ORACLE

仮想クラウド・ネットワーク (VCN) 概要

Virtual Cloud Network Level 100

Oracle Cloud Infrastructure 技術資料

2020年5月

Safe harbor statement

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。

以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。

オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。

OracleとJavaは、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。

文中の社名、商品名等は各社の商標または登録商標である場合があります。

目標

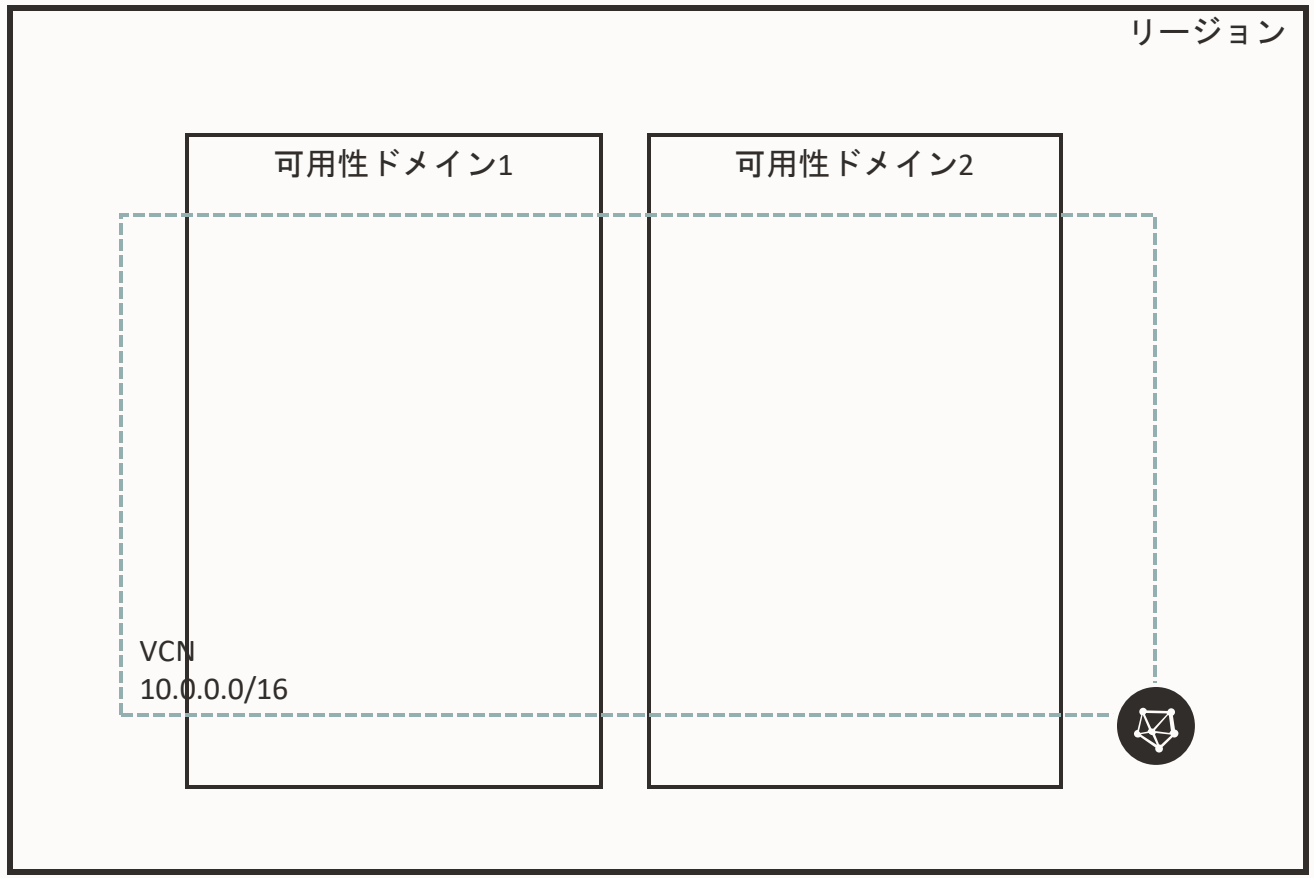
このレッスンを修了すると、次のことができるようになります

- 主要な仮想クラウド・ネットワーク (VCN) の概念についての理解
- 次のようなクラウド・ネットワーク・コンポーネントの管理
  - サブネット、ルート表、セキュリティ・リスト、プライベートIP、パブリックIP
- さまざまなOCI接続オプションの詳細
  - インターネット・ゲートウェイ、NATゲートウェイ、サービス・ゲートウェイ、ローカルおよびリモート・ピアリング
  - VPN、FastConnect

VCNとサブネット

VCNs and Subnets

仮想クラウド・ネットワーク (VCN)



Oracle Cloud Infrastructure内に作成するプライベート・ネットワーク

- 連続する単一 IPv4 CIDR が設定可能
- RFC1918のアドレス範囲を推奨
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- サイズは /30(4 IP) ～ /16(65534 IP)
- 一度作成するとアドレス範囲変更不可
- リソース有効範囲はリージョン
- 以下のアドレス範囲はOCIサービスが使用するためユーザー利用不可
  - 全般 : 169.254.0.0/16
  - DBCS : 192.168.16.16/28
  - Exadata CS : 192.168.128.0/20

CIDR の基本

CIDR (Classless Inter-Domain Routing) 記法

- xxx.xxx.xxx.xxx/n、n はサブネットマスクに使用されるビット数
  例) /24 の場合 サブネットマスク = 255.255.255.0
- 192.168.1.0/24 は IPアドレス範囲 : 192.168.1.0-192.168.1.255
  - 128 64 32 16 8 4 2 1 →27 26 25 24 23 22 21 20
  - 192は 1 1 0 0 0 0 0 0 として表される

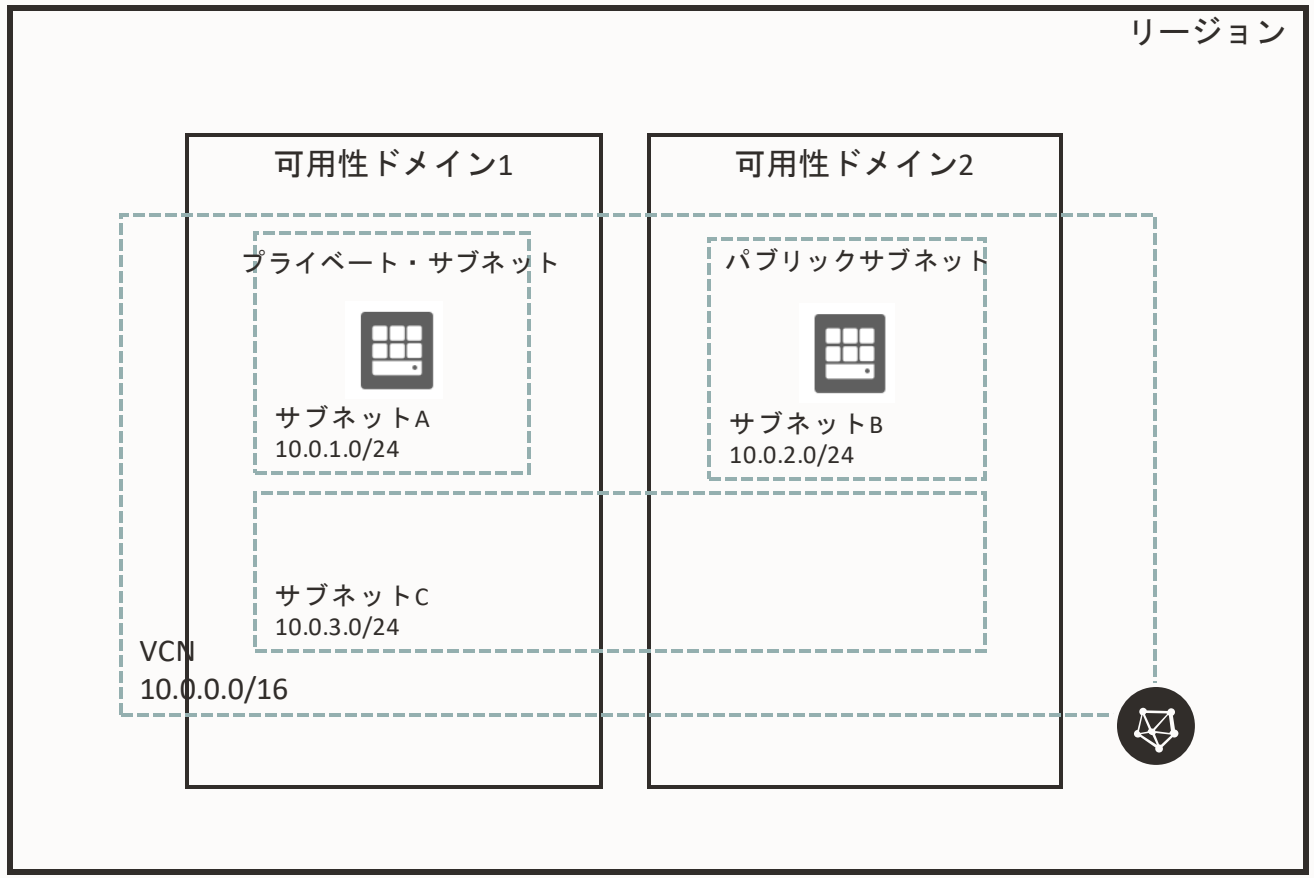
192.168.1.0	11000000.10100000.00000001.00000000	
255.255.255.0	11111111.11111111.11111111.00000000	→ 192.168.1.0 –192.168.1.255
AND	11000000.10100000.00000001.00000000	

- 192.168.1.0/27 は IP 範囲:192.168.1.0-192.168.1.31
  - ネットワークは8つのサブネットに分割され、32ホストは /27 マスク (255.255.255.224)

