Déployer l'ASA virtuel sur Oracle Cloud Infrastructure

Vous pouvez déployer l'ASA virtuel sur Oracle Cloud Infrastructure (OCI).

Aperçu

OCI est un service informatique en nuage public qui vous permet d'exécuter vos applications dans un environnement hébergé hautement disponible offert par Oracle.

L'ASA virtuel exécute le même logiciel que les ASA virtuel physiques afin d'offrir des fonctionnalités de sécurité éprouvées dans un format virtuel. L'ASA virtuel peut être déployé dans l'OCI 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.

Formats de traitement OCI

Une forme est un modèle qui détermine le nombre de CPU, la quantité de mémoire et d'autres ressources qui sont allouées à une instance. L'ASA virtuel prend en charge les types de forme OCI *standard : à usage général* suivants :

Tableau 1 : Calculer les formes prises en charge pour ASA virtuel

Forme OCI	Version ASAv prise en charge	Attributs		Interfaces
		oCPU	RAM (Go)	
Intel VM.DenseIO2.8	9.19 ou versions ultérieures	8	120	Minimum 4, Maximum 8

Forme OCI	Version ASAv prise en charge	Attributs		Interfaces
		oCPU	RAM (Go)	
Intel VM.StandardB1.4	9.19 ou versions ultérieures	4	48	Minimum 4, Maximum 4
Intel VM.StandardB1.8	9.19 ou versions ultérieures	4	96	Minimum 4, Maximum 8
Intel VM.Standard1.4	9.19 ou versions ultérieures	4	28	Minimum 4, Maximum 4
Intel VM.Standard1.8	9.19 ou versions ultérieures	8	56	Minimum 4, Maximum 8
Intel VM.Standard 2.4	9.15, 9.16, 9.17, 9.18, 9.19, 9.20, 9.21 et 9.22 ou versions ultérieures	4	60	Minimum 4, Maximum 4
IntelVM.Standard2.8	9.15, 9.16, 9.17, 9.18, 9.19, 9.20, 9.21 et 9.22 ou versions ultérieures	8	120	Minimum 4, Maximum 8
Intel VM.Standard3.Flex	9.19 ou versions ultérieures	4	16	Minimum 4, Maximum 4
	9.19 ou versions ultérieures	6	24	Minimum 4, Maximum 4
	9.19 ou versions ultérieures	8	32	Minimum 4, Maximum 8
Intel VM.Optimized3.Flex	9.19 ou versions ultérieures	4	16	Minimum 4, Maximum 8
	9.19 ou versions ultérieures	6	24	Minimum de 4, Maximum 10
	9.19 ou versions ultérieures	8	32	Minimum de 4, Maximum 10
AMD VM.Standard.E4.Flex	9.19 ou versions ultérieures	4	16	Minimum 4, Maximum 4
	9.19 ou versions ultérieures	6	24	Minimum 4, Maximum 4
	9.19 ou versions ultérieures	8	32	Minimum 4, Maximum 8

- L'ASA virtuel nécessite un minimum de 3 interfaces.

- Dans OCI, 1 oCPU équivaut à 2 vCPU.
- Le maximum de vCPU pris en charge est de 16 (8 oCPU).

Recommandations pour l'utilisation des formes de calcul OCI prises en charge par les versions ASA virtuel 9.19 et les versions ultérieures.

- Les images du Marché OCI version **9.19.1-v3** et versions ultérieures sont compatibles uniquement avec les formes de calcul OCI de ASA virtuel 9.19 ou versions ultérieures.
- Vous pouvez utiliser les formes de calcul OCI prises en charge par ASA virtuel 9.19 et versions ultérieures uniquement pour les nouveaux déploiements.
- Les formes de calcul OCI version **9.19.1-v3** et versions ultérieures ne sont pas compatibles avec la mise à niveau des machines virtuelles déployées avec ASA virtuel à l'aide des versions de la forme de calcul OCI vers ASA virtuel 9.19.
- La facturation se poursuivra pour l'abonnement à la forme de calcul **VM.DenseIO2.8**, même après que vous ayez arrêté l'instance. Pour plus d'informations, consultez la documentation OCI.

Vous créez un compte sur OCI, lancez une instance de calcul à l'aide de l'offre de pare-feu virtuel Cisco ASA (ASA virtuel) sur le Marché Oracle Cloud et choisissez une forme OCI.

Prérequis

- Créez un compte sur https://www.oracle.com/cloud/sign-in.html.
- Obtenez une licence pour l'ASA virtuel. Jusqu'à ce que vous obteniez une licence pour l'ASA virtuel, il fonctionnera en mode dégradé, ce qui n'autorisera que 100 connexions et un débit de 100 kbit/s. Consultez Licences : gestion des licences Smart Software.

