ORACLE

Learn OCI Network Firewall in Oracle Cloud Infrastructure with Examples

テクニカル・スタッフ、コンサルティング・メンバー
Troy Levin 2025年1月、バージョン1.0

免責事項

このドキュメントには、ソフトウェアまたは印刷物などの形式を問わず、オラクルが独占的な権利を有する財産的情報が含まれています。この機密資料へのアクセスと使用は、オラクルとの間で締結され遵守に同意したオラクル・ソフトウェア・ライセンスおよびサービス契約の条件に従うものとします。このドキュメントとその内容の開示、コピー、複製および配布には、オラクルによる事前の承諾を必要とします。このドキュメントはライセンス契約の一部となるものではなく、オラクルおよびその子会社や関連会社との契約を構成するものではありません。

このドキュメントは情報提供のみを目的としており、記載した製品機能の実装およびアップグレードの計画を支援することのみを意図しています。このドキュメントはマテリアルやコード、機能の提供をコミットメント（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。このドキュメントに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。製品アーキテクチャの性質により、コードの大幅な不安定化を招くリスクを冒さずに本書に記載されているすべての機能を安全に組み込むことは不可能な場合もあります。

改訂履歴

このドキュメントには、次の改訂が加えられています。

日付	改訂内容
2025年1月	初版

目次

はじめに

Oracle Cloud Infrastructure (OCI) Network Firewallサービスは、OCIのネットワーク・セキュリティ・オファリングの基礎となるもので、最新のクラウド・ワークロードを保護しながらシームレスなネットワーク機能を保証するように設計されています。オラクルは、OCIワークロードの保護を目的としたクラウド・ネイティブなフル・マネージド型の次世代ファイアウォール・サービスであるOCI Network Firewallサービスを、Palo Alto Networksと提携して提供しています。OCI Network Firewallは、高度なセキュリティ機能を幅広く提供し、様々なネイティブOCIサービスとシームレスに統合されています。

このテクニカル・ペーパーでは、OCI Network Firewallサービスについて深く掘り下げ、ネットワーク・トラフィックの保護、脅威の検知と防止、セキュリティ・ポリシーの施行においてこのサービスが果たす役割を明らかにします。さらに、OCIネットワーク・ファイアウォールがOCIクラウド・ネットワーク内のセキュリティを強化する一般的な設計シナリオとユース・ケースに焦点を当て、ファイアウォールの核となる機能を紹介します。ネットワーク・アーキテクト、セキュリティ・エンジニア、クラウド管理者、技術的ビジネス意思決定者向けのガイドとして構成されているこのテクニカル・ペーパーでは、ファイアウォールの機能と実務での応用について説明します。

このガイドでは、まずファイアウォールの機能の概要を示し、堅牢なクラウド・セキュリティ・ソリューションを実現するファイアウォールの機能を紹介します。次に、ファイアウォール・ポリシーの作成について掘り下げ、トラフィック・フローを管理してセキュリティを強化するルールを定義および実装するためにポリシー・モデルを利用する方法を説明します。最後に、ファイアウォール挿入の一般的なルーティング・シナリオを検討し、様々なネットワーク・アーキテクチャ内にファイアウォールを戦略的に配置して、ファイアウォールの有効性を最大限に高める方法を示します。目標は、読者が自身の環境にOCIネットワーク・ファイアウォールを効果的に実装し、その潜在能力をフルに活用してセキュアで効率的なクラウド運用を実現できるようにすることです。

記載されている内容は、公開の時点で利用可能な機能と構成に基づいています。OCIとOCI Network Firewallサービスは進化を続けているため、新しい機能や改善点が導入されて、それらが記載の情報に影響を与える可能性があります。最新の情報については、OCI Network Firewallのドキュメントを参照することをお薦めします。このドキュメントは、定期的に更新して、OCI Network Firewallサービスの最新の動向を正確に反映させることが求められているためです。

OCIネットワーク・ファイアウォール機能の概要

この項では、堅牢なネットワーク・セキュリティ戦略を策定する上で欠かせない主要なファイアウォール機能の総合的な概要を示します。ファイアウォールを効果的に使用してトラフィック・フローを制御し、セキュリティ・ポリシーを施行するには、核となる機能を理解することが重要です。ファイアウォールの主要な機能には次のものがあります。

- **ステートフル・ネットワーク・フィルタリング:** トラフィックを動的にモニタリングし、トラフィックの状態に基づいて接続を許可または拒否します
- **カスタムURLフィルタリング:** Webトラフィック・アクセスの正確な制御を可能にします
- **侵入検知および防止:** 脅威をリアルタイムに識別してブロックします
- **Secure Sockets Layer (SSL)検査:** 暗号化されたトラフィックを復号して分析し、隠れたリスクを明らかにします。