192.168.1.0	11000000.10100000.00000001.00000000
255.255.255.224	11111111.11111111.11111111.11100000
AND	11000000.10100000.00000001.00000000

  - Subnets – 2 x 2 x 2 = 8. Hosts – 2 x 2 x 2 x 2 x 2 = 32
  - Subnetworks – 192.168.1.0/27, 192.168.1.32/27, 192.168.1.64/27…

サブネット



VCNを分割する小さなネットワーク

他と重複しない連続したCIDRで構成

2種類の有効範囲

- **可用性ドメイン固有サブネット**–特定の可用性ドメイン(AD)に所属するサブネット
- **リージョナル・サブネット**–全ての可用性ドメインを跨るサブネット

2種類のインターネットアクセス制御

- **パブリック・サブネット**–所属するインスタンスの仮想NICがパブリックIPを持ち、インターネットと直接通信できる
- **プライベート・サブネット**–所属するインスタンスの仮想NICはプライベートIPしか持てず、インターネットと直接通信不可

IPアドレスのうち、最初の2つと最後の1つは予約済みで使用不可
(例 10.0.0.0/24 の場合 .0, .1, .255は予約済)

仮想NICとIPアドレス

Virtual NICs and IP Addresses

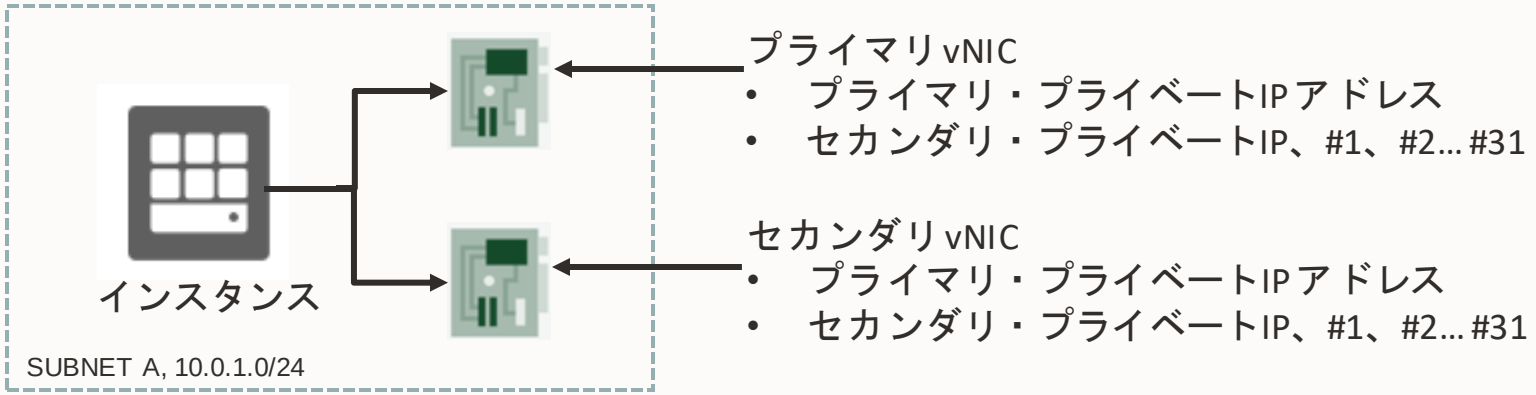
仮想NICとプライベートIPアドレス

各インスタンスは、必ず1つのプライマリ仮想NICと、その仮想NICにアサインされた1つのプライマリ・プライベートIPアドレスを持つ

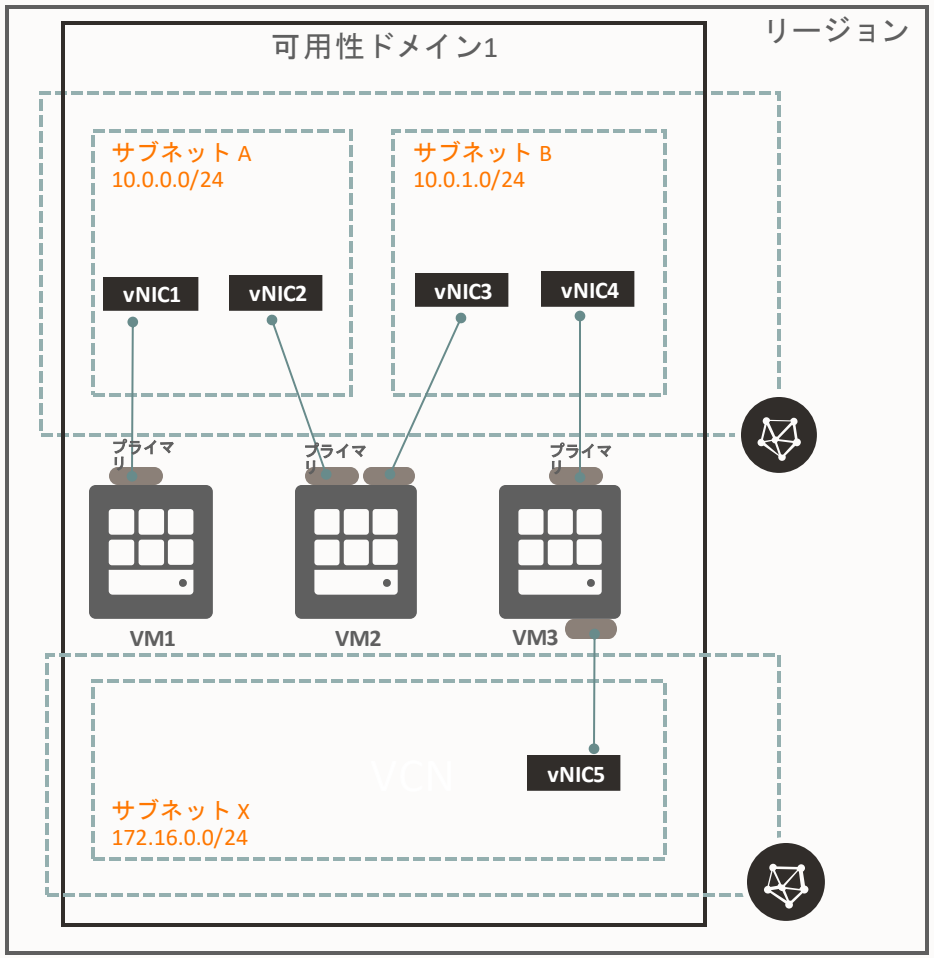
インスタンスには、少なくとも1つ以上のセカンダリ仮想NICを追加できる (最大数はコンピュート・シェイプによる)

各仮想NICには、セカンダリIPアドレスとしてプライベートIPを31個まで追加できる(IPエイリアス)

パブリック・サブネットに存在するプライベートIPアドレスには、オプションでそれぞれにパブリックIPアドレスを割り当てできる



仮想マシンインスタンスの複数仮想NIC

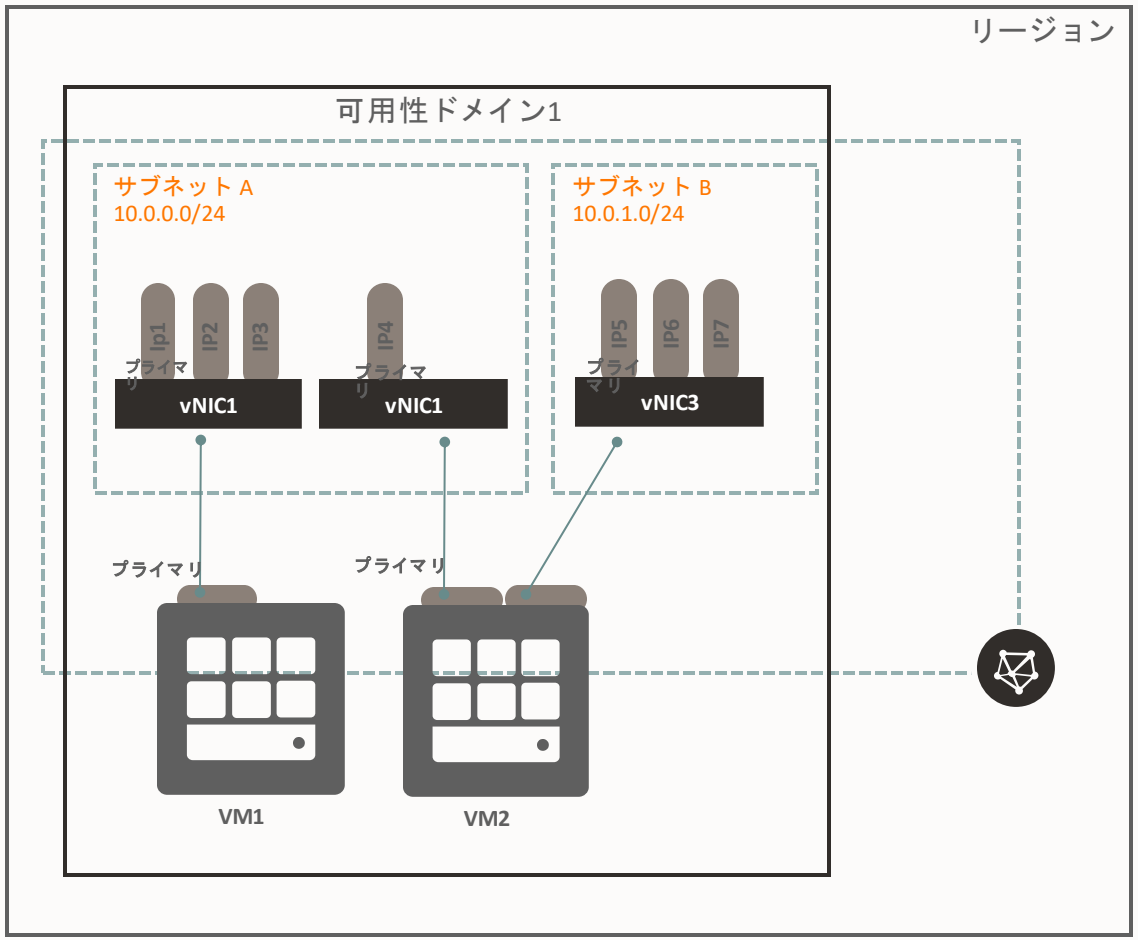


仮想マシン(VM)インスタンスは、1つのプライマリ仮想NICと、OS上にイーサネットデバイスが設定されて起動される

セカンダリ仮想NICを追加すると、OSで新しいイーサネットデバイスが認識される

- VM1 : 仮想NIC1つ
- VM2 : 仮想NICを2つ持ち、それぞれが同じVCN内の別のサブネットに接続
  - ユースケース : ネットワークアプライアンス
- VM3 : 仮想NICを2つ持ち、それぞれが別のVCNに接続
  - ユースケース : サービス用のネットワークと管理用のネットワークを分離する場合