Remarque Tous les droits de licence par défaut proposés par Cisco, précédemment pour ASA virtuel, prendront en charge la configuration IPv6.

- Exigences d'interface :
  - Interface de gestion
  - Interfaces interne et externe
  - (Facultatif) Sous-réseau supplémentaire (DMZ)
- Chemins de communication :
  - Interface de gestion : utilisée pour connecter l'ASA virtuel à ASDM; ne peut pas être utilisée pour le trafic traversant.
  - Interface interne (requise) : utilisée pour connecter l'ASA virtuel aux hôtes internes.
  - Interface externe (requise) : utilisée pour connecter l'ASA virtuel au réseau public.
  - Interface DMZ (facultative) : utilisée pour connecter l'ASA virtuel au réseau DMZ.

- Pour les exigences du système ASA virtuel, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

Lignes directrices et limites relatives à la licence

Fonctionnalités prises en charge

L'ASA virtuel sur OCI prend en charge les fonctionnalités suivantes :

- Déploiement dans le réseau virtuel en nuage (VCN) OCI
- Maximum de 16 vCPU (8 oCPU) par instance
- Mode avec routeur (par défaut)
- Licences : seul le protocole BYOL est pris en charge
- Prise en charge de la virtualisation des E/S à racine unique (SR-IOV)
- IPv6

Niveaux de performance pour Smart Licensing ASA virtuel

L'ASA virtuel 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.

Niveau de performance	Type d'instance (cœur/RAM)	Limite du débit	Limite de session RA VPN
ASAv5	VM.Standard2.4 4 cœurs/60 Go	100 Mbit/sec	50
ASAv10	VM.Standard2.4 4 cœurs/60 Go	1 Gbit/sec	250
ASAv30	VM.Standard2.4 4 cœurs/60 Go	2 Gbit/s	750
ASAv50	VM.Standard2.8 8 cœurs/120 Go	S.O.	10 000
ASAv100	VM.Standard2.8 8 cœurs/120 Go	S.O.	20 000

Fonctionnalités non prises en charge

L'ASA virtuel sur OCI ne prend pas en charge les éléments suivants :

- Haute disponibilité en natif ASA virtuel
- Modes transparent/en ligne/passif

- Mode multi-contexte

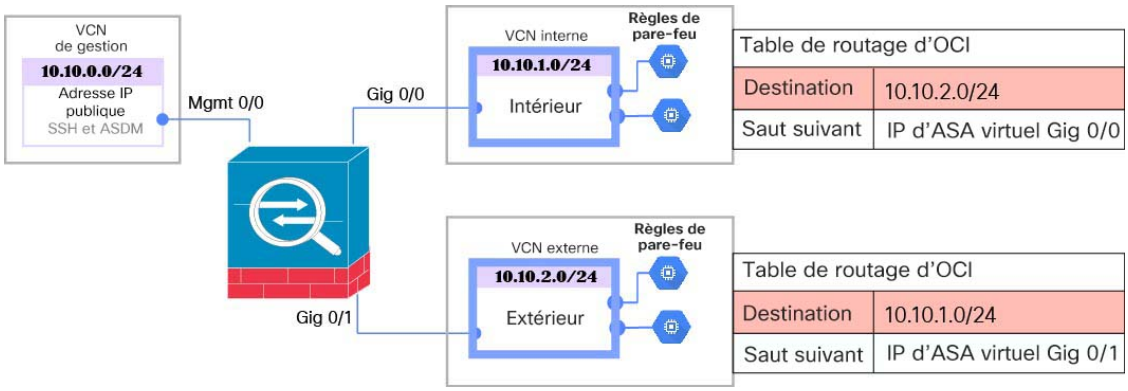
Restrictions

- Le déploiement d'ASA virtuel sur OCI ne prend pas en charge Mellanox 5 tant que vNIC en mode SR-IOV.
- OCI prend en charge uniquement la configuration en mode de pile double (IPv4 et IPv6), et la configuration IPv6 autonome n'est pas prise en charge dans un réseau privé virtuel (VPN).
- Règles de routage distinctes requises pour la configuration d'ASAv statique et DHCP.

