仮想セキュア ゲートウェイ アプリケーション コンテナの設定

この章は、次の項で構成されています。

仮想セキュア ゲートウェイ アプリケーション コンテナ

Cisco Virtual Secure Gateway（VSG）コンテナ タイプは、強化されたセキュリティを仮想環境で提供するために使用します。Cisco UCS Director を使用して、Prime Network Services Controller（PNSC）とともに、その内部ファイアウォール（Cisco Virtual Security Gateway）を設定できます。このファイアウォールは、設定後、アプリケーション コンテナに統合されます。

Cisco VSG は仮想ファイアウォール アプライアンスで、仮想データセンターおよびクラウド環境への信頼できるアクセスを提供します。Cisco VSG では、さまざまなセキュリティ プロファイルを持つ複数のテナント ワークロードの広範な組み合わせによって、仮想データセンターのプライベート クラウドまたはパブリック クラウドにおける共通のコンピューティング インフラストラクチャの共有を可能にします。1 つ以上の仮想マシン（VM）を固有の信頼ゾーンに割り当てることで、Cisco VSG は確立されたセキュリティ ポリシーを通じて信頼ゾーンへのアクセスを制御し、モニタするようにします。

Cisco VSG には次の利点があります。

- 信頼できるマルチテナント アクセス：マルチテナント（スケールアウト）環境で適用されたコンテキスト認識型セキュリティ ポリシーに基づいた、きめ細かいゾーンベースの管理およびモニタリングにより、法規制の遵守を強化し、監査を簡略化します。セキュリティ ポリシーはセキュリティ プロファイル テンプレートとして構成され、数多くの Cisco VSG にわたる管理と展開を簡略にします。

- 動的操作：セキュリティ テンプレートと信頼ゾーンの VM インストール時のオンデマンド プロビジョニング、トランスペアレントモビリティの強化、およびVMのライブ マイグレーションとしてのモニタリングがさまざまな物理サーバで実行されます。
- 中断のない管理：セキュリティ チームとサーバ チームの分別管理により、コラボレーションを強化しながら、管理上のエラーを排除し、監査を簡略にします。

Cisco VSG は次を実行します。

- 業界規制への準拠の強化
- 仮想化環境の監査プロセスを簡略化します。
- 仮想データセンターか、プライベート/パブリック クラウド コンピューティング環境かにかかわらず、幅広い仮想化されたワークロード セットを共有コンピューティング インフラストラクチャ上の複数のテナントに安全に展開して、コストを削減します。

仮想セキュリティ ゲートウェイ アプリケーション コンテナの前提条件

以下に示すのは、VSG コンテナ設定の前提条件です。

- コンテナVMリソースの割り当てタスクを実行する場合、デフォルトの仮想ネットワーク タイプは、VSG コンテナの分散仮想ポートグループ N1K です。VSG コンテナのプライマリ DVSwitch 名は必ず変更します。

仮想セキュリティ ゲートウェイ アプリケーション コンテナの制限

VSG アプリケーション コンテナの作成プロセス

PNSC アカウントの追加

PNSCは、Cisco仮想サービスのデバイスおよびセキュリティ ポリシーを一元管理できる仮想アプライアンスで、Red Hat Enterprise Linux に基づいています。マルチテナント操作用に設計された PNSC は、シームレスで、拡張可能な自動化中心の管理を仮想データセンター環境およびクラウド環境で実現します。PNSC は基本的にセキュリティ コンポーネント（ファイアウォール）を VSG およびアプリケーション コンテナに提供し、VM を互いに分離します。PNSC は、管理者がシスコ仮想サービスの一元管理を Cisco UCS Director を通じて実行できるようにします。

（注） PNSC は特定のポッドに関連付けられていません。

ステップ 1 [管理（Administration）] > [物理アカウント（Physical Accounts）] を選択します。

ステップ 2 [物理アカウント（Physical Accounts）] ページで [マルチドメイン マネージャ（Multi-Domain Managers）] をクリックします。