仮想NICのセカンダリIPアドレス



両方の仮想NICが同じサブネットに属している場合、あるインスタンスの 仮想NICから別のインスタンスの仮想NIC にセカンダリ・プライベートIPを移動することが可能

- ユースケース : インスタンスのフェールオーバー

パブリックIP

パブリックIP アドレスは、インターネットから到達可能な IPv4 アドレス
インスタンスのプライベートIPに割り当て
仮想NICに複数のセカンダリIPが割り当てている場合、それぞれに対しパブリックIPを割り当て可能

インスタンス以外のパブリックIP の割り当て先

- OracleがパブリックIPを提供し、選択や変更は不可だがIPアドレスを接続などに使用できるもの
  - パブリック・ロードバランサー
  - NATゲートウェイ
  - DRG - IPsecトンネル
  - OKE マスターおよびワーカーノード
- OracleがパブリックIPを提供し、アドレスの選択、変更、閲覧が不可なもの
  - インターネット・ゲートウェイ
  - Autonomous Database

パブリックIP

2種類のパブリックIP

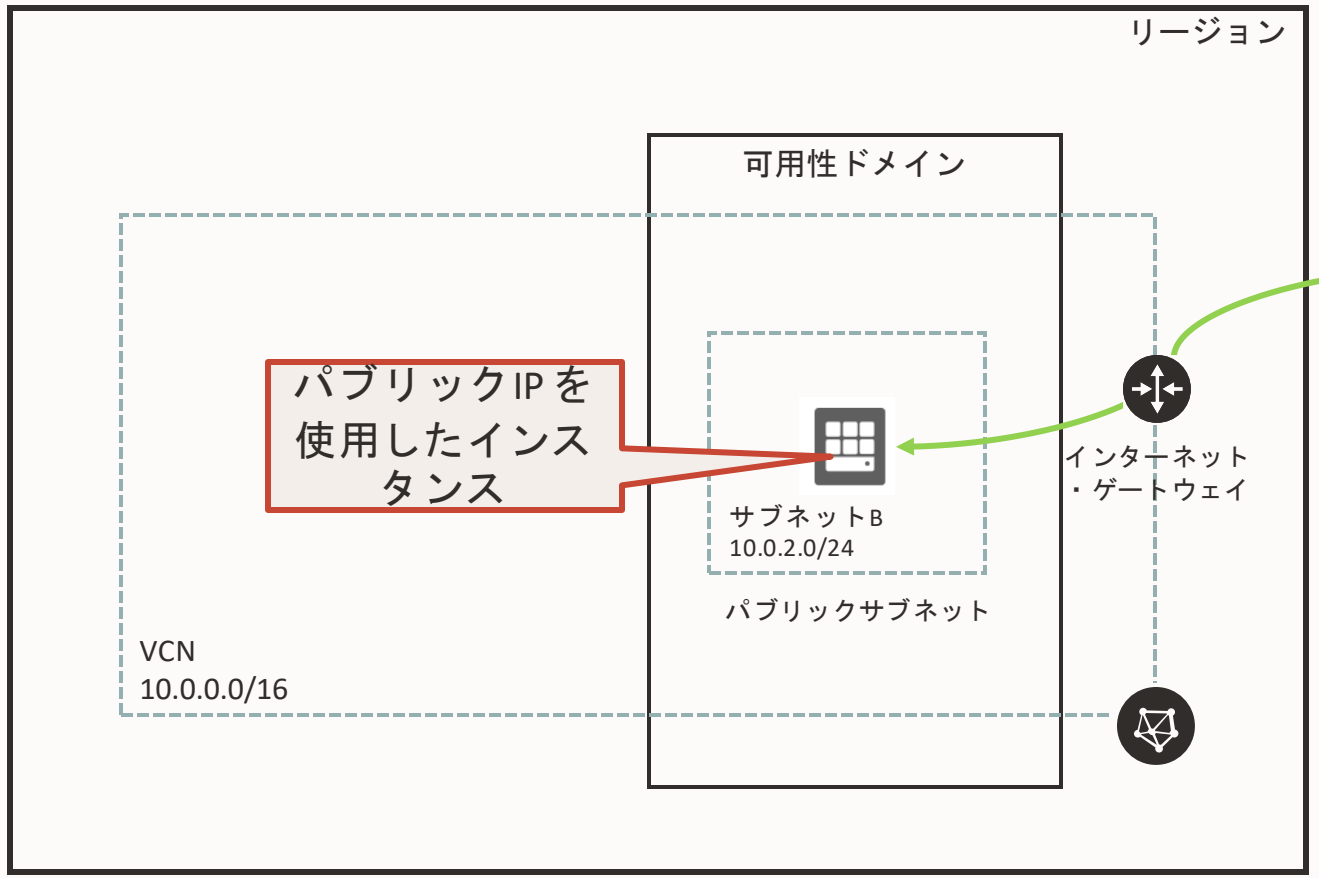
- エフェメラルIP
  - インスタンスに割り当てている間だけ有効
  - デタッチすると削除される
  - プライマリ・プライベートIP にのみ割り当て可能
- 予約済みIP
  - 永続的なIP
  - 割り当てられているインスタンスの存続期間を超えて存在できる
  - 割り当てを解除して別のインスタンスに再割り当てすることが可能
  - 仮想NICあたり最大32個割り当て可能

全てのパブリックIPは無料

ゲートウェイとルーティング

Gateways and Routings

インターネット・ゲートウェイ

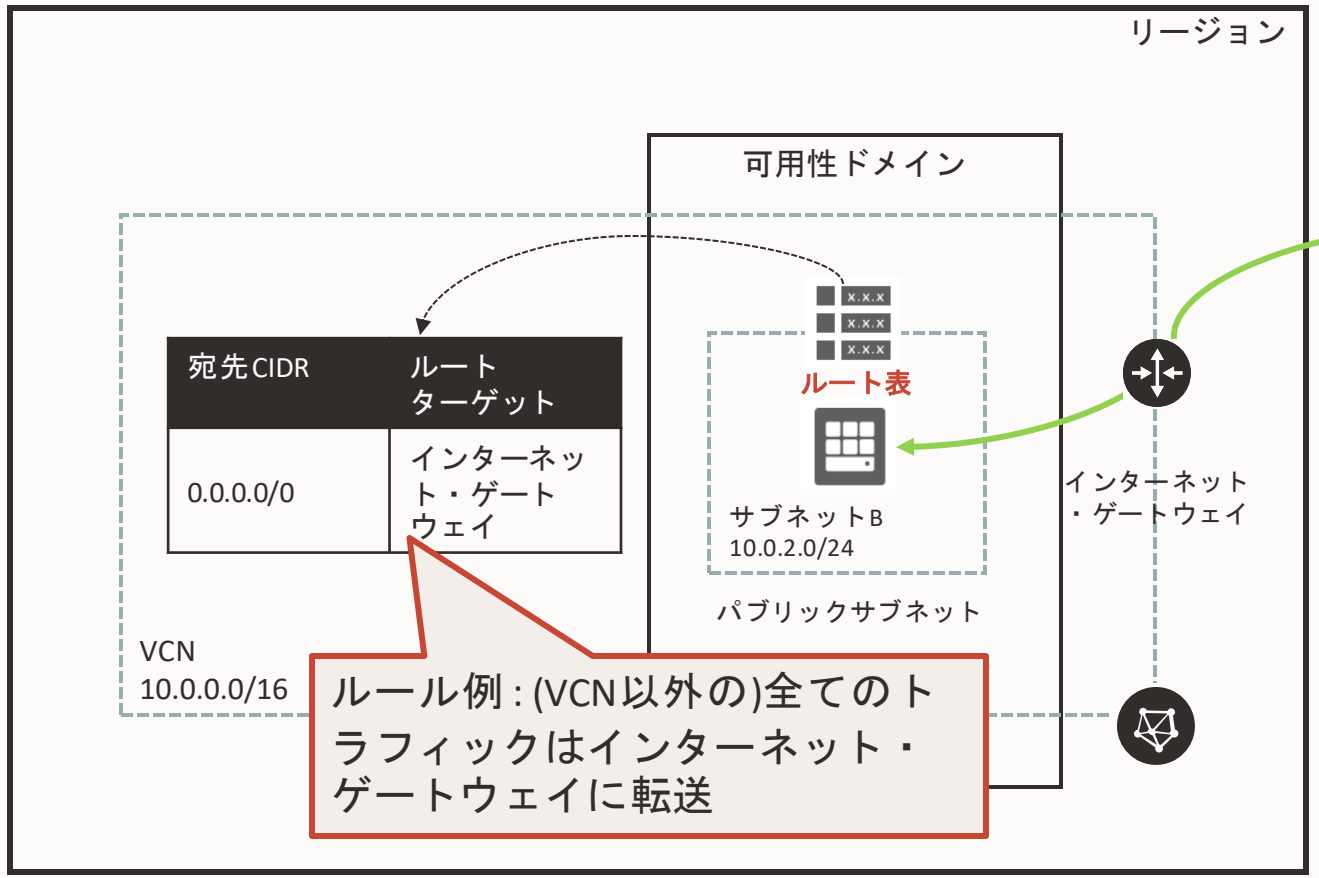


VCN内とインターネットの間の通信パスを提供するのためのゲートウェイ

インターネット・ゲートウェイはVCN毎に1つだけ設定可能(物理回線は冗長化されているためインターネット・ゲートウェイを複数設定する必要はない)