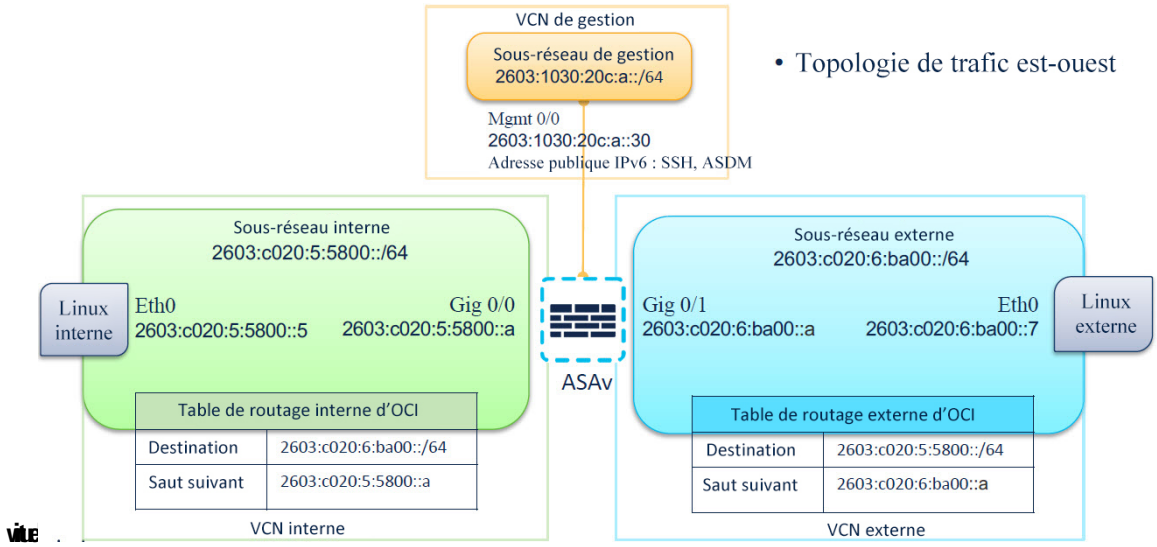
Exemple de topologie de réseau

La figure suivante montre la topologie de réseau recommandée pour l'ASA virtuel en mode pare-feu routé avec trois sous-réseaux configurés dans OCI pour l'ASA virtuel (gestion, interne et externe).

Illustration 1 : Exemple d'ASA virtuel sur le déploiement OCI



Topologie de déploiement IPv6 d'ASA



Déployer l'ASA virtuel

Les procédures suivantes décrivent comment préparer votre environnement OCI et lancer l'instance ASA virtuel. Vous vous connectez au portail OCI, recherchez dans le Marché OCI l'offre de pare-feu virtuel Cisco ASA (ASA virtuel) et lancez l'instance de calcul. Après avoir lancé l'ASA virtuel, vous devez configurer les tables de routage pour diriger le trafic vers le pare-feu en fonction de la source et de la destination du trafic.

Configurer le réseau virtuel en nuage (VCN)

Vous configurez le réseau en nuage virtuel (VCN) pour votre déploiement d'ASA virtuel. Au minimum, vous avez besoin de trois VCN, un pour chaque interface d'ASA virtuel.

Vous pouvez poursuivre les procédures suivantes pour terminer le VCN de gestion. Ensuite, vous revenez à **Networking** (Mise en réseau) pour créer des VCN pour les interfaces interne et externe.

Avant de commencer

Remarque Après avoir sélectionné un service dans le menu de navigation, le menu de gauche comprend la liste des compartiments. Les compartiments vous aident à organiser des ressources pour faciliter le contrôle d'accès. Votre compartiment racine est créé pour vous par Oracle lorsque votre location est provisionnée. Un administrateur peut créer d'autres compartiments dans le compartiment racine, puis ajouter les règles d'accès pour contrôler quels utilisateurs peuvent voir et agir en leur nom. Consultez le document Oracle « Gestion des compartiments » pour en savoir plus.

Procédure

Étape 1 Connectez-vous à OCI et choisissez votre région.

OCI est divisé en plusieurs régions isolées les unes des autres. La région est affichée dans le coin supérieur droit de votre écran. Les ressources d'une région n'apparaissent pas dans une autre région. Vérifiez périodiquement que vous êtes dans la région prévue.

Étape 2 Sélectionnez **Networking (Mise en réseau)** > **Virtual Cloud Networks (Réseaux de nuage virtuel)** et cliquez sur Create Virtual Cloud Networks (Créer des réseaux de nuage virtuel).

Étape 3 Saisissez un **Name** (Nom) descriptif pour votre réseau VCN, par exemple *ASAvManagement*.

Étape 4 Saisissez un **CIDR block** (Bloc CIDR) pour votre VCN.

a) Un **bloc CIDR IPv4** d'adresses IP. La notation CIDR (Classless Inter-Domain Routing) est une représentation compact d'une adresse IP et de son préfixe de routage associé. Par exemple, 10.0.0.0/24.