ステップ 3 [追加（Add）]（+）をクリックします。

ステップ 4 [アカウントの追加（Add Account）] 画面で、次のフィールドに入力します。

名前	説明
[アカウントタイプ（Account Type）] フィールド	アカウント タイプとして PNSC を選択し、[送信（Submit）] をクリックします。
[アカウント名（Account Name）] フィールド	マルチドメイン アカウント名。
[説明（Description）] フィールド	マルチドメイン アカウントの説明。
[サーバ管理（Server Management）] ドロップダウン リスト	ドロップダウン リストから、[すべてのサーバ（All Servers）] または [選択したサーバ（Selected Servers）] を選択し、それに応じてサーバを管理します。
[サーバアドレス（Server Address）] フィールド	PNSC サーバの IP アドレス。
[クレデンシャル ポリシーの使用（Use Credential Policy）] チェック ボックス	手動で情報を入力する代わりに、このアカウントのクレデンシャル ポリシーを使用する場合は、このチェック ボックスをオンにします。
[クレデンシャルポリシー（Credential Policy）] ドロップダウン リスト	[クレデンシャルポリシーの使用（Use Credential Policy）] チェック ボックスをオンにした場合は、このドロップダウン リストから使用するクレデンシャル ポリシーを選択します。 このフィールドが表示されるのは、クレデンシャル ポリシーの使用を選択した場合のみです。
[ユーザ ID（User ID）] フィールド	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフになっている場合にのみ表示されます。アカウントにアクセスするユーザ ID。

名前	説明
[パスワード（Password）] フィールド	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフになっている場合にのみ表示されます。ユーザ名に関連付けられたパスワードです。
[共有秘密パスワード（Shared Secret Password）] フィールド	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフになっている場合にのみ表示されます。アカウントの事前共有秘密キー。
[通信タイプ（Transport Type）] ドロップダウン リスト	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェック ボックスがオフになっている場合にのみ表示されます。次の転送タイプを選択します。 • HTTP：標準プロトコル。 • HTTPS：標準セキュア プロトコル。
[ポート（Port）] フィールド	このフィールドは、[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフになっている場合にのみ表示されます。ポート番号（転送タイプに基づく）。
[連絡先の電子メール（Contact Email）] フィールド	このアカウントを使用する管理者または個人の電子メール アドレス。
[ロケーション（Location）] フィールド	アカウントと関連付けられたデバイスの場所。

ステップ 5 [送信（Submit）] をクリックします。

PNSC レポートの表示

PNSC アカウントを作成後に、Cisco UCS Director を使用して関連レポートを表示できます。

[物理（Physical）] > [ネットワーク（Network）] メニューから、次のレポートを使用できます。

- 要約
- Tenants
- vDC

- [vApps]
- [PNSC ファイアウォール ポリシー（PNSC Firewall Policy）]
- [VM マネージャ（VM Manager）]
- Clients
- [HA ID 使用状況レポート（HA ID Usage Report）]

ステップ 1 [物理（Physical）] > [ネットワーク（Network）] を選択します。

ステップ 2 [マルチ ドメイン マネージャ（Multi-domain Manager）] を展開します。
マルチドメイン マネージャのアカウントに追加された PNSC アカウントを表示できます。

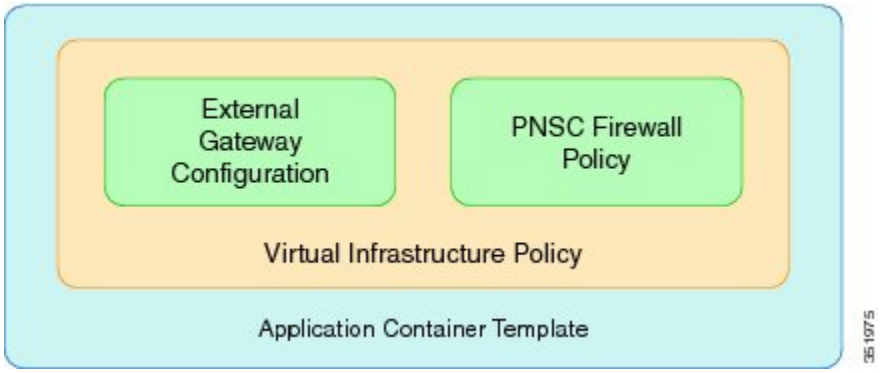
ステップ 3 PNSC のエントリをクリックし、使用可能なレポートを表示します。