これらの機能が個々にどう働くのか、連係してどう働くのかを理解することで、特定のニーズに即したセキュリティ戦略をより的確に設計できます。これらの機能は、不正なアクセスのブロックからネットワーク全体にわたるセキュアなデータ・フローの確保まで、トラフィックの動作を定義して管理するポリシーを作成するための構成要素となります。この基本的な理解があれば、これらの高度な機能を正確で実行可能なコントロールに変えるポリシーを作成できます。

ステートフル・ネットワーク・フィルタリング

ステートレス・ルールは、一方向に移動している1つのパケットのヘッダーのみに注目して、各パケットを個別に評価します。状態情報は保持されません。ステートレス・ルールはトラフィックの処理をそれほど必要としないため、パフォーマンスとスケールに優れています。ステートフル・ルールは、各パケットの情報を保持したまま、通信フロー全体のコンテキスト内でアクティブな接続状態を追跡するため、双方向でのパケット・フローの検査が可能になります。この機能により、トラフィックを許可するかブロックするかの決定を十分な情報に基づいて下すことができます。

OCI Networkingには、仮想クラウド・ネットワーク(VCN)向けにステートレスとステートフル両方のセキュリティ・リストとネットワーク・セキュリティ・グループ(NSG)が用意されており、これらを使用してワークロードを保護できます。これらのセキュリティ・リストとNSGは、許可リスト・モデルに従い、定義済のプロトコルとポートに基づいてトラフィックを許可する一方で、一致しないトラフィックを暗黙的に拒否します。ただし、特にインフラストラクチャが拡大するにつれて、よりスケーラブルで柔軟なセキュリティ・ソリューションが必要になることも多くあります。

OCI Network Firewallを使用すると、IPv4/IPv6のソースまたは宛先アドレス、プロトコル、ポートに基づいてトラフィックを許可またはブロックするステートフル・フィルタリング・ルールを実装できます。OCI Network Firewallは、高度なステートフル・ネットワーク・フィルタリングでセキュリティを強化するため、スケーラビリティと柔軟性を求める企業に最適です。OCI Network Firewallは、許可リストと拒否リストの両方の作成をサポートし、サービス・リストとNSGよりも優れたコントロール、スケール、適応性を提供するとともに、多様で複雑なセキュリティ要件を効果的に満たします。

ステートフル・セキュリティ・ルールは、Transmission Control Protocol (TCP)セッションやUser Diagram Protocol (UDP)フローなどのネットワーク接続の状態を追跡し、個々のパケットではなく接続のコンテキストに基づいてトラフィックを許可または拒否します。クライアントからサーバー(c2s)とサーバーからクライアント(s2c)とは、クライアントが開始したフローとサーバーの間のデータ・フローの方向を意味します。ファイアウォールは、各セッション内でc2sとs2c両方のフローをモニタリングし、着信パケットを既存のセッションに対してチェックして、元のセキュリティ・ポリシーを適用します。ポリシーを定義する際には、c2s方向のみを考慮し、保護対象リソースへの着信トラフィックに的を絞って構成を簡素化します。一方、s2cフローは自動的に管理されます。この方法であれば、IPアドレス、ポート、プロトコル、シーケンス番号などの詳細をモニタリングして、トラフィックのフィルタリングと接続の追跡を効率的に行うことができます。

セッションが確立され、パケットがファイアウォールに到着すると、トラフィックは当初、アプリケーションのタイプを特定する目的で通過を許可されます。ファイアウォールは、最も寛容なセキュリティ・ルールに従ってトラフィックを処理します。その際、セキュリティ・ルールは上から下へ、左から右へ評価されます。トラフィックが不完全または不十分な場合、アプリケーションを特定できなかったか、TCPハンドシェイクが正常に完了しなかったことを意味します。トラフィックは当初、アプリケーションを特定する目的で通過を許可され、(許可されたとおり)それ以上の処理は行われなかったため、トラフィックのログではトラフィックが「許可された」ように見えます。

ファイアウォールは、セキュリティ・ルールを使用して、トラフィックを許可するか拒否するかを決定します。各ルールは、ソースと宛先のIPアドレス、サービス、ポート、プロトコル(TCPまたはUDP)などのパラメータに基づいています。トラフィックがセキュリティ・ルールに一致すると、ファイアウォールは対応するアクション(許可、ドロップ、拒否、侵入検知、侵入防止)を適用します。それ以上のルールは処理されません。TCPの場合、ファイアウォールは3方向ハンドシェイクを追跡し、パケットのシーケンス番号、TCPフラグ、接続終端に基づいて接続にフラグを立てます。UDPのようなその他のステートレス・プロトコル(コネクションレス)の場合、ファイアウォールはタイミングと通信パターンに基づいてフローを追跡し、セッションを見積もります。セキュリティ・ルールに一致せず、確立されたセッションの一部ではないトラフィックは、暗黙的に拒否されます。アクションがドロップの場合、トラフィックはサイレントにドロップされ、リセットの通知は送信されません。アクションが拒否で、TCPの場合、リセットがクライアントとサーバーの双方向に送信されます。UDPの場合、ICMP Type 3 - Destination Unreachable、Code 13 - Communication Administratively Prohibitedがクライアントに送信されます。