Remarque
Utiliser les noms de domaine DNS dans ce VCN.

b) Cochez la case **Assign an Oracle allocated IPv6 /56** (Affecter un IPv6 /56 attribué par Oracle) pour ajouter une seule adresse IPv6 attribuée par Oracle à votre VCN.

Étape 5 Cliquez sur **Create VCN** (Créer un VCN).

Créer le groupe de sécurité réseau

Un groupe de sécurité réseau se compose d'un ensemble de vNIC et d'un ensemble de règles de sécurité qui s'appliquent à ces vNIC.

Procédure

Étape 1 Sélectionnez **Networking (Mise en réseau)** > **Virtual Cloud Networks (Réseaux virtuels en nuage)** > **Virtual Cloud Network Details (Détails du réseau virtuel en nuage)** > **Network Security Groups (Groupes de sécurité réseau)** et cliquez sur **Create Network Security Group** (Créer un groupe de sécurité réseau).

Étape 2 Saisissez un **Name** (Nom) de description pour votre groupe de sécurité réseau, par exemple *ASAv-Mgmt-Allow-22-443*.

Étape 3 Cliquez sur **Next** (suivant).

Étape 4 Ajoutez vos règles de sécurité :

a) Ajoutez une règle pour autoriser le port TCP 22 pour l'accès SSH à la console ASA virtuel.

b) Ajoutez une règle pour autoriser le port TCP 443 pour l'accès HTTPS à ASDM.

L'ASA virtuel peut être géré par ASDM, ce qui nécessite l'ouverture du port 443 pour les connexions HTTPS.

Étape 5 Cliquez sur **Create** (créer).

Créer la passerelle Internet

Une passerelle Internet est requise pour rendre votre sous-réseau de gestion accessible au public.

Procédure

Étape 1 Sélectionnez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails de réseau virtuel en nuage)** > **Internet Gateways (passerelles Internet)** et cliquez sur **Create Internet Gateway (créer une passerelle Internet)**.

Étape 2 Saisissez un **nom** descriptif pour votre passerelle Internet, par exemple, *ASAv-IG*.

Étape 3 Cliquez sur **Create Internet Gateway** (créer une passerelle Internet).

Étape 4 Ajouter le routeur à la passerelle Internet :

a) Choisissez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails du réseau virtuel en nuage)** > **Route Tables (tableaux de routage)**.
b) Cliquez sur le lien de votre tableau de routage par défaut pour ajouter des règles de routage.
c) Cliquez sur **Add Route Rules** (ajouter des règles de routage).
d) Dans la liste déroulante **Target Type** (type de cible), sélectionnez **Internet Gateway** (passerelle Internet).
e) Saisissez le bloc CIDR de l'IPv4 de destination, par exemple 0.0.0.0/0.
f) Saisissez le bloc CIDR de l'IPv6 de destination, par exemple [::/0]
g) Dans la liste déroulante **Target Internet Gateway** (passerelle Internet cible), sélectionnez la passerelle que vous avez créée.
h) Cliquez sur **Add Route Rules** (ajouter des règles de routage).

Créer le sous-réseau

Chaque VCN aura au moins un sous-réseau. Vous créerez un sous-réseau de gestion pour le VCN de gestion. Vous aurez également besoin d'un sous-réseau interne pour le VCN interne et d'un sous-réseau externe pour le VCN externe.

Procédure

Étape 1 Sélectionnez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > **Virtual Cloud Network Details (détails du réseau virtuel en nuage)** > **Subnets (sous-réseaux)** et cliquez sur **Create Subnet (créer un sous-réseau)**.

Étape 2 Saisissez un **nom** descriptif pour votre sous-réseau, par exemple, *Gestion*.

Étape 3 Sélectionnez un **type de sous-réseau** (conservez la valeur par défaut recommandée de **Regional** (régional)).

Étape 4 Saisissez un **CIDR Block** (bloc CIDR), par exemple 10.10.0.0/24. L'adresse IP interne (non publique) du sous-réseau est extraite de ce bloc CIDR.

Étape 5 Cochez la case **Assign an Oracle allocated IPv6 /56 prefix** (affecter un préfixe IPv6 /56 alloué par Oracle). Une adresse IPv6 unique est générée, dans laquelle vous devez saisir manuellement les deux derniers chiffres hexadécimaux. Cependant, le préfixe IPv6 dans le sous-réseau est toujours fixé à **/64**.

