le dossier, sélectionnez les fichiers, cliquez avec le bouton droit et sélectionnez « compress | archive » (compresser | archiver) pour créer un fichier.zip que GCP peut lire.

Étape 4 Chargez les paquets zip compressés (`ftdv_scaleout.zip` et `ftdv_scalein.zip`) dans l'espace de travail de l'éditeur en nuage.

Étape 5 Chargez les fichiers suivants du modèle de gestionnaire de déploiement dans l'espace de travail de l'éditeur en nuage.

- ftdv_predeployment.yaml
- ftdv_predeployment.jinja
- ftdv_parameters.yaml
- ftdv_template.jinja

Étape 6 Copiez les paquets zip compressés dans le compartiment de stockage.

- `gsutil cp ftdv_scaleout.zip gs://bucket_name`
- `gsutil cp ftdv_scalein.zip gs://bucket_name`

Étape 7 Créez un VPC et un sous-réseau pour les interfaces internes, externes et de gestion.

Dans le VPC de gestion, vous devez avoir un sous-réseau/28, par exemple, 10.8.2.0/28.

Étape 8 Vous avez besoin de quatre règles de pare-feu pour les interfaces interne, externe, de gestion et de diagnostic. En outre, vous devez avoir une règle de pare-feu pour autoriser les sondes de vérification de l'intégrité.

Étape 9 Créez deux secrets pour les éléments suivants à l'aide de l'interface graphique utilisateur de Secret Manager. Consultez https://console.cloud.google.com/security/secret-manager.

- fmc-password
- ftdv-new-password

Étape 10 Créez le connecteur VPC.

```
gcloud beta compute networks vpc-access connectors create <vpc-connector-name>
--region <region> --subnet=</28 subnet name>
```

Exemple :

```
gcloud beta compute networks vpc-access connectors create demo-vpc-connector
--region us-central1 --subnet=outside-connect-28
Create request issued for: [demo-vpc-connector]
Waiting for operation [projects/asavgcp-poc-4krn/locations/us-central1/operations/
10595de7-837f-4c19-9396-0c22943ecf15] to complete...done.
Created connector [demo-vpc-connector].
```

Étape 11 Déployez centre de gestion virtuel sur n'importe quelle plateforme en nuage public avec une adresse IP publique. Consultez le Guide de démarrage de Cisco Secure Firewall Management Center Virtual pour en savoir plus sur le déploiement de centre de gestion virtuel sur diverses plateformes de nuage public.

Remarque
Exécutez les étapes 12 à 16 sur l'instance centre de gestion virtuel déployée.

Étape 12 Sur l'instance centre de gestion virtuel , créez un utilisateur restapi pour centre de gestion virtuel et utilisez le même mot de passe que celui enregistré dans le secret fmcpassword. Consultez la section sur les utilisateurs (Users) pour en savoir plus.

Étape 13 Sur l'instance centre de gestion virtuel , créez un groupe d'appareils, une politique de contrôle d'accès et une règle de contrôle d'accès. Consultez l'information sur l'ajout d'un groupe d'appareils, la création d'une politique de contrôle d'accès de base et de Création et de modification des règles de contrôle d'accès pour de plus amples renseignements.

Étape 14 Sur l'instance centre de gestion virtuel , créez les objets ci-dessous. Consultez la gestion des objets pour plus d'informations sur la création d'objets sur centre de gestion virtuel .

- ELB-IP
- ILB-IP
- Application-IP
- Plages d'adresses IP de vérification la de l'intégrité (4)
- Métadonnées

```
object network hc1
  subnet 35.191.0.0 255.255.0.0
object network metadata
  host 169.254.169.254
object network ilb-ip
  host 10.52.1.218
object network hc2
```

```
  subnet 130.211.0.0 255.255.252.0
object network elb-ip
  host 34.85.214.40
object network hc3
  subnet 209.85.152.0 255.255.252.0
object network hc4
  subnet 209.85.204.0 255.255.252.0
object network inside-linux
  host 10.52.1.217
object network outside-gateway
  host <>
object network inside-gateway
  host <>
```

Étape 15 Sur l'instance centre de gestion virtuel : Créez des zones de sécurité (objets d'interface). Consultez la création d'objets de zone de sécurité et de groupe d'interface pour en savoir plus.