インターネット・ゲートウェイ作成後、VCNのルート表にゲートウェイへのルートを追加して、通信フローを有効にする必要がある

ルート表



VCN から外部のネットワークにトラフィックを送信する際に使用される

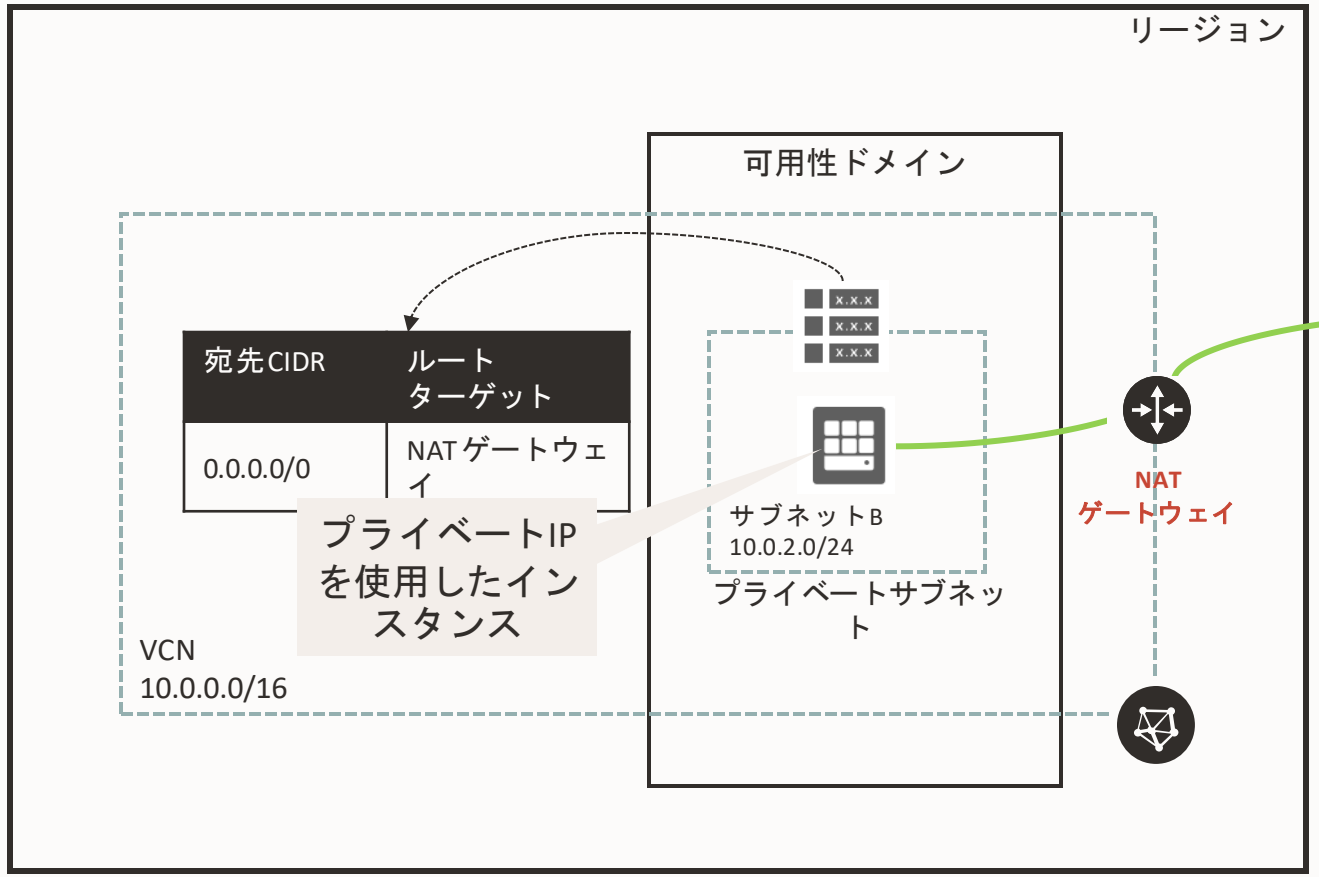
ルート表は複数のルールで構成

- ルールには以下を設定
  - 宛先ネットワークの CIDR ブロック
  - その CIDR に一致するトラフィックのルート・ターゲット(次ホップ)