Étape 6 Sélectionnez l'un des tableaux de routage que vous avez créés précédemment dans la liste déroulante **Route Table** (tableau de routage).

Étape 7 Sélectionnez **Subnet Access** (accès au sous-réseau) pour votre sous-réseau.

Pour le sous-réseau de gestion, il doit s'agir de **Public Subnet** (sous-réseau public).

Étape 8 Sélectionnez **DHCP Option** (option DHCP).

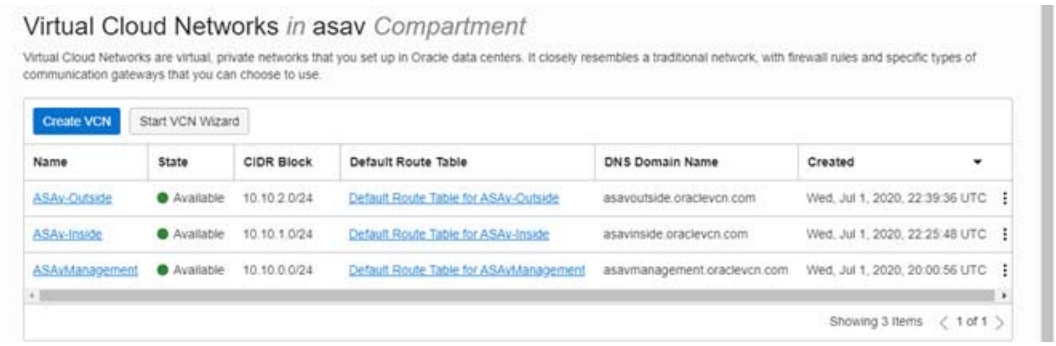
Étape 9 Sélectionnez une **Security List** (liste de sécurité) que vous avez créée précédemment.

Étape 10 Cliquez sur **Create Subnet** (créer un sous-réseau).

Prochaine étape

Après avoir configuré vos VCN (Gestion, Interne, Externe), vous pouvez lancer l'ASA virtuel. Consultez le schéma suivant pour un exemple de configuration VCN d'ASA virtuel.

Illustration 2 : Réseaux en nuage ASA virtuel



Configurer l'adresse de passerelle IPv6 à l'aide de Cloud Shell

Dans OCI, chaque sous-réseau a une adresse de passerelle IPv6 unique que vous devez configurer dans ASAv pour que le trafic IPv6 fonctionne. Cette adresse de passerelle est extraite des détails du sous-réseau en exécutant une commande OCI dans le Cloud Shell.

Procédure

Étape 1 Accédez à **OCI** > **Open CloudShell (OCI Cloud Terminal)** .

Étape 2 Exécutez la commande suivante pour obtenir les détails IPv6 du sous-réseau :

```
oci network subnet get –subnet_id <subnet_OCID>
```

Étape 3 Dans le résultat de la commande, recherchez la clé `ipv6-virtual-router-ip`.

Étape 4 Copiez la valeur de cette clé et utilisez-la selon vos besoins.

Créer l'instance ASA virtuel sur OCI

Vous déployez l'ASA virtuel sur OCI par l'intermédiaire d'une instance de traitement en utilisant l'offre de pare-feu virtuel Cisco ASA (ASA virtuel) sur le Marché Oracle Cloud. Vous sélectionnez la forme de machine

la plus appropriée en fonction de caractéristiques telles que le nombre de CPU, la quantité de mémoire et les ressources du réseau.

Procédure

Étape 1 Connectez-vous au portail OCI.

La région est affichée dans le coin supérieur droit de votre écran. Assurez-vous que vous êtes dans la région prévue.

Étape 2 Choisissez **Marketplace (Marché)** > **Applications**.

Étape 3 Effectuez une recherche sur le Marché pour « Cisco ASA virtual firewall (ASAv) » (Pare-feu virtuel Cisco ASA (ASAv)) et choisissez l'offre.

Étape 4 Passez en revue les conditions générales et cochez la case **I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.** (J'ai lu et j'accepte les conditions d'utilisation d'Oracle et les conditions générales des partenaires).

Étape 5 Cliquez sur **Launch Instance** (Lancer l'instance).

Étape 6 Saisissez un **Name** (Nom) descriptif pour votre instance, par exemple, *ASAv-9-15*.

Étape 7 Cliquez sur **Change Shape** (Modifier la forme) et sélectionnez la forme avec le nombre d'oCPU, la quantité de RAM et le nombre d'interfaces requises pour l'ASA virtuel; par exemple, VM.Standard2.4 (voir Tableau 1 : Calculer les formes prises en charge pour ASA virtuel, à la page 1).