アプリケーション コンテナへの VSG の統合

内部ファイアウォール（Cisco Virtual Security Gateway）に加えて PNSC を設定する Cisco UCS Director を使用し、アプリケーション コンテナに統合することができます。

統合プロセスには、いくつかの段階があります。

- Cisco UCS Director に OVA ファイルをアップロードします。
- PNSC ファイアウォール ポリシー（PNSC を使用したコンテナの作成に使用）を作成します。
- 仮想インフラストラクチャ ポリシーを作成します。使用する仮想アカウントと、プロビジョニングを行うコンテナのタイプをこのポリシーで定義します。
- アプリケーション コンテナ テンプレートを作成します。このテンプレートは、仮想インフラストラクチャ ポリシー、コンピューティング ポリシー、ストレージ ポリシー、およびネットワーク ポリシーをテンプレートへの入力として使用します。



OVA ファイルのアップロード

Cisco UCS Director では、管理者、グループ管理者、またはエンドユーザが事前に定義されたストレージの場所に OVA ファイルをアップロードできます。

（注） OVA ファイルをアップロードする権限のある唯一のタイプが、グループ管理者とエンドユーザです。

はじめる前に

適切なアクセス権があることを確認します。

ステップ 1 [管理（Administration）] > [統合（Integration）] を選択します。

ステップ 2 [統合（Integration）] ページで [ユーザ OVF 管理（User OVF Management）] をクリックします。

ステップ 3 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 4 [ファイルのアップロード（Upload File）] 画面で、次のフィールドに値を入力します。

名前	説明
[フォルダタイプ] ドロップダウン リスト	OVF ファイルを含んでいるフォルダのタイプ。次のいずれかを実行します。 • [パブリック（Public）] : パブリック ファイルのみを表示するには、このロールを選択します。 • [ユーザ（User）] : エンドユーザである場合は、このロールを選択します。エンド ユーザには広範囲の権限は付与されません。ユーザ ロールは第 1 レベルのサポートに適していますが、その主要な目的は問題の識別、修復、およびエスカレートにあります。 • [グループ（Group）] : このロールでは OVA ファイルを展開できます。
[ファイル名（File Name）] フィールド	アップロードし、表示する OVF ファイルの名前。
[ファイル（File）] フィールド	OVA ファイルをドロップするか、または [ファイルの選択（Select a File）] をクリックして、必要なファイルを参照して選択します。
[ファイルの説明（File Description）] フィールド	ファイルの説明（必要な場合）。

ステップ 5 [送信（Submit）] をクリックします。

PNSC ファイアウォール ポリシーの作成

ファイアウォール ポリシーを使用して Cisco VSG にネットワーク トラフィックを適用します。Cisco VSG は、PNSC の一環として使用される内部ファイアウォールです。Cisco VSG の主要コンポーネントはポリシー エンジンです。ポリシー エンジンは、Cisco VSG で受信するネットワーク トラフィックをフィルタする設定としてポリシーを使用します。

（注） PNSC ファイアウォール ポリシーはスタンドアロン モードと高可用性（HA）モードの両方をサポートします。

ステップ 1 [物理（Physical）] > [ネットワーク（Network）] を選択します。

ステップ 2 [マルチドメイン マネージャ（Multi-Domain Managers）] の下にリストされている [PNSC アカウント（PNSC accounts）] を展開します。

ステップ 3 ファイアウォール ポリシーを作成する PNSC アカウントをクリックします。

ステップ 4 [PNSC ファイアウォール ポリシー（PNSC Firewall Policy）] をクリックします。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [ファイアウォール ポリシーの作成（Create Firewall Policy）] 画面で、次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	ファイアウォール ポリシーの一意の名前。
[ポリシーの説明（Policy Description）] フィールド	ファイアウォール ポリシーの説明。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 PNSC ゾーンを展開し、[追加（+）（Add (+)）] をクリックしてゾーンを作成します。

ステップ 9 [PNSC ゾーンへのエントリの追加（Add Entry to PNSC Zones）] 画面で、次のフィールドに入力します。

名前	説明
[ゾーン名（Zone Name）] フィールド	ゾーンの一意の名前。
[ゾーンの説明（Zone Description）] フィールド	ゾーンの説明。
[ゾーン条件（Zone Conditions）]	[ゾーン条件（Zone Conditions）] を展開し、[追加（Add）] をクリックしてゾーン条件を追加します。