VCN内は暗黙的にルーティングされるため明示的な設定不要、宛先アドレスがVCN内にない場合のみルート表が参照

各ゲートウェイを作成した場合は必ずセットでルート表の設定が必要

NAT ゲートウェイ

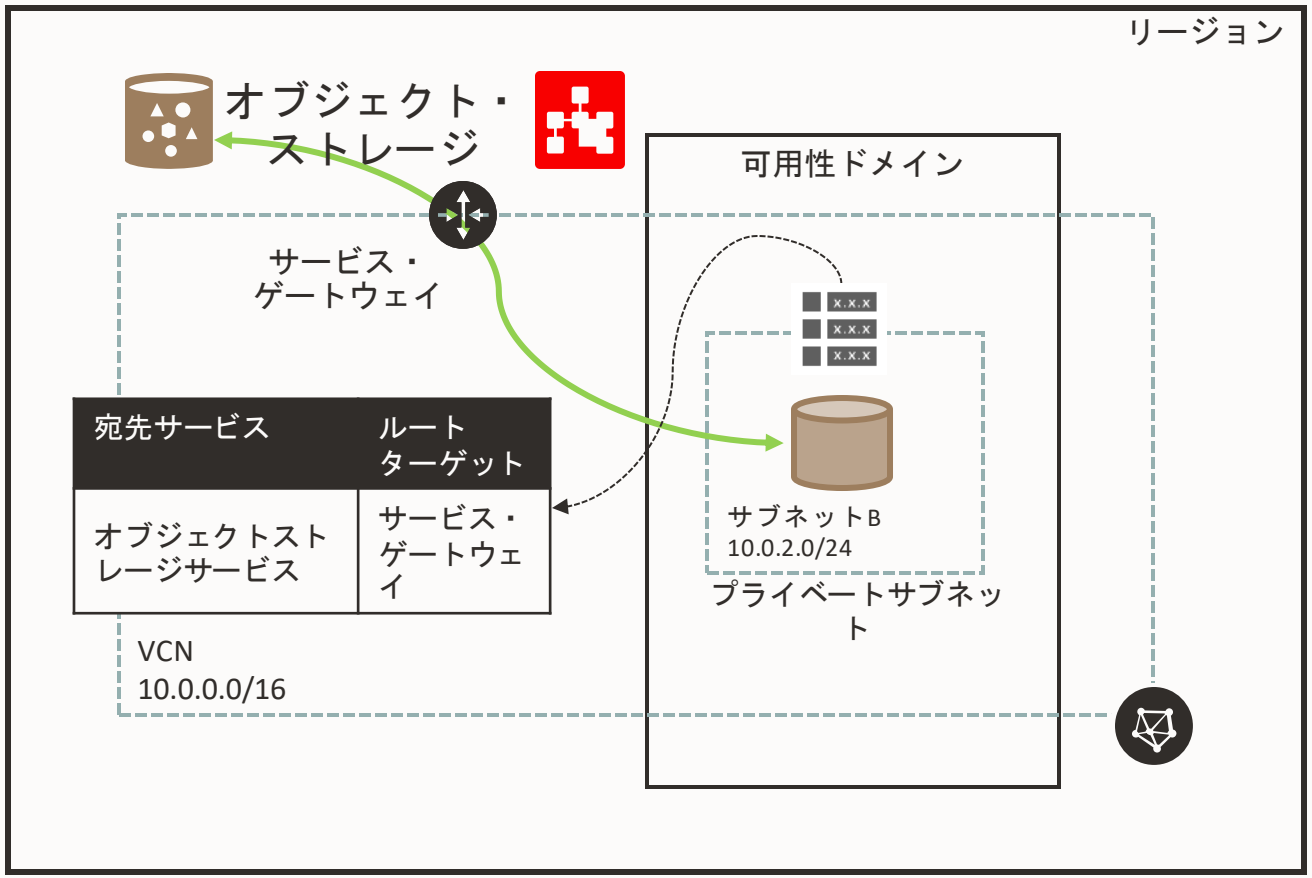


パブリックIPを持たないインスタンスにインターネットへのアクセスを提供するゲートウェイ

インターネットへのアウトバウンド通信とその応答の受信はできるが、インターネットからのインバウンド通信の受信は不可

VCNに複数のNATゲートウェイを紐づけることができるが、特定のサブネットは1つのNATゲートウェイにのみルーティングできる

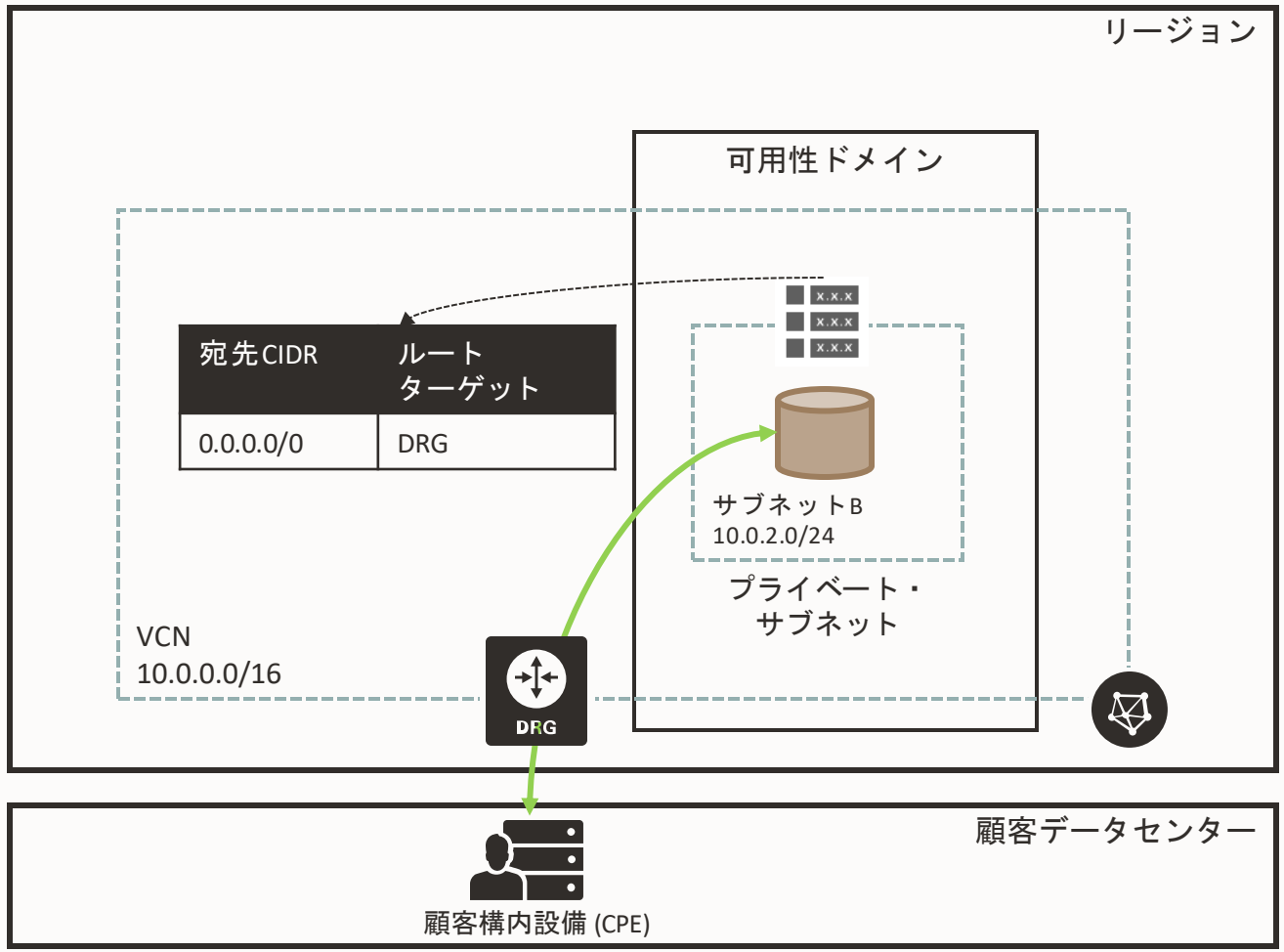
サービス・ゲートウェイ



VCNからOCIのリージョン内のサービスにアクセスできるゲートウェイ

- 特徴
  - インターネットを経由しない
  - OCIリージョン内にのみ到達できる
- メリット
  - インターネット・ゲートウェイやNATゲートウェイ不要
  - 外部との予期せぬ通信を防止できる
- ユースケース
  - DBシステムのバックアップをオブジェクトストレージに取得
  - VCN内のアプリからAutonomous Databaseに接続

動的ルーティング・ゲートウェイ(DRG)



VCN とインターネット以外のネットワークとの間のプライベート通信経路を提供する仮想ルーター

IPsec VPN または FastConnect (プライベート、専用接続) を介してオンプレミスネットワークとの接続を確立するために使用できる

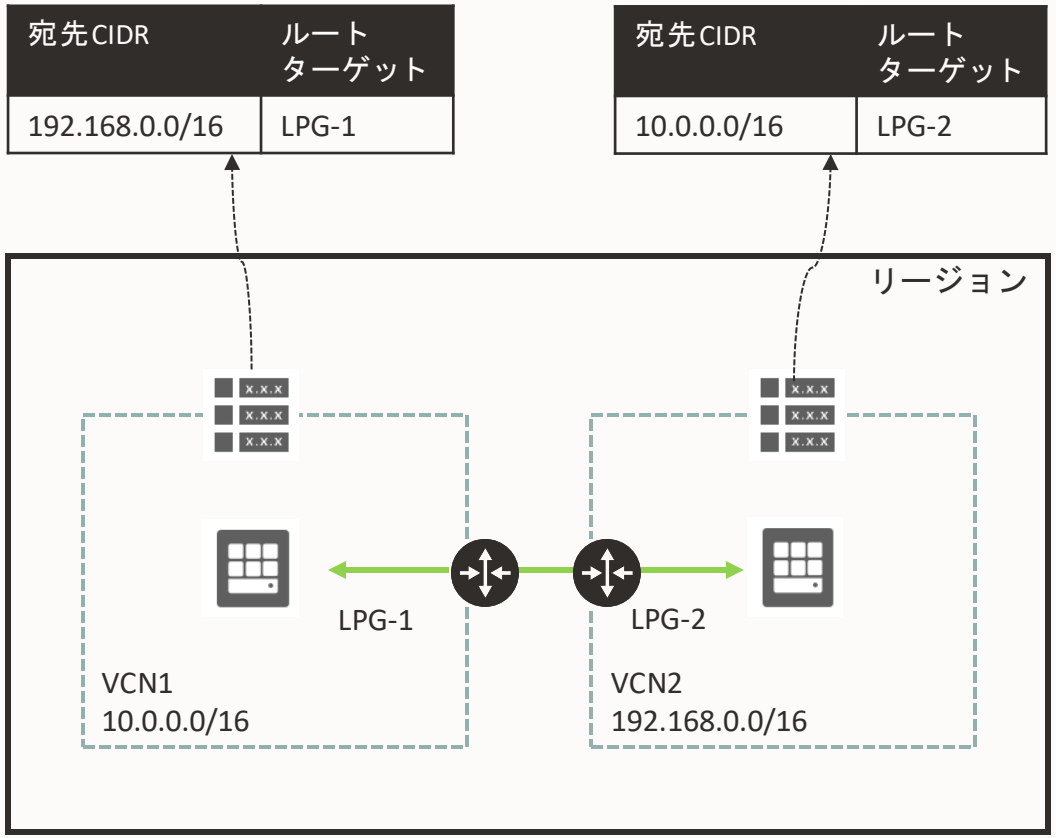
通信フローを有効にするには、VCN に DRG をアタッチした後 VCN のルート表に DRGへのルートをルールとして追加する必要がある

DRG はスタンドアロンオブジェクトのため、VCN と別個に作成したあと VCN にアタッチする必要がある。VCN と DRG は 1:1 の関係

ピアリング

Peerings

ローカルVCN ピアリング



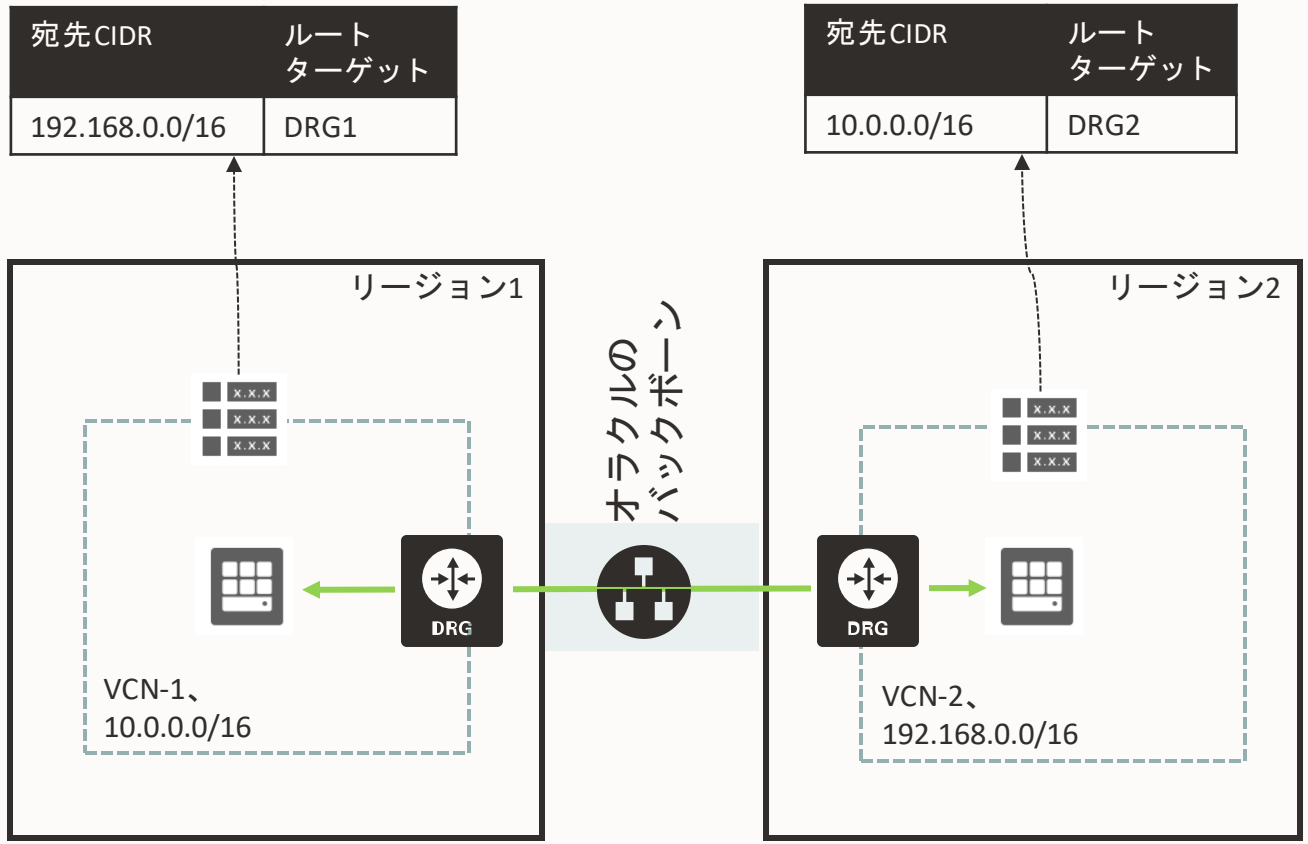
ローカル VCN ピアリングは、**同じリージョン**内にある2つのVCNを接続し、プライベートIP アドレスを使用して通信できるようにするもの