Étape 8 Dans la liste déroulante **Virtual Cloud Network** (Réseau en nuage virtuel), choisissez le VCN de gestion.

Étape 9 Dans la liste déroulante **Subnet** (Sous-réseau), choisissez le sous-réseau de gestion s'il n'est pas rempli automatiquement.

Étape 10 Cochez la case **Use Network Security Groups to Control Traffic** (Utiliser les groupes de sécurité réseau pour contrôler le trafic) et choisissez le groupe de sécurité que vous avez configuré pour le VCN de gestion.

Étape 11 Cliquez sur le bouton radio **Assign a Public Ip Address** (Affecter une adresse IP publique).

Étape 12 Sous **Add SSH Keys** (Ajouter des clés SSH), cliquez sur le bouton radio **Paste Public Keys** (Coller des clés publiques) et collez la clé SSH.

Les instances basées sur Linux utilisent une paire de clés SSH au lieu d'un mot de passe pour authentifier les utilisateurs distants. Une paire de clés est composée d'une clé privée et d'une clé publique. Vous conservez la clé privée sur votre ordinateur et fournissez la clé publique lorsque vous créez une instance. Consultez la section Gestion des paires de clés sur les instances Linux pour obtenir des instructions.

Étape 13 Cliquez sur le lien **Show Advanced Options** (Afficher les options avancées) pour développer les options.

Étape 14 (Facultatif) Sous **Initialization Script** (Script d'initialisation), cliquez sur le bouton radio **Paste Cloud-Init Script** (Coller le script d'initialisation en nuage) pour fournir une configuration day0 (jour0) pour l'ASA virtuel. La configuration day0 (jour0) est appliquée lorsque l'ASA virtuel est lancé.

L'exemple suivant montre une configuration day0 (jour0) que vous pouvez copier et coller dans le champ **Cloud-Init Script** (Script d'initialisation en nuage) :

Consultez les Guides de configuration ASA et la Référence sur les commandes ASA pour en savoir plus sur les commandes ASA.

Important
Lorsque vous copiez du texte à partir de cet exemple, vous devez valider le script dans un éditeur de texte ou un moteur de validation tiers pour éviter les erreurs de format et supprimer les caractères Unicode non valides.

```
!ASA Version 9.18.1
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
ipv6 enable
ipv6 address dhcp default
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh ::/0 management

ssh timeout 60
ssh version 2
username admin nopassword privilege 15
username admin attributes
service-type admin
http server enable
http 0 0 management
aaa authentication ssh console LOCAL
```

Étape 15 Cliquez sur **Create** (créer).

Prochaine étape

Surveillez l'instance ASA virtuel, qui indique l'état Provisioning (Provisionnement) après avoir cliqué sur le bouton **Create** (Créer).

Important Il est important de surveiller l'état. Dès que l'instance ASA virtuel passe de l'état Provisioning (provisionnement) à l'état Running (En cours d'exécution), vous devez associer les VNIC comme nécessaire avant la fin du démarrage de l'ASA virtuel.

Associer les interfaces

L'ASA virtuel passe à l'état en cours d'exécution avec une VNIC associée (consultez **Compute (calculer)** > **Instances** > **Instance Details (détails de l'instance)** > **Attached VNICs (VNIC associées)**). C'est ce que l'on appelle la VNIC principale, et mappe au VCN de gestion. Avant que l'ASA virtuel ne termine le premier démarrage, vous devez associer les VNIC pour les autres sous-réseaux VCN que vous avez créés précédemment (à l'intérieur, à l'extérieur) afin que les VNIC soient correctement détectées sur ASA virtuel.

Procédure

Étape 1 Sélectionnez votre nouvelle instance ASA virtuel.

Étape 2 Choisissez **Attached VNICs (VNIC associées)** > **Create VNIC (créer une VNIC)**.

Étape 3 Saisissez un **nom** descriptif pour votre VNIC, par exemple *Inside* (intérieur).

Étape 4 Sélectionnez le VCN dans la liste déroulante **Virtual Cloud Network** (réseau virtuel en nuage).

Étape 5 Sélectionnez votre sous-réseau dans le menu déroulant **Subnet** (sous-réseau).

Étape 6 Cochez la case **Use Network Security Groups to Control Traffic (utiliser les groupes de sécurité réseau pour contrôler le trafic)** et choisissez le groupe de sécurité que vous avez configuré pour le VCN sélectionné.

Étape 7 Cochez la case **Skip Source Destination Check** (ignorer la vérification de la source de la destination) groupes de sécurité réseau pour contrôler le trafic.