- inside-security-zone
- outside-security-zone

Étape 16 Sur l'instance centre de gestion virtuel , créez la politique de NAT et les règles de NAT. Pour en savoir plus, consultez l'information sur la traduction d'adresses réseau.

```
nat (inside,outside) source dynamic hc1 interface destination static ilb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (inside,outside) source dynamic hc2 interface destination static ilb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (inside,outside) source dynamic any interface
nat (outside,inside) source dynamic hc1 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic hc2 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic hc3 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic hc4 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic any interface destination static elb-ip inside-linux
```

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
1	→	D...	inside-zone	outside-zone	hc1	ilb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
2	→	D...	inside-zone	outside-zone	hc2	ilb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
3	→	D...	inside-zone	outside-zone	any-ipv4			Interface			Dns:false
4	→	D...	outside-zone	inside-zone	hc1	elb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
5	→	D...	outside-zone	inside-zone	hc2	elb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
6	→	D...	outside-zone	inside-zone	hc3	elb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
7	→	D...	outside-zone	inside-zone	hc4	elb-ip	Original HTTP	Interface	metadata	Original HTTP	Dns:false
8	→	D...	outside-zone	inside-zone	any-ipv4	elb-ip		Interface	inside-linux		Dns:false

Étape 17 Mettez à jour les paramètres dans les fichiers Jinja et YAM pour les prédéploiements préalables et le déploiement de l'évolutivité automatique Défense contre les menaces virtuelles.

a) Ouvrez le fichier `ftdv_predeployment.yaml` et mettez à jour les paramètres suivants.

- **resourceNamePrefix** : <resourceNamePrefix>
- **region** : <region>

- **serviceAccountMailId** : <serviceAccountMailId>
- **vpcConnectorName** :<VPC-Connector-Name>
- **bucketName** :<bucketName>
- **fmcIP** : <centre de gestion-IP-address>
- **IregID** : <registration-ID>
- **natID** :<unique-NAT-ID>
- **grpID** :<device-group-name>
- **policyID** : <acl-policy-name>
- **licenseCAPS** : <licenses>
- **fmcPasswordSecret** : <centre de gestion-password>
- **newFtdPasswordSecret** : <new-défense contre les menaces virtuelles-password>
- **fmcUsername** : <username>
- **ftdvPassword** : <password>
- **outsideGwName** : <outside-gateway-name>
- **insideGwName** : <inside-gateway-name>
- **outsideSecZone** : <outside-security-zone>
- **insideSecZone** : <inside-security-zone>
- **sshUsingExternalIP** : <true/false>

b) Le fichier `ftdv_predeployment.jinja` prend les paramètres du fichier `ftdv_predeployment.yaml`.
c) Ouvrez le fichier `ftdv_parameters.yml` et mettez à jour les paramètres suivants.

VPC and Firewall Parameters

- **mgmtVpcName** : <mgmt-vpc-name>
- **diagVpcName** : <diagnostic-vpc-name>
- **outsideVpcName** : <outside-vpc-name>
- **insideVpcName** : <inside-vpc-name>
- **mgmtSubnetworkName** : <mgmt-subnet-name>
- **diagSubnetworkName** : <diagnostic-subnet-name>
- **outsideSubnetworkName** : <outside-subnet-name>
- **insideSubnetworkName** : <inside-subnet-name>
- **mgmtFirewallRule** : <mgmt-firewall-rule>
- **diagFirewallRule** : <diagnostic-firewall-rule>
- **outsideFirewallRule** : <outside-firewall-rule>

- **insideFirewallRule** : <inside-firewall-rule>
- **healthCheckFirewallRule** : <healthcheck-firewall-rule>
- **adminPassword** : <initial-défense contre les menaces virtuelles-password>
- **deployUsingExternalIP** : <true/false>