セッションは、ルーティングが対称的な場合にのみ、完全に分析されます。これは、ステートフル・セキュリティ・ルールの性質上、必要であるためです。サーバーのレスポンスがなければアプリケーションの状況を特定できないため、不完全なセッションを非対称のパスでの脅威から保護することはできません。

カスタムURLフィルタリング

OCI Network FirewallでカスタムURLフィルタリングを使用すると、管理者は特定のWebサイトへのアクセスを管理およびモニタリングできます。インバウンドおよびアウトバウンドのHTTP/HTTPSトラフィックを完全修飾ドメイン名(FQDN)の事前定義済リストに制限するなどのアクションがあり、ワイルドカード、サブドメイン、カスタムURLがサポートされています。管理者は、特定のURLやドメインをブロックまたは許可するカスタムURLリストを作成できます。カスタムURLフィルタリングは、制限されたサイトや業務に関係のないサイトへのアクセスをブロックすることで、ネットワークのセキュリティを高め、組織の利用規定へのコンプライアンスを強化します。

カスタムURLフィルタリングを平文のHTTP Webトラフィックと暗号化されたHTTPS Webトラフィックの両方に適用することで、次のシナリオにおけるポリシー施行が可能になります。

- **平文のHTTPトランザクション**: URLフィルタリング・ポリシーは、クライアントのリクエストのHTTPホストおよびURLパス・ヘッダーを検査して、ルールを施行します。
- **暗号化されたHTTPSトランザクション**: ポリシーは、TLS Client HelloハンドシェイクのServer Name Indication (SNI)フィールドを調べて、URLを特定します(TLSのバージョンが1.2以前の場合)。TLSのバージョンが1.3以降の場合、SNIフィールドは暗号化されていない場合にのみ使用できます。
- **暗号化されたHTTPSがポリシーの復号ルールに一致**: URLフィルタリング・ポリシーは、復号されたリクエストのHTTPホストおよびURLパス・ヘッダーを検査します。TLS Client HelloハンドシェイクのSNIフィールドは無視されます。

侵入検知および防止

侵入検知と侵入防止の2つは、ネットワークを悪意のある活動から保護するのに役立つ、OCI Network Firewallの重要なセキュリティ機能です。侵入検知システム(IDS)は、ネットワーク・トラフィックをモニタリングし、疑わしいパターンや既知の脅威がないか分析して、潜在的な侵入が検知された場合はアラートを生成します。ただし、脅威を阻止するためのアクションは実行しません。これとは対照的に、侵入防止システム(IPS)は、疑わしい活動を検知するだけでなく、リアルタイムで脅威を能動的にブロックまたは軽減し、脅威がネットワークに害を及ぼすのを防止します。IDSが可視性と警告に焦点を当てているのに対し、IPSは積極的な防御と自動化された対応を重視しています。この2つを併用することで、ファイアウォールのネットワーク保護機能を強化できます。OCI Network Firewallには、業界をリードするPalo Altoの侵入検知および防止システムが含まれており、すべてのポートおよびプロトコルでマルウェアや脆弱性の悪用、コマンドアンドコントロール(C2)活動を識別します。暗号化されたトラフィックと暗号化されていないトラフィックの両方がこの機能の対象となります。

OCI Network Firewallが使用する脅威シグネチャは次のカテゴリに分類されます。

- **アンチウイルス:** ワーム、トロイの木馬、スパイウェアのダウンロードなど、様々な形態のマルウェアやウイルスを識別します。
- **アンチスパイウェア:** セキュリティ侵害を受けたホストに、外部C2サーバーへの接続やビーコン送信を行おうとするC2スパイウェアがないかモニタリングします。
- **脆弱性:** システムの脆弱性を検知して利用するように設計されています。