名前	説明
[属性タイプ（Attribute Type）] ドロップダウン リスト	属性のタイプとして [ネットワーク（Network）] または [VM] を選択します。
[属性名（Attribute Name）] ドロップダウン リスト	属性タイプに応じて異なるリストから属性を選択します。
[演算子（Operator）] ドロップダウン リスト	演算子のタイプを選択します。
[属性値（Attribute Value）] フィールド	選択した属性タイプに基づいて属性値を入力します。

ステップ 10 [送信（Submit）] をクリックします。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [PNSC ACL ルール（PNSC ACL Rules）] を展開し、[追加（+）（Add (+)）] をクリックして PNSC ACL ルール エントリを作成します。

ステップ 13 [PNSC ACL ルールへのエントリの追加（Add Entry to PNSC ACL Rules）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ACL ルールの名前。名前はコンテナに固有である必要があります。
[説明（Description）] フィールド	ACL ルールの説明。
[アクション（Action）] ドロップダウン リスト	ルールに許可されたアクションのタイプ。次のいずれかを実行します。 • [許可（Permit）] : 一致するトラフィックでの使用を許可します。 • [却下（Drop）] : 一致するトラフィックでの使用を却下します。 • [リセット（Reset）] : 一致するトラフィックでのルールをリセットします。
[条件一致基準（Condition Match Criteria）] ドロップダウン リスト	満たす必要がある条件を選択します。
[プロトコル/サービス（Protocol/Service）] ドロップダウン リスト	リストからプロトコルまたはサービスを選択します。

名前	説明
[任意のプロトコル（Any Protocol）] チェック ボックス	オンにした場合は、すべてのプロトコルにルールが適用されます。オフにした場合は、演算子（「equals」、「notequals」）およびプロトコル（たとえば、IP や EGP）を指定する必要があります。
[送信元の条件（Source Conditions）]	
[属性タイプ（Attribute Type）] ドロップダウン リスト	属性のタイプを選択します。
[属性名（Attribute Name）] ドロップダウン リスト	属性タイプに応じて異なるドロップ ダウン リストから、属性名を選択します。
[演算子（Operator）] ドロップダウン リスト	演算子のタイプを選択します。
[属性値（Attribute Value）] フィールド	属性値。
[送信先の条件（Destination Conditions）]	
[属性タイプ（Attribute Type）] ドロップダウン リスト	属性のタイプを選択します。
[属性名（Attribute Name）] ドロップダウン リスト	属性タイプに応じて異なるドロップ ダウン リストから、属性名を選択します。
[演算子（Operator）] ドロップダウン リスト	演算子のタイプを選択します。
[属性値（Attribute Value）] フィールド	属性値。

ステップ 14 [送信（Submit）] をクリックします。

ステップ 15 [次へ（Next）] をクリックします。

ステップ 16 [PNSC-VSG 設定（PNSC-VSG Configuration）] 画面で、次のフィールドに入力します。

名前	説明
[ユニファイド ファブリックの使用（Use Unified Fabric）] チェック ボックス	ユニファイドファブリックを使用するには、チェック ボックスをオンにします。
[VSG OVF URL] ドロップダウン リスト	Cisco UCS Director にアップロードされている OVA ファイルのリストから OVA ファイルを選択します。

名前	説明
[VSG の管理者パスワード（Admin Password for the VSG）] フィールド	VSG の管理者パスワード。
[ポリシー エージェントの共有シークレット パスワード（Policy agent shared secret Password）] フィールド	ポリシー エージェントの共有パスワード。
[展開モード（Deployment mode）] ドロップダウン リスト	展開のタイプ。次のいずれかを実行します。 • [スタンドアロン（Standalone）]：スタンドアロン モード。 • [HA]：高可用性モード。
[VSG HA Id] フィールド	VSG HA の ID。使用可能な範囲は 1 ～ 4095 です。
[ネットワークタイプ（Network Type）] ドロップダウンリスト	リストからネットワーク タイプを選択します。
[VLAN ID 範囲（VLAN ID Range）] フィールド	VLAN ID の範囲（たとえば、100 ～ 199）。
[同じ VLAN/VXLAN の使用（Use same vlan/vxlan）] チェック ボックス	オンにした場合は、VSG HA とデータ ポート グループの両方に同じ VLAN ID または VXLAN ID を使用します。
[名前（Name）] フィールド	VSG の名前。
*[プライマリ VSG（Primary VSG）]*セクション（*HA* モードのみ）	
[名前（Name）] フィールド	プライマリ VSG の名前。
[展開設定（Deployment Configuration）] ドロップダウン リスト	展開設定。次のいずれかを実行します。 • [小 VSG の展開（Deploy Small VSG）] • [中 VSG の展開（Deploy Medium VSG）] • [大 VSG の展開（Deploy Large VSG）]