Étape 8 (Facultatif) Précisez une **Private IP Address** (adresse IP privée). C'est obligatoire uniquement si vous souhaitez choisir une adresse IP particulière pour la VNIC.

Si vous ne spécifiez pas d'adresse IP, le protocole OCI attribuera une adresse IP du bloc CIDR que vous avez attribué au sous-réseau.

Si vous configurez une adresse IPv6, sélectionnez et attribuez une adresse IPv6 unique à chaque interface.

Étape 9 Cliquez sur **Save Changes** (enregistrer les modifications) pour créer la carte VNIC.

Étape 10 Répétez cette procédure pour chaque VNIC requise par votre déploiement.

Ajouter des règles de routage pour les VNIC associées

Ajoutez des règles de tableau de routage aux tableaux de routage interne et externe.

Procédure

Étape 1 Choisissez **Networking (réseautage)** > **Virtual Cloud Networks (réseaux virtuels en nuage)** > et cliquez sur le tableau de routage par défaut associé au VCN (interne ou externe).

Étape 2 Cliquez sur **Add Route Rules** (ajouter des règles de routage).

Étape 3 Dans la liste déroulante **Target Type** (type de cible), sélectionnez **Private IP** (adresse IP privée).

Étape 4 Dans la liste déroulante **Destination Type** (type de destination), sélectionnez **CIDR Block** (bloc CIDR).

Étape 5 Saisissez le **bloc CIDR de l'IPv4 de destination**, par exemple, 0.0.0.0/0.

Étape 6 Saisissez le **bloc CIDR de l'IPv6 de destination**, par exemple [::/0]

Étape 7 Saisissez l'adresse IP privée de la VNIC dans le champ **Target Selection** (sélection de cible).

Si vous n'avez pas explicitement attribué d'adresse IP à la VNIC, vous pouvez trouver l'adresse IP attribuée automatiquement à partir des détails de la VNIC (**Compute (calcul)** > **Instances** > **Instance Details (détails de l'instance)** > **Attached VNICs (VNIC associées)**).

Étape 8 Cliquez sur **Add Route Rules** (ajouter des règles de routage).

Étape 9 Répétez cette procédure pour chaque VNIC requise par votre déploiement.

Remarque
Règles de routage distinctes requises pour la configuration d'ASA virtuel (statique et DHCP).

route ipv6<interface_name><interface_subnet_CIDR><ipv6_virtual_router_ip>

Exemple

- route ipv6 à l'intérieur de 2603:c020:5:5800::/64 fé80::200:17ff:fe96:921b
- route ipv6 à l'extérieur de 2603:c020:6:ba00::/64 f80::200:17ff:fe21:748c

Accéder à l'instance ASA virtuel sur OCI

Vous pouvez vous connecter à une instance en cours d'exécution en utilisant une connexion Secure Shell (SSH).

- La plupart des systèmes de type UNIX incluent un client SSH par défaut.
- Les systèmes Windows 10 et Windows Server 2019 doivent inclure le client OpenSSH, dont vous aurez besoin si vous avez créé votre instance à l'aide des clés SSH générées par Oracle Cloud Infrastructure.
- Pour les autres versions de Windows, vous pouvez télécharger PuTTY, le client SSH gratuit depuis http://www.putty.org.

Prérequis

Vous aurez besoin des renseignements suivants pour vous connecter à l'instance :

- L'adresse IP publique de l'instance. Vous pouvez obtenir l'adresse à partir de la page Instance Details (Détails de l'instance) dans la console. Ouvrez le menu de navigation. Sous **Core Infrastructure** (Infrastructure principale), accédez à **Compute** (Informatique) et cliquez sur **Instances**. Ensuite, sélectionnez votre instance. Vous pouvez également utiliser les opérations ListVnicAttachments et GetVnic de l'API de services principaux.
- Le nom d'utilisateur et le mot de passe de votre instance.
- Le chemin complet vers la partie clé privée de la paire de clés SSH que vous avez utilisée lors du lancement de l'instance. Pour en savoir plus sur les paires de clés, consultez Gestion des paires de clés sur les instances Linux.

Remarque Vous pouvez vous connecter à l'instance ASA virtuel en utilisant les renseignements d'authentification spécifiés dans la configuration day0 (jour0) ou en utilisant la paire de clés SSH que vous avez créée lors du lancement de l'instance.

Se connecter à l'instance ASA virtuel à l'aide de SSH

Pour vous connecter à l'instance ASA virtuel 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>
```

Lieu :

<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>
```

Lieu :

<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.

<username> correspond au nom d'utilisateur pour l'instance ASA virtuel.