ピアリング先の VCN には、ローカル・ピアリング・ゲートウェイ (LPG) を通してトラフィックがルーティングされる

CIDRが重複する VCN 同士には ピアリングを設定できない

別のテナンシーにある VCN との間でもローカル VCN ピアリングが可能

リモートVCNピアリング



リモートVCNピアリングは、**異なるリージョンの**2つのVCNを接続して、プライベートIPアドレスを使用して通信できるようにするプロセス

ピアリング先のVCNには、動的ルーティング・ゲートウェイ(DRG)を通してトラフィックがルーティングされる

リージョン間の通信はOCIが持つバックボーン回線を経由

ピアリングの確立には、DRGでリモートピアリング接続(RPC)を作成する

CIDRが重複するVCN同士には ピアリングを設定できない

シナリオ別のOCIネットワーク接続オプション

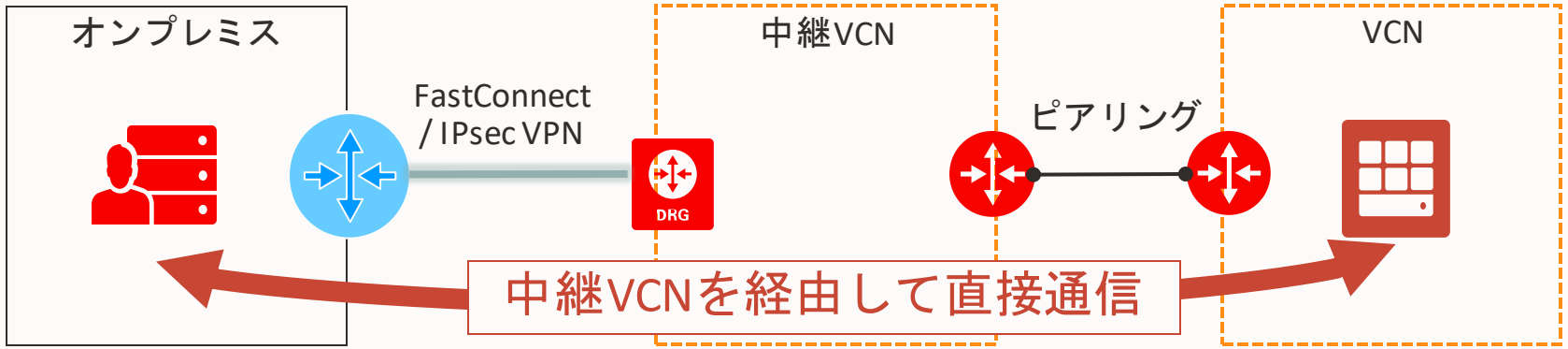
シナリオ	ソリューション
インターネットに公開するWebサーバーの設置	インターネット・ゲートウェイ
インバウンド通信は許可せず、インスタンスからのアウトバウンド通信のみを許可	NAT ゲートウェイ
インスタンスがプライベートにオブジェクト・ストレージに接続	サービス・ゲートウェイ
オンプレミスネットワークをクラウドに拡張	IPsec VPN FastConnect
同じリージョンの2つの VCN を接続	ローカルVCNピアリング
別リージョンの2つの VCN を接続	リモートVCNピアリング

トランジット・ルーティング

Transit Routing

VCN トランジット・ルーティング

VCNの1つを中継ネットワークとして機能させ、そのVCNを経由(トランジット)してオンプレミス・ネットワークと別のネットワークとの間の直接通信を可能にする技術



2つのユースケースで利用可

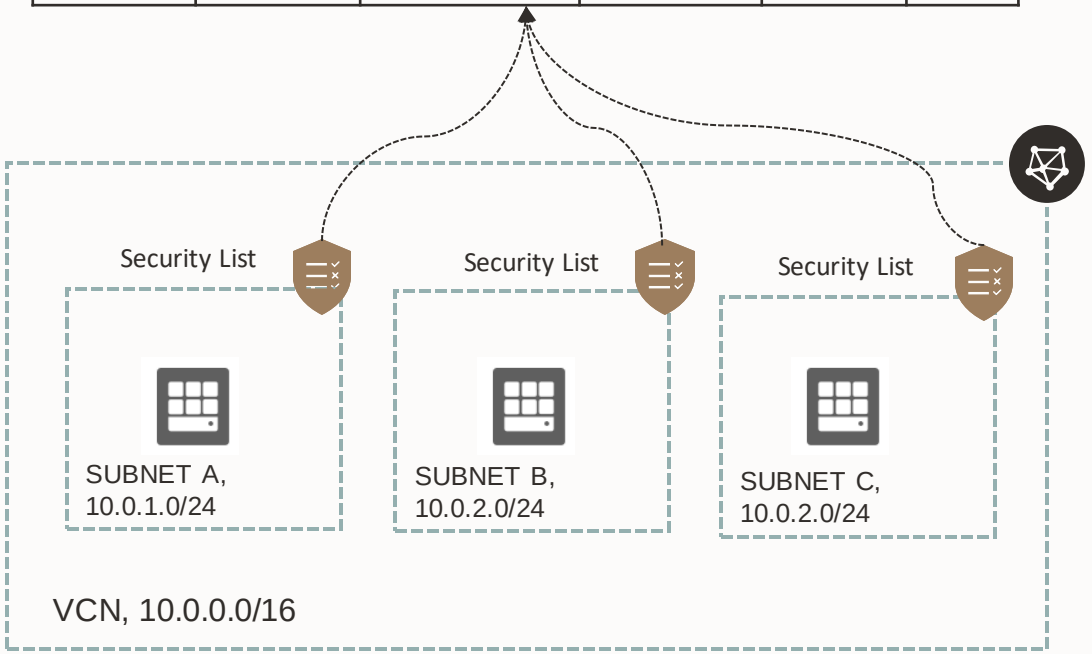
- **複数VCNでのFastConnect/VPN接続の共有**
  - 1つのFastConnectのプライベート仮想回線またはVPN接続を共有して、オンプレミスネットワークと同リージョンの複数のVCN間の直接通信が可能になる(別リージョンには不可)
- **VCN外のOracleサービスへのプライベート接続**
  - FastConnectやVPN接続を経由し、オンプレミスのホストからプライベートIPアドレスでVCN外のOracleサービス(Object Storage/Autonomous DB) にアクセスできる

セキュリティ

Security

セキュリティ・リスト

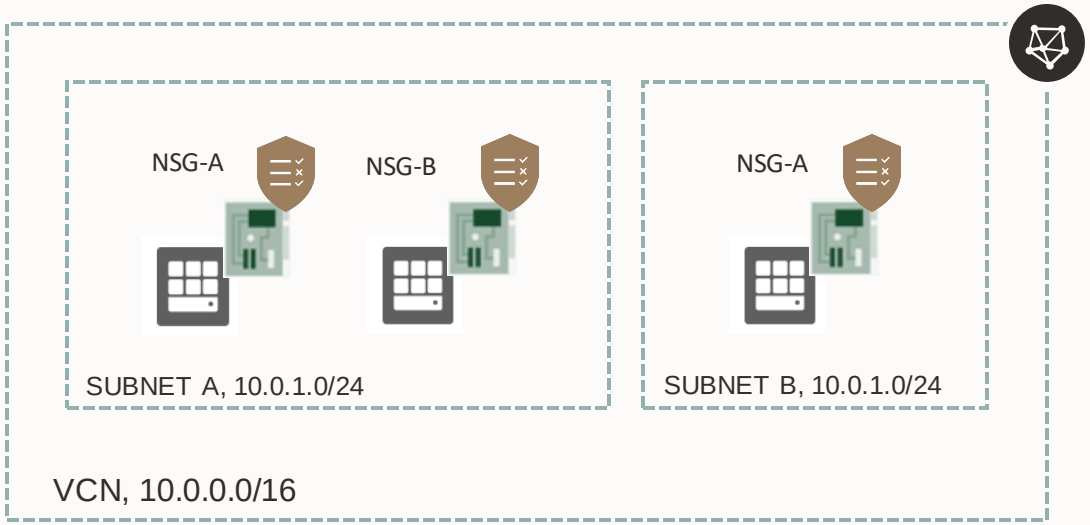
	Direction	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	10.0.2.0/24	TCP	All	1521



- サブネットに所属する仮想NICに適用されるファイアウォールのルール
- 各セキュリティ・リストには、インバウンド方向(イングレス)とアウトバウンド方向(エグレス) のルールを定義する
- ルールには通信の許可リストのみが定義可能
- ステートフル・ルールとステートレス・ルールを両方サポート
- 作成したセキュリティ・リストはサブネットに対してのみ紐づけ可能で、サブネット内のすべてのインスタンスの仮想NICにルールが一括適用される