名前	説明
[ディスク形式（Disk Format）] ドロップダウンリスト	仮想ディスクを保存する形式。次のいずれかを実行します。 • [シック プロビジョニング（Lazy Zeroed）（Thick Provision Lazy Zeroed）] • [シック プロビジョニング（Easy Zeroed）（Thick Provision Easy Zeroed）] • [シン プロビジョニング（Thin Provision）]
[セカンダリ VSG（Secondary VSG）]（*HA* モードのみ）	
[名前（Name）] フィールド	プライマリ VSG の名前。
[展開設定（Deployment Configuration）] ドロップダウン リスト	展開設定。次のいずれかを実行します。 • [小 VSG の展開（Deploy Small VSG）] • [中 VSG の展開（Deploy Medium VSG）] • [大 VSG の展開（Deploy Large VSG）]
[ディスク形式（Disk Format）] ドロップダウンリスト	仮想ディスクを保存する形式。次のいずれかを実行します。 • [シック プロビジョニング（Lazy Zeroed）（Thick Provision Lazy Zeroed）] • [シック プロビジョニング（Easy Zeroed）（Thick Provision Easy Zeroed）] • [シン プロビジョニング（Thin Provision）]

ステップ 17 [送信（Submit）] をクリックします。

ステップ 18 [OK] をクリックします。

仮想インフラストラクチャ ポリシーの作成

仮想インフラストラクチャ ポリシーは、使用する VM やプロビジョニングするコンテナのタイプを定義します。また、このポリシーは、この特定のアカウントに関連付ける PNSC アカウントも定義します。

（注） ゲートウェイ関連の Linux ベースの VM イメージパラメータをこのポリシーに追加できます。

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [仮想インフラストラクチャ ポリシー（Virtual Infrastructure Policies）] をクリックします。

ステップ 3 [ポリシーを追加（+）（Add Policy (+)）] をクリックします。

ステップ 4 [仮想インフラストラクチャ ポリシーの作成（Create a virtual infrastructure policy）] 画面で、次のフィールドに入力します。

名前	説明
[ポリシー名（Policy Name）] フィールド	仮想インフラストラクチャ ポリシーの一意の名前。
[ポリシーの説明（Policy Description）] フィールド	仮想インフラストラクチャ ポリシーの説明。
[コンテナ タイプ（Container Type）] ドロップダウン リスト	VSG コンテナ タイプを選択します。
[仮想アカウントの選択（Select Virtual Account）] ドロップダウン リスト	仮想アカウント（クラウド）を選択します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [仮想インフラストラクチャ ポリシー：PNSC 情報（Virtual Infrastructure Policy - PNSC Information）] 画面で、次のフィールドに入力します。

名前	説明
[PNSC アカウント（PNSC Account）] フィールド	PNSC アカウントを展開し、PNSC アカウントを選択します。
[VSG テンプレート設定（VSG Template Configuration）] セクション	
[PNSC ファイアウォール ポリシー（PNSC Firewall Policy）] ドロップダウン リスト	ファイアウォール ポリシーを選択します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [仮想インフラストラクチャ ポリシー：フェンシング ゲートウェイ（Virtual Infrastructure Policy - Fencing Gateway）] 画面で、次のフィールドに入力します。