Instance Template parameters

- **Type de machine** : <machine-type>
- **source ImageURL** : <source-image-URL>

FTDv Health Check

- **ftdvHealthCheckPort** : <port-number>
- **ftdvCheckIntervalSec** : <interval-in-seconds>
- **ftdvTimeoutSec** : <timeout-in-seconds>
- **ftdvHealthCheckProtocolName** : <protocol-name>
- **ftdvUnhealthyThreshold** : <threshold-count>

FTDv Autoscaler

- **cpuUtilizationTarget** : <percentage-in-decimals (for example, 0.7)>
- **coolDownPeriodSec**: <cooldown-period-in-seconds>
- **minFTDReplicas** : <min-number-of-FTDv-instances>
- **maxFTDReplicas** : <max-number-of-FTDv-instances>

ELB Services

- **elbPort** : <port-number>
- **elbPortName** : <port-name>
- **elbProtocol** : <protocol-name>
- **elbTimeoutSec** : <timeout-in-seconds>
- **elbProtocolName** : <protocol-name>
- **elbUnhealthyThreshold** : <threshold-number-for-failed-health-checks>
- **elbIpProtocol** : <IP-Protocol>
- **elbPortRange** : <port-range>
- **elbFePorts** : <fast-ethernet-ports>

ILB Services

- **ilbProtocol** : <protocol-name>
- **ilbDrainingTimeoutSec** :<timeout-in-seconds>

- **ilbPort** : <port-number>
- **ilbCheckIntervalSec** : <interval-in seconds>
- **ilbCheckIntervalSec** : <interval-in seconds>
- **ilbProtocolName** : <protocol-name>
- **ilbUnhealthyThreshold** : <threshold-number-for-failed-health-checks>

Remarque
Pour l'évolutivité automatique dedéfense contre les menaces virtuelles, le paramètre **cpuUtilizationTarget: 0.5** est défini et vous pouvez le modifier en fonction de vos besoins. Cette valeur signifie une utilisation du processeur de 50 % de tout le groupe d'instances défense contre les menaces virtuelles.

d) Le fichier `ftdv_template.jinja` prend les paramètres du fichier `ftdv_parameters.yaml` .

Étape 18 Déployez la configuration YAML de pré-déploiement.

```
gcloud deployment-manager deployments create <pre-deployment-name>
--config ftdv_predeployment.yaml
```

Exemple :

```
gcloud deployment-manager deployments create demo-predeployment
--config ftdv_predeployment.yaml

The fingerprint of the deployment is b'9NOy0gsTPgg16SqUEVsBjA=='
Waiting for create [operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c]...done.
Create operation operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c
completed successfully
```

Étape 19 Créez le déploiement d'évolutivité automatique de défense contre les menaces virtuelles.

```
gcloud deployment-manager deployments create <deployment-name>
--config ftdv_parameters.yaml
```

Exemple :

```
gcloud deployment-manager deployments create demo-asav-autoscale
--config ftdv_parameters.yaml
The fingerprint of the deployment is b'1JCQi7Il-laWOY7vOLza0g=='
Waiting for create [operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16]...done.
Create operation operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16
completed successfully.
```

Étape 20 Créez une route pour qu'ILB transfère les paquets de l'application interne à Internet.

```
gcloud beta compute routes create <ilb-route-name>
--network=<inside-vpc-name> --priority=1000 --destination-range=0.0.0.0/0
--next-hop-ilb=<ilb-forwarding-rule-name> --next-hop-ilb-region=<region>
```

Exemple :

```
gcloud beta compute routes create demo-ilb --network=sdt-test-asav-inside
--priority=1000 --destination-range=0.0.0.0/0 --next-hop-ilb=demo-asav-fr-ilb
--next-hop-ilb-region=us-central1
Created [https://www.googleapis.com/compute/beta/projects/asavgcp-poc-4krn/global
/routes/demo-ilb].
```