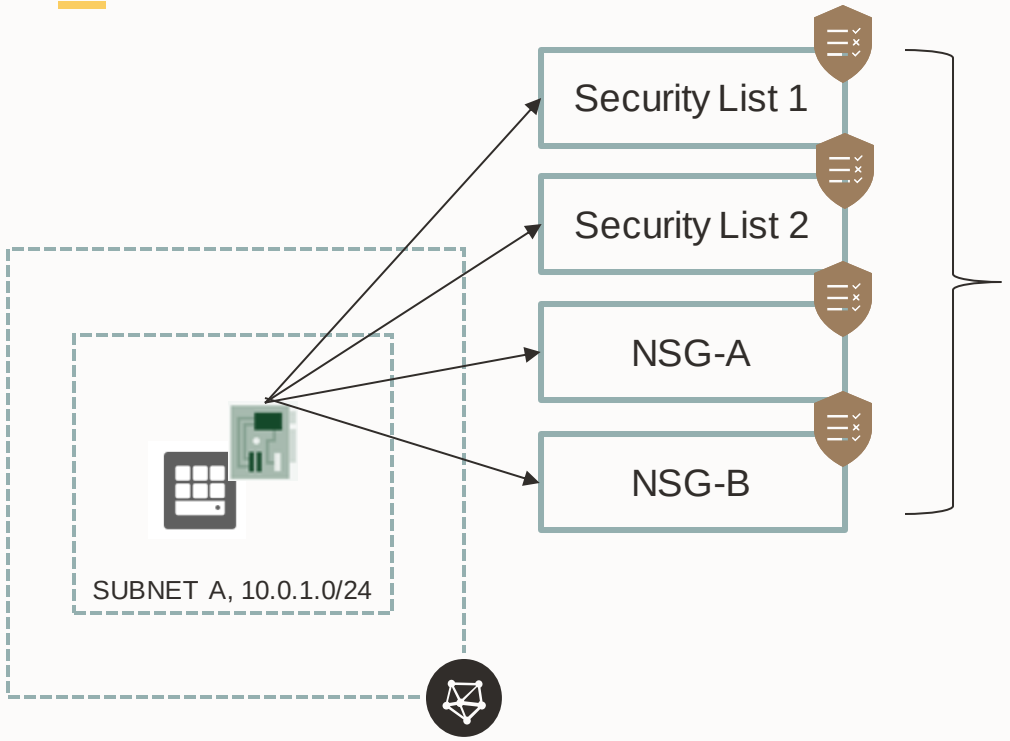
ネットワーク・セキュリティ・グループ(NSG)

		Direction	CIDR	Protocol	Source Port	Dest Port
NSG-A	Stateful	Ingress	0.0.0.0/0	TCP	All	80
NSG-B	Stateful	Ingress	0.0.0.0/0	TCP	All	22



- 任意の仮想NICの集まりに適用されるセキュリティ・ルールの設定
- NSGを使うと、セキュリティ・ルールの設定をサブネットと分離できる(セキュリティ・リストの場合はサブネット単位でのみ適用可能)
- NSG自身をソースまたは宛先としてルールに指定できる(セキュリティ・リストではCIDRのみが指定可能)

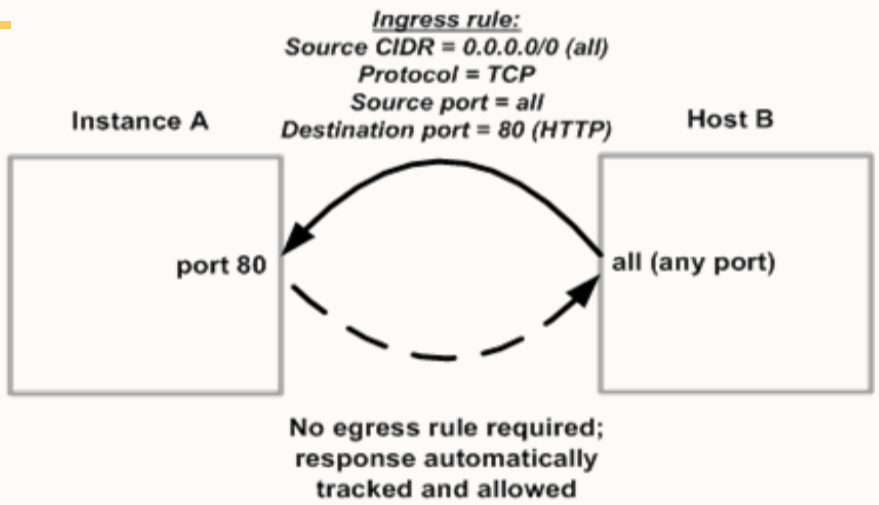
セキュリティ・リストとネットワーク・セキュリティ・グループの組み合わせ



SLとNSGの両方を使用した場合は、全てのルールがOR条件で通信が許可される

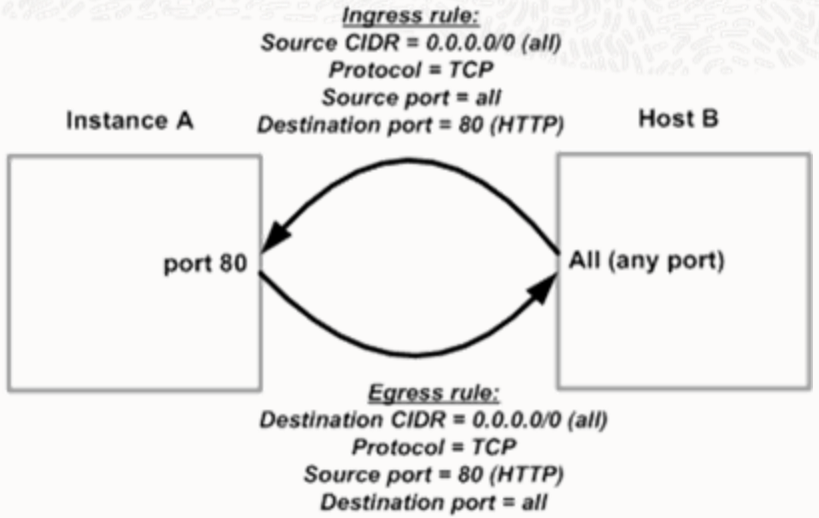
- 仮想NICが所属するサブネットに関連付けられたSL
- 仮想NICが関連づけられているNSG

ステートフル・ルールとステートレス・ルール



ステートフル・ルール

- エグレス・ルールで許可したパケットは、出入りするパケットの通信を追跡し、外部から送信されたパケットの通過の可否を**動的**に判断し、イングレス・ルール不要で双方向通信が可能
- 外部ホストからOCIへトラフィックを送信するイングレス・ルール場合も同様にステートフル・ルール設定が可能
- デフォルトはステートフル



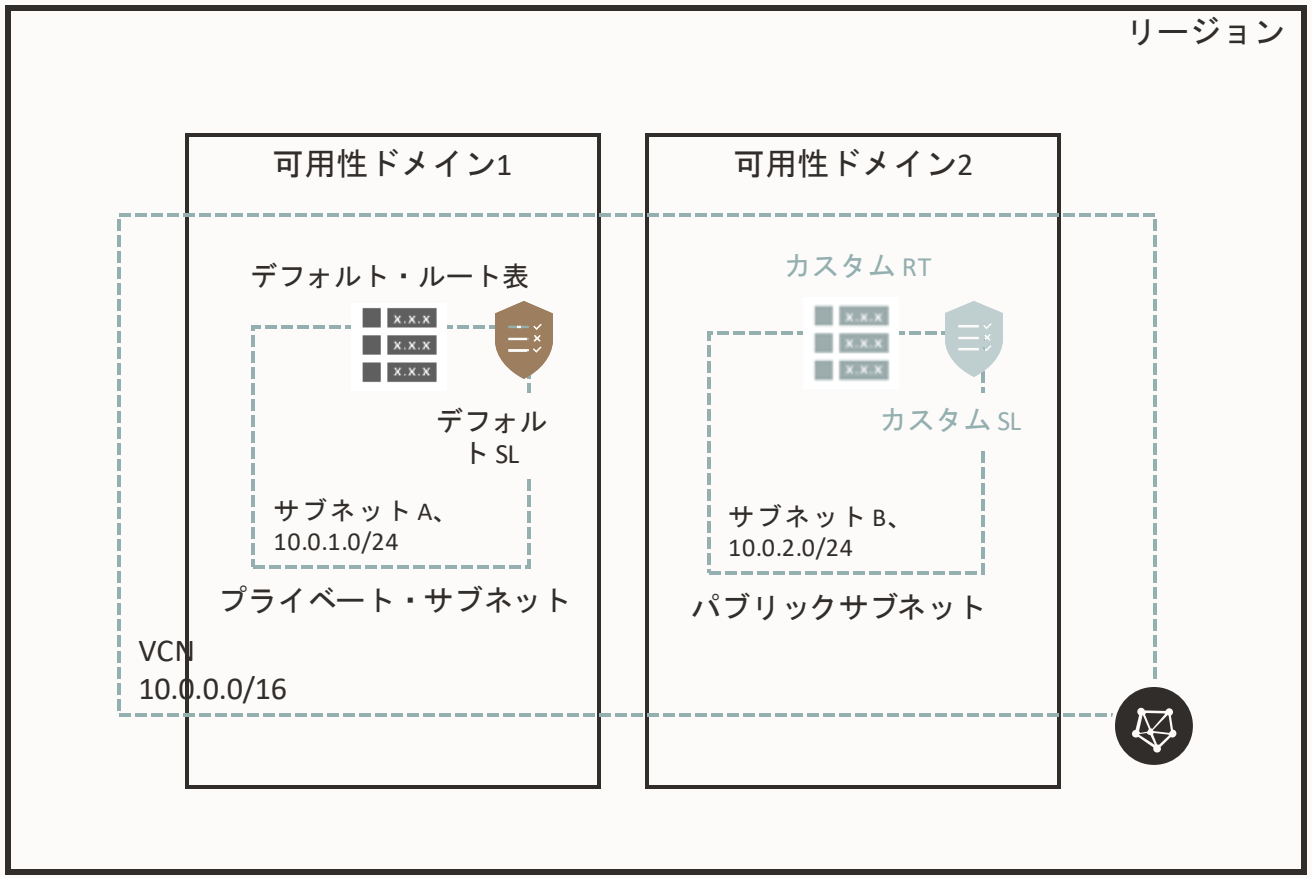
ステートレス・ルール

- エグレス・ルールで許可したパケットは、外部から応答されたパケットが条件に適合するかイングレス・ルールに従い、通過の可否を静的に判断
- ステートレス・ルールの設定は、そのルールに一致するすべてのトラフィックに対して接続追跡を使用しないことを示します。
- ステートレス・ルールは、 接続数が多い負荷のかかるシナリオWebサイト(HTTP/HTTPSトラフィック用) で有効