名前	説明
[ゲートウェイが必要（Gateway Required）] チェック ボックス	ゲートウェイが必要な場合は、このボックスをオンにします。
[ゲートウェイ ポリシーの選択（Select Gateway Policy）] ドロップダウン リスト	このフィールドは、[ゲートウェイが必要（Gateway Required）] チェック ボックスがオンになっている場合にのみ表示されます。ゲートウェイ ポリシーを選択します。
ゲートウェイの要約	仮想インフラストラクチャ ポリシーのゲートウェイ設定の概要が表示されます。

ステップ 9 [次へ（Next）] をクリックします。[仮想インフラストラクチャ ポリシー：概要（Virtual Infrastructure Policy - Summary）] 画面が表示され、現在の設定が示されます。

ステップ 10 [送信（Submit）] をクリックします。

VSG 用アプリケーション テンプレートの作成

ステップ 1 [ポリシー（Policies）] > [アプリケーション コンテナ（Application Containers）] を選択します。

ステップ 2 [アプリケーション コンテナ（Application Containers）] ページで [アプリケーション コンテナのテンプレート（Application Container Templates）] をクリックします。

ステップ 3 [テンプレートの追加（Add Template）] をクリックします。[アプリケーション コンテナ テンプレートの追加（Add Application Container Template）] ページが表示されます。次のフィールドに入力します。

名前	説明
[テンプレート名（Template Name）] フィールド	新しいテンプレートの名前。
[テンプレートの説明（Template Description）] フィールド	テンプレートの説明。

ステップ 4 [次へ（Next）] をクリックします。[アプリケーション コンテナ テンプレート：仮想インフラストラクチャ ポリシーの選択（Application Container Template - Select a Virtual Infrastructure policy）] 画面が表示されます。この画面で、アプリケーション コンテナを展開するクラウドを選択します。次のフィールドに入力します。

名前	説明
[仮想インフラストラクチャ ポリシーの選択（Select Virtual Infrastructure Policy）] ドロップダウン リスト	コンテナに展開する仮想インフラストラクチャ ポリシーを選択します。

ステップ 5 [次へ（Next）] をクリックします。[アプリケーション コンテナ：テンプレート：内部ネットワーク（Application Container Template - Internal Networks）] 画面が表示されます。

（注） VSG コンテナごとに 1 つのネットワークのみを設定できます。

ステップ 6 [追加（+）（Add (+)）] アイコンをクリックしてネットワークを追加します。[ネットワークへのエントリの追加（Add Entry to Networks）] 画面が表示されます。次のフィールドに入力します。

名前	説明
[ネットワーク名（Network Name）] フィールド	ネットワーク名。この名前はコンテナで一意である必要があります。最大 128 文字を使用できます。
[ネットワークタイプ（Network Type）] ドロップダウンリスト	ネットワーク タイプを選択します。
[情報ソース（Information Source）] ドロップダウン リスト	リストから情報ソースのタイプを選択します。
[VLAN ID 範囲（VLAN ID Range）] フィールド	VLAN ID の範囲。この値は、複製または作成できるコンテナの数を制御します。
[ネットワーク IP アドレス（Network IP Address）] フィールド	コンテナのネットワーク IP アドレス。
[ネットワークマスク（Network Mask）] フィールド	ネットワーク マスク。
[ゲートウェイ IP アドレス（Gateway IP Address）] フィールド	ネットワークのデフォルト ゲートウェイの IP アドレス。この IP アドレスの NIC が GW VM に作成されます。 （注） ゲートウェイの内部インターフェイスにこの IP アドレスが設定されます。

ステップ 7 [送信（Submit）] をクリックします。

この後、アプリケーション コンテナでプロビジョニングされるゲートウェイ VM を追加および設定できます。

ステップ 8 [OK] をクリックします。

ステップ 9 [次へ（Next）] をクリックします。
[アプリケーション コンテナ テンプレート：VM（Application Container Template - VMs）] 画面が表示されます。