Logique d'évolutivité automatique

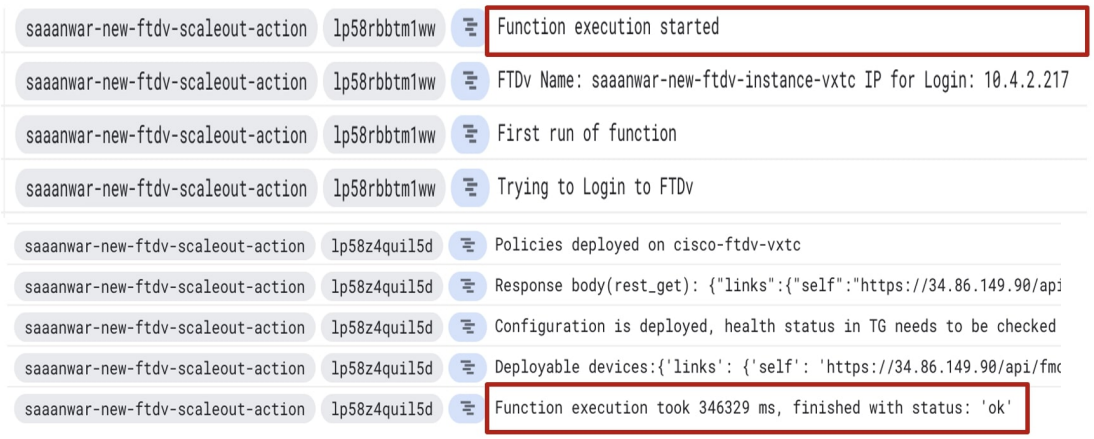
- Le dispositif d'évolutivité automatique traite le niveau d'utilisation de l'unité centrale cible comme une fraction de l'utilisation moyenne de tous les vCPU au fil du temps dans le groupe d'instances.
- Si l'utilisation moyenne de vos vCPU totaux dépasse l'utilisation cible, le dispositif d'évolutivité automatique ajoute d'autres instances de VM. Si l'utilisation moyenne de vos vCPU totaux est inférieure à l'utilisation cible, le dispositif d'évolutivité automatique supprime les instances.
- Par exemple, la définition d'une utilisation cible de 0,75 indique au dispositif d'évolutivité automatique de maintenir une utilisation moyenne de 75 % parmi tous les vCPU du groupe d'instances.
- Seules les mesures d'utilisation du CPU sont utilisées dans les décisions en matière d'évolutivité.
- Cette logique est basée sur l'hypothèse que l'équilibreur de charges tentera de répartir également les connexions sur tous les défense contre les menaces virtuelles et qu'en moyenne, tous les défense contre les menaces virtuelles doivent être chargés de la même manière.

Journalisation et débogage

Les journaux des fonctions en nuage peuvent être consultés comme suit.

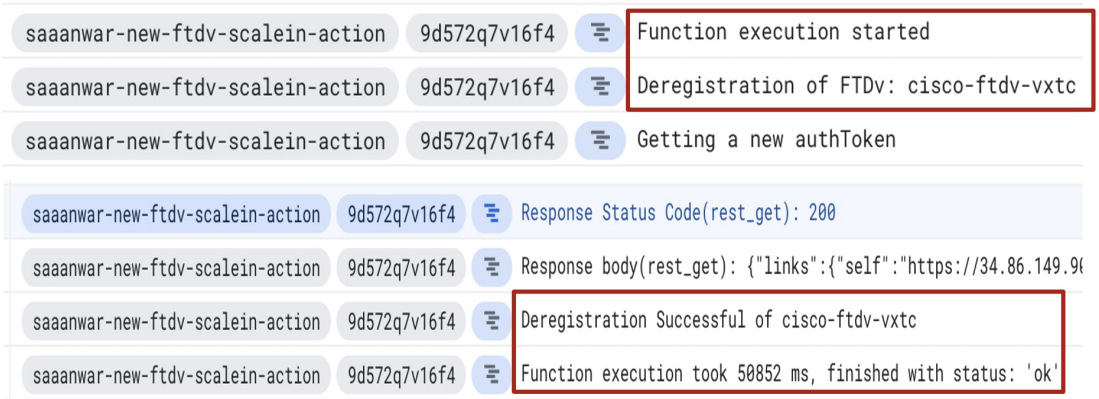
- Journaux de la fonction d'évolutivité à la hausse