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

<ipv6-address> est l'adresse IPv6 de votre interface de gestion d'instance.

Se connecter à l'instance ASA virtuel à l'aide d'OpenSSH

Pour vous connecter à l'instance ASA virtuel à partir d'un système Windows, connectez-vous à l'instance à l'aide d'OpenSSH.

Procédure

Étape 1 Si c'est la première fois que vous utilisez cette paire de clés, vous devez définir les autorisations de fichier de sorte que vous puissiez être le seul à lire le fichier.

Procédez comme suit :

a) Dans Windows Explorer, accédez au fichier de clé privée, cliquez avec le bouton droit sur le fichier, puis cliquez sur **Properties** (Propriétés).
b) Dans l'onglet **Security** (Sécurité), cliquez sur **Advanced** (Avancé).
c) Assurez-vous que le **Owner** (Propriétaire) est votre compte d'utilisateur.
d) Cliquez sur **Disable Inheritance** (Désactiver l'hérédité), puis sélectionnez **Convert inherited permissions into explicit permissions on this object** (Convertir les autorisations héritées en autorisations explicites sur cet objet).
e) Sélectionnez chaque entrée d'autorisation qui ne correspond pas à votre compte d'utilisateur et cliquez sur **Remove** (Supprimer).
f) Assurez-vous que l'autorisation d'accès pour votre compte d'utilisateur est **Full control** (Contrôle complet).
g) Enregistrez vos modifications.

Étape 2 Pour vous connecter à l'instance, ouvrez Windows PowerShell et exécutez la commande suivante :

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

Lieu :

<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.

<username> correspond au nom d'utilisateur pour l'instance ASA virtuel.

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

Se connecter à l'instance ASA virtuel à l'aide de PuTTY

Pour vous connecter à l'instance ASA virtuel à partir d'un système Windows à l'aide de PuTTY :

Procédure

Étape 1 Ouvrez PuTTY.

Étape 2 Dans le volet **Category (catégorie)**, sélectionnez **Session (session)** et saisissez la commande suivante :

- **Host Name (or IP address) (nom d'hôte ou adresse IP non valide)** :

  <username>@<public-ip-address>

  Lieu :

  <username> correspond au nom d'utilisateur pour l'instance ASA virtuel.

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

- **Port:** 22
- **Connection type:** SSH

Étape 3 Dans le volet **Category** (catégorie), développez **Window**, puis sélectionnez **Translation** (traduction).

Étape 4 Dans la liste déroulante **Remote character set** (jeu de caractères du système distant), sélectionnez **UTF-8**.

Sur les instances basées sur Linux, les paramètres régionaux par défaut sont définis pour UTF-8. PuTTY est configuré pour utiliser les mêmes paramètres régionaux.

Étape 5 Dans le volet **Category** (catégorie), développez la section **Connection** (connexion), puis la section **SSH**. Cliquez ensuite sur **Auth** (authentification).

Étape 6 Cliquez sur **Browse** (parcourir), puis sélectionnez votre clé privée (private key).

Étape 7 Cliquez sur **Open** (ouvrir) pour lancer la session.

S'il s'agit de votre première connexion à l'instance, un message indiquant que la clé d'hôte du serveur n'est pas mise en cache dans le registre pourrait s'afficher. Cliquez sur **Yes** (oui) pour poursuivre.

Dépannage

Problème SSH : ASA virtuel avec IPv6 ne fonctionne pas

- **Solution** Vérifiez si la route pour ::/0 via la passerelle Internet est présente dans la table de routage VPC.
- **Solution** Vérifiez si le port 22 est autorisé dans le groupe de sécurité associé au sous-réseau ou à l'interface de gestion.
- **Solution** Vérifiez par la session SSH IPv4 si l'interface de gestion est configurée avec une adresse IPv6.
- **Solution** Vérifiez la « ssh config » (configuration ssh) dans ASA virtuel et que toutes les configurations requises sont fournies dans le cadre de day0 (jour0) ou configurées ultérieurement.

Problème Le trafic Est-Ouest ne fonctionne pas.

- **Solution** Vérifiez dans **EC2** > **Instance** > **Networking (Mise en réseau)** si la « Change source/destination check » (Modification de la source/destination) est arrêtée.
- **Solution** Vérifiez que les routes sont correctement configurées sur Linux interne/externe.
- **Solution** Ajoutez les routes appropriées dans ASA virtuel en cas d'adressage IPv6 manuel.
- **Solution** Cocher la case « show aspdrop » (afficher l'abandon asp) pour tous les abandons de paquets et agir en conséquence.

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.