ステップ 10 [追加（+）（Add (+)）] をクリックして VM を追加します。次のフィールドに入力します。

名前	説明
[VM] フィールド	VM の名前。フルネームには、コンテナ名とこの名前が含まれます。
[説明（Description）] フィールド	VM の説明。
[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックス	コンテンツ ライブラリ VM テンプレートから VM テンプレートを表示して選択するには、オンにします。オフにした場合には、VM イメージ テンプレートから VM テンプレートを選択する必要があります。
[コンテンツ ライブラリ VM テンプレート（Content Library VM Template）] フィールド	このフィールドは、[コンテキスト ライブラリ VM テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library VM Template）] チェック ボックスがオンの場合にのみ表示されます。リストを展開して、コンテンツ ライブラリから VM テンプレートを選択します。
[VM イメージ（VM Image）] ドロップダウン リスト	このフィールドは、[コンテンツ ライブラリ テンプレートを使用した VM のプロビジョニング（Provision VM using Content Library Template）] チェック ボックスがオフになっている場合にのみ表示されます。展開するイメージを選択します。
[仮想 CPU の数（Number of Virtual CPUs）] ドロップダウン リスト	VM に割り当てる仮想 CPU の数を選択します。
[メモリ（Memory）] ドロップダウン リスト	VM に割り当てるメモリの量（MB 単位）を選択します。
[CPU予約(MHz)] フィールド	VM に対する CPU 確保（Mhz 単位）。
[メモリ予約(MB)（Memory Reservation (MB)）] フィールド	VM のメモリ予約。

名前	説明
[ディスク サイズ（GB）（Disk Size (GB)）] フィールド	VM のカスタム ディスク サイズ。テンプレートのディスク サイズを使用するには、値にゼロを指定します。指定したディスク サイズで選択したイメージのディスク サイズが上書きされます。 （注） この値がテンプレート サイズ未満の場合、この値は無視されます。
[VMパスワード共有オプション（VM Password Sharing Option）] ドロップダウン リスト	VMのユーザ名とパスワードをエンドユーザと共有する方法のオプションを選択します。[パスワードのリセット後に共有（Share after password reset）] または [共有テンプレート クレデンシャル（Share template credentials）] を選択した場合、エンドユーザは選択したテンプレートのユーザ名とパスワードを指定する必要があります。
[イメージからのネットワーク設定の使用（Use Network Configuration from Image）] チェックボックス	オンにした場合は、イメージからのネットワーク設定がプロビジョニング済みの VM に適用されます。
[VM ネットワーク インターフェイス（VM Network Interfaces）] フィールド	VM ネットワーク インターフェイスを展開し、VM ネットワーク インターフェイス情報を選択します。別のネットワーク インターフェイスを追加する場合は、ステップ 11 に進みます。
[最大数量（Maximum Quantity）] フィールド	作成後にこのコンテナで追加可能なインスタンスの最大数。
[初期数量（Initial Quantity）] フィールド	コンテナを作成する際にプロビジョニングする VM インスタンスの数。 （注） 各 VM には一意の名前と IP アドレスが設定されます。

ステップ 11 （任意） [追加（+）（Add (+)）] をクリックして、新しい（複数の）VM ネットワーク インターフェイスを追加します。次のフィールドに入力します。

名前	説明
[VM ネットワーク インターフェイス名（VM Network Interface Name）] フィールド	VM ネットワーク インターフェイスの名前。
[ネットワークの選択（Select the Network）] ドロップダウン リスト	ネットワークを選択します。

名前	説明
[Ipアドレス（IP Address）] フィールド	ネットワークの IP アドレス。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 13 [OK] をクリックします。
[アプリケーション コンテナ テンプレート：外部ゲートウェイ セキュリティ設定（Application Container Template - External Gateway Security Configuration）] 画面が表示されます。ポート マッピングや発信アクセス制御リスト（ACL）などのセキュリティ設定コンポーネントを指定できます。

ステップ 14 [追加（+）（Add (+)）] をクリックし、ポート マッピングを追加します。次のフィールドに入力します。

名前	説明
[プロトコル（Protocol）] ドロップダウン リスト	ポート マッピング用のプロトコルを選択します。
[マッピングされたポート（Mapped Port）] ドロップダウン リスト	選択したプロトコルにマッピングされたポートを選択します。
[リモート IP アドレス（Remote IP Address）] フィールド	リモート マシンの IP アドレス。
[リモートポート（Remote Port）] フィールド	リモート マシンのポート番号。

ステップ 15 [送信（Submit）] をクリックします。

ステップ 16 [OK] をクリックします。

ステップ 17 [アプリケーション コンテナ テンプレート：外部ゲートウェイ セキュリティの設定（Application Container Template - External Gateway Security Configuration）] 画面で、[追加（+）（Add (+)）] アイコンをクリックしてアウトバウンド ACL を追加します。次のフィールドに入力します。