Illustration 6 : Journaux de la fonction d'évolutivité à la hausse



Dans les journaux de fonction d'évolutivité donnés ci-dessus, les entrées **Function execution started** et **Function execution took 346329 ms, finish with status: 'ok'** indiquent respectivement le début et la fin des journaux de fonction. Vous pouvez également faire le suivi d'autres opérations telles que la première exécution de la fonction, la connexion défense contre les menaces virtuelles, le déploiement de la politique, etc.

- Journaux de la fonction d'évolutivité à la baisse



Dans les journaux de fonction d'évolutivité donnés ci-dessus, les entrées **Function execution started** et **Function execution took 50852 ms, finish with status: 'ok'** indiquent respectivement le début et la fin des journaux de fonction. Vous pouvez également faire le suivi d'autres opérations telles que le lancement du processus d'annulation de l'enregistrement, l'état de l'annulation de l'enregistrement, l'obtention d'un nouveau jeton d'authentification, etc.

Dépannage

Voici des scénarios d'erreurs courants et des conseils de débogage pour l'évolutivité automatique de Défense contre les menaces virtuelles pour GCP :

- `main.py` introuvable : assurez-vous que le paquet zip est créé uniquement à partir des fichiers. Vous pouvez accéder aux fonctions en nuage et vérifier l'arborescence des fichiers. Il ne devrait y avoir aucun dossier.
- Erreur lors du déploiement du modèle : assurez-vous que toutes les valeurs des paramètres dans « <> » sont renseignées en .jinja et .yaml, ou que le déploiement du même nom existe déjà.
- La fonction Google ne peut pas atteindre défense contre les menaces virtuelles : assurez-vous que le connecteur VPC est créé et que le même nom est mentionné dans le fichier de paramètres YAML.
- Échec de l'authentification pendant la connexion par SSH défense contre les menaces virtuelles : vérifiez que la paire de clés publique et privée est correcte.
- Auth-token introuvable : assurez-vous que le mot de passe centre de gestion virtuel dans Secret est correct.
- défense contre les menaces virtuelles et problèmes de trafic non intègres : assurez-vous qu'il n'y a aucun problème dans les règles et routages de pare-feu.
- Impossible de se connecter manuellement à défense contre les menaces virtuelles : assurez-vous d'utiliser le nouveau mot de passe. L'ancien mot de passe est modifié par la fonction d'évolutivité.
- Impossible d'enregistrer l'appareil sur centre de gestion virtuel : assurez-vous que défense contre les menaces virtuelles est accessible à partir de centre de gestion virtuel . L'interface de gestion de défense contre les menaces virtuelles et centre de gestion virtuel doit se trouver dans le même sous-réseau.

- Les connexions conservées qui forment une boucle entre ILB et défense contre les menaces virtuelles entraînent une utilisation élevée du processeur en raison du lancement de demandes de sonde d'intégrité. Pour réduire l'utilisation élevée du processeur, vous pouvez utiliser l'une des options suivantes :

  Option 1 – Dans centre de gestion virtuel , désactivez l'interface de données, configurez les règles de NAT de sonde d'intégrité et activez l'interface de données. Pour en savoir plus sur les interfaces de données et la NAT, consultez Interface Overview et Network Address Translation.

  Option 2 : Après avoir appliqué les règles de NAT de sonde d'intégrité de centre de gestion virtuel , connectez-vous à la console défense contre les menaces virtuelles et utilisez la commande **clear conn**. Si vous avez configuré la mise en grappes, utilisez la commande **cluster exec clear conn**.

  Vérifiez l'utilisation du processeur à l'aide de la commande **show cpu** sur la console défense contre les menaces virtuelles.

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.