デフォルトのVCN設定、名前解決

Default VCN and Internal DNS

デフォルトVCN コンポーネント



VCN作成時には、初期状態でいくつかのコンポーネントが付属

- デフォルト・ルート・テーブル
- デフォルト・セキュリティ・リスト
- DHCP オプションのデフォルトセット

これらの既定のコンポーネントは削除不可、ただし内容は変更可能

- ルート・ルール、セキュリテイ・ルールの追加/変更
- 新規ルート・テーブル、セキュリティ・リストの追加

VCN内の名前解決

VCN内部ではプライベート・ドメインネーム・システム (DNS) により、インスタンスはIPアドレスの代わりにホスト名を使用して相互に通信できる

各インスタンスは、仮想NICの初期化時にVCN内に設置されたDHCPサーバーからリゾルバとサーチドメインの情報を受け取る

DHCPサーバーのリゾルバ設定のオプション：

- **インターネットおよびVCN**：VCN内部のDNSを利用しVCN内とグローバルの名前解決を行う(デフォルト)
- **カスタムリゾルバ**: VCN内やIPsec VPN / FastConnectで接続されたオンプレミス・ネットワーク内に独自に設置したDNSを利用し名前解決を行う(プライベートDNSサーバーのIPアドレスを指定)

VNC内のリゾルバを利用する場合は、VCN、サブネットの作成時にDNSラベルを指定できる

- インスタンスのFQDN : <hostname>.<サブネットのDNSラベル>.<VCNのDNSラベル>.oraclevcn.com

インスタンスのホスト名およびFQDNは、インスタンスのプライベートIPアドレスに解決される

パブリックIPアドレスのFQDNの自動作成はありません

- 例: <hostname>.<サブネットDNSラベル>.<VCN DNSラベル>.oraclevcn.comは、インターネットからの接続では使用不可

VCN レビュー

各サブネットは、1つのルート・テーブルと、複数の セキュリティ・リストを設定することが可能

ルート・テーブルは、VCN からルーティングできるものを定義

プライベート・サブネットは、VCN 外部のトラフィックフローを制御するために個別のルート表を持つことが推奨

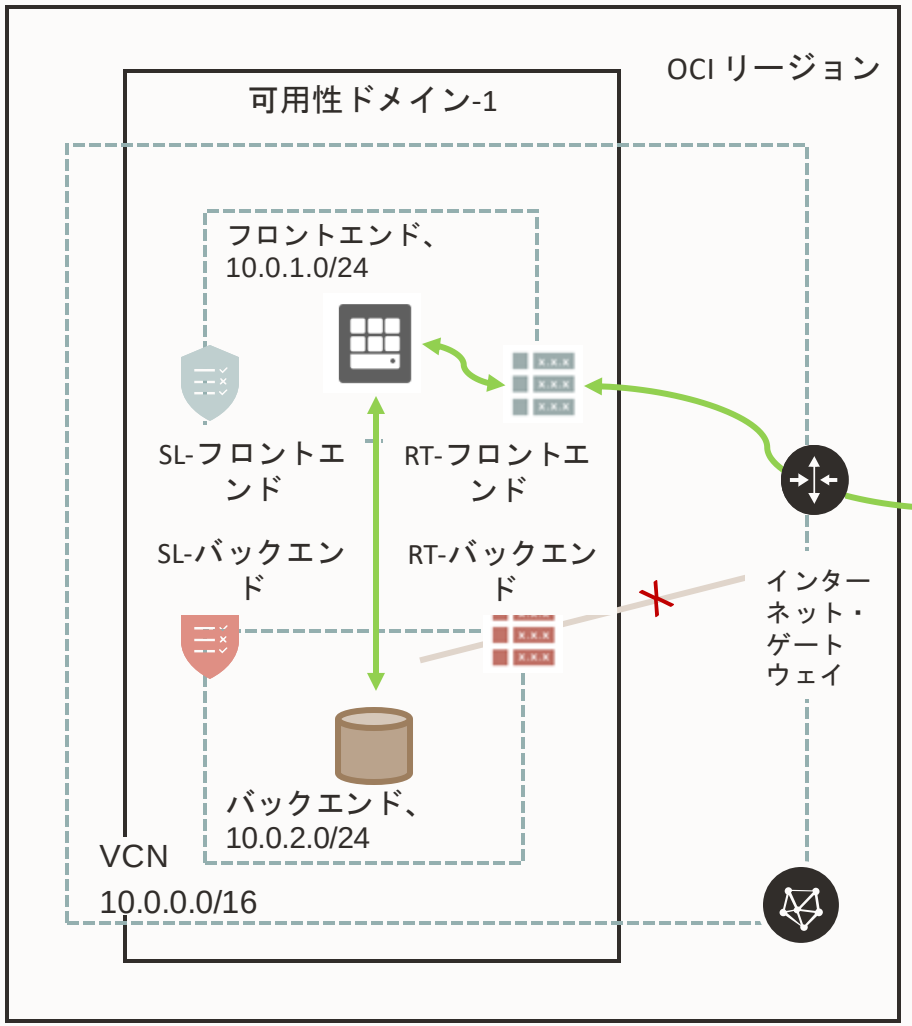
VCN 内のすべてのホストは、VCN 内の他のすべてのホストにルーティング可能 (ルート・テーブル不要)。

セキュリティ・リストは、 着信/発信 VCN トラフィック と複数のサブネット間の内部 VCN トラフィックの接続を管理

OCIはホワイト・リスト・モデルに従います（ホワイト・リストに含まれるトラフィック・フローを手動で指定する必要があります）デフォルトでは、すべてロックされています

セキュリティ・リストで許可しなければ、同じサブネット内であっても他のインスタンスと通信することはできません。

VCN レビュー



宛先CIDR	ルートターゲット
0.0.0.0/0	インターネット・ゲートウェイ

	タイプ	CIDR	プロトコル	送信元ポート	Destポート
ステートフル	Ingress	0.0.0.0/0	Tcp	すべて	80
ステートフル	Egress	10.0.2.0/24	Tcp	すべて	1521

宛先CIDR	ルートターゲット
0.0.0.0/0	NAT/サービス・ゲートウェイ/DRG

	型	CIDR	プロトコル	送信元ポート	Destポート
ステートフル	Ingress	10.0.1.0/24	Tcp	すべて	1521
~~ステートフル~~	~~Egress~~		~~すべて~~	~~すべて~~	

まとめ

このレッスンでは、次のことを学習しました

- 主要な仮想クラウド・ネットワーク (VCN) の概念についての理解
- 次のようなクラウド・ネットワーク・コンポーネントの管理
  - サブネット、ルート表、セキュリティ・リスト、プライベートIP、パブリックIP
- さまざまなOCI接続オプションの詳細
  - インターネット・ゲートウェイ、NATゲートウェイ、サービス・ゲートウェイ、ローカルおよびリモート・ピアリング
  - VPN、FastConnect

VCN 関連の技術情報

日本語マニュアル – ネットワーキング

- https://docs.oracle.com/cd/E97706_01/Content/Network/Concepts/overview.htm

チュートリアル – クラウドに仮想ネットワーク(VCN)を作る

- https://community.oracle.com/docs/DOC-1019114

Oracle Cloud Infrastructure マニュアル・ドキュメント

Oracle Cloud Infrastructure マニュアル

- https://docs.oracle.com/cd/E97706_01/Content/home.htm - マニュアル(日本語)
- https://docs.cloud.oracle.com/iaas/api/ - APIリファレンス
- https://docs.oracle.com/cd/E97706_01/Content/General/Reference/aqswhitepapers.htm - テクニカル・ホワイト・ペーパー
- https://docs.cloud.oracle.com/iaas/releasenotes/ - リリースノート
- https://docs.oracle.com/cd/E97706_01/Content/knownissues.htm - 既知の問題(Known Issues)
- https://docs.oracle.com/cd/E97706_01/Content/General/Reference/graphicsfordiagrams.htm - OCIアイコン・ダイアグラム集(PPT、SVG、Visio用)

Oracle Cloud Infrastructure トレーニング・技術フォーラム

Oracle Cloud Infrastructure 活用資料集

- https://community.oracle.com/docs/DOC-1035494

チュートリアル - Oracle Cloud Infrastructureを使ってみよう

- https://community.oracle.com/docs/DOC-1019313

Oracle 主催 セミナー、ハンズオン・ワークショップ

- https://www.oracle.com/search/events/
  (右側の Filter から Locations -> Asia Pacific -> Japan と絞り込み)

Oracle Cloud Infrastructure – General Forum (英語)

- https://cloudcustomerconnect.oracle.com/resources/9c8fa8f96f/summary

Thank You

ORACLE