名前	説明
[プロトコル（Protocol）] ドロップダウン リスト	プロトコルを選択します。
[ネットワークの選択（Select the Network）] ドロップダウン リスト	ルールを適用する必要があるネットワーク。
[ソースアドレス（Source Address）] フィールド	送信元のクラスレス ドメイン間ルーティング（CIDR）の IP アドレス。

名前	説明
[接続先アドレス（Destination Address）] フィールド	送信先 CIDR の IP アドレス。
[アクション（Action）] フィールド	一致するネットワーク トラフィックで適用されるアクション。

ステップ 18 [送信（Submit）] をクリックします。

ステップ 19 [OK] をクリックします。

ステップ 20 [次へ（Next）] をクリックします。

ステップ 21 [アプリケーション コンテナ テンプレート：ポリシーの展開（Application Container Template - Deployment Policies）] 画面で、次のフィールドに入力します。

名前	説明
[コンピューティング ポリシー（Compute Policy）] ドロップダウン リスト	仮想コンテナのすべてのコンピューティング コンポーネントを展開するポリシーを選択します。
[ストレージポリシー（Storage Policy）] ドロップダウン リスト	仮想コンテナのすべてのストレージ コンポーネントを展開するポリシーを選択します。
[ネットワーク ポリシー（Network Policy）] フィールド	コンテナ ゲートウェイに展開するポリシーを選択します。コンピューティングポリシーの一部とみなされるホストは、Cisco Nexus 1000（Cisco VSG の展開に使用）と関連付ける必要があります。 （注） このフィールドは、コンテナ ゲートウェイの外部インターフェイスのみに使用されます。また、リソース割り当ては Cisco Nexus 1000 シリーズ スイッチと関連付ける必要があります。
[システム ポリシー（Systems Policy）] フィールド	DNS とその他の OS ライセンスの設定に使用される値。
[コスト モデル（Cost Model）] フィールド	コスト モデルを選択します。
[共通のネットワークポリシーを使用します（Use common network policy）] チェックボックス	VSG 管理ネットワークに上記で定義した共通ネットワーク ポリシーを使用するには、このチェックボックスをオンにします。
[管理ネットワーク ポリシー（Management Network Policy）] ドロップダウン リスト	[共通のネットワーク ポリシーを使用します（Use common network policy）] をオンにしなかった場合は、VSG 管理ネットワークのネットワーク ポリシーを選択します。

ステップ 22 [次へ（Next）] をクリックします。

ステップ 23 [アプリケーション コンテナ テンプレート：オプション（Application Container Template - Options）] 画面で、次のフィールドに入力します。

名前	説明
[エンドユーザ セルフサービス ポリシー（End User Self-Service Policy）] ドロップダウン リスト	アプリケーション コンテナ テンプレートに該当するエンドユーザ セルフサービス ポリシーを選択します。
[コンテナのセルフサービス削除の有効化（Enable Self-Service Deletion of Containers）] チェックボックス	オンにした場合は、コンテナのセルフサービス削除が有効になります。
[VNC ベースのコンソール アクセスの有効化（Enable VNC Based Console Access）] チェックボックス	オンにした場合は、VNC ベースの VM へのコンソールアクセスが有効になります。
[テクニカル サポート用の電子メール（Technical Support Email Addresses）] フィールド	コンテナのプロビジョニングに関して電子メールを受け取る担当者の電子メール アドレスのカンマ区切りのリストを入力します。

ステップ 24 [次へ（Next）] をクリックします。

ステップ 25 コンテナをセットアップするワークフローを選択します。

ステップ 26 ワークフロー リストを展開し、ワークフロー（たとえば、ワークフロー ID 431 フェンスド コンテナ セットアップ：VSG（Workflow Id 431 Fenced Container Setup - VSG））を選択します。

（注） ワークフローには、割り当てられたリソースが含まれている必要があります。たとえば、VSG ワークフローの場合は、Cisco Nexus 1000 シリーズのリソースが含まれている必要があります。

ステップ 27 [選択（Select）] をクリックします。

ステップ 28 [送信（Submit）] をクリックします。