OCI Network Firewallサービスは、アンチウイルス・コンテンツのアップデートとアプリケーションおよび脅威コンテンツのアップデートという2つのアップデート・パッケージの形でシグネチャのアップデートを受け取ります。パッケージは、サービスの一部として自動的に更新されます。アンチウイルス・コンテンツのアップデートには、アンチウイルスとアンチスパイウェアのセキュリティ・プロファイルでそれぞれ使用される、アンチウイルス・シグネチャとDNS (C2)シグネチャが含まれています。アプリケーションおよび脅威コンテンツのアップデートには、脆弱性とアンチスパイウェアのセキュリティ・プロファイルでそれぞれ使用される、脆弱性シグネチャとアンチスパイウェア・シグネチャが含まれています。Palo Altoは、すべてのシグネチャ・カテゴリをタイプ(アンチウイルス、スパイウェア、脆弱性)別およびコンテンツのアップデート(アプリケーションおよび脅威、アンチウイルス)別にまとめ、各カテゴリのシグネチャを示した表を提供しています。詳細は、Palo Altoの「Threat Signature Categories」ドキュメントを参照してください。無料のPalo LIVEコミュニティ・アカウントを使用すると、Palo Altoの脅威ボールト(Palo Alto Networksの次世代ファイアウォールによる検知と防止が可能な、脆弱性、エクスプロイト、ウイルス、スパイウェアなどの最新の脅威を格納するデータベース)にアクセスできます。

各脅威シグネチャには、Palo Altoの脅威ボールトで定義されている内部的な重大度とデフォルト・アクションがあります。すべてのOCI Network Firewallにアンチウイルス、アンチスパイウェア、脆弱性保護の事前定義済セキュリティ・プロファイルが含まれており、侵入検知または侵入防止のセキュリティ・ポリシー・ルール・アクションにアタッチされています。セキュリティ・プロファイルは侵入セキュリティ・ポリシー・ルールと連係して、トラフィック・フローにウイルスやマルウェア、スパイウェア攻撃などの脅威がないかスキャンし、OCIのセキュリティ推奨事項に基づいてアクションを実行します。IPSを使用している場合のアクションは、重大度がクリティカル、中または高の脅威をブロックすることです。IDSを使用している場合は、OCI Network Firewallの脅威ログにアラートを送信するだけです。OCI Network Firewallには、ブロックされた脅威と検知された脅威の両方を確認するための脅威ログがあります。

侵入検知および防止システムは、セキュリティ・ルール・アクションが侵入検知または侵入防止として構成されている場合に、セキュリティ・ポリシーで有効化します。本書後出のOCIネットワーク・ポリシーの作成の概要の項で、侵入検知および防止も含め、ポリシーの作成について説明しています。侵入と検知の構成の詳細は、「Create a Security Rule」ドキュメントのセキュリティ・ルールの項を参照してください。

Secure Sockets Layer (SSL)検査

ファイアウォールでのSSL検査は、インバウンドとアウトバウンド両方の通信の暗号化されたトラフィックを復号および検査してセキュリティを強化する上で、重要な役割を果たします。ファイアウォールは、SSL証明書を使用することで、暗号化されたデータを捕捉および分析して、セキュア接続に隠れた潜在的な脅威を識別できます。インバウンド・トラフィックの場合、SSL検査により、内部サーバーへの着信リクエストが安全であることが保証されます。アウトバウンド・トラフィックの場合、内部ユーザーまたはアプリケーションによって開始された接続をモニタリングして保護できます。

SSLとその後継プロトコルであるTransport Layer Security (TLS)は、クライアントとサーバーの間のデータを暗号化することで通信を暗号化するために広く使用されています。悪意のあるアクターも、暗号化を利用して従来のセキュリティ対策から脅威を隠すことができます。OCI Network Firewallでは、インバウンドおよびアウトバウンドのSSL検査によってこの課題に対処しており、SSLトラフィックの復号、検査、再暗号化が可能です。このプロセスにより、暗号化された通信が組織のセキュリティにおける盲点とならないことを保証し、潜在的な脅威に対する可視性と保護を強化することができます。

インバウンドSSL検査とフォワード・プロキシSSL検査のどちらも、SSLで暗号化されたトラフィックに隠れた脅威を識別しながら、データの整合性とセキュリティを確保する上で、きわめて重要です。SSLインバウンド検査とフォワード・プロキシSSL検査の主な違いは、検査されるSSLトラフィックの方向と目的にあります。この項では、インバウンドSSL検査とフォワード・プロキシSSL検査の両方について詳しい概要を示し、信頼の確立、トラフィックの復号、検査および再暗号化をセキュアに行うプロセスについて説明します。

SSL検査がセキュリティを強化する仕組みを深く理解するには、インバウンドSSL検査とフォワード・プロキシSSL検査という2つの重要なコンテキストでSSL検査がどのように応用されているかを確認することが不可欠です。どちらのアプローチでも、暗号化されたトラフィックを処理する際の固有の課題に対処し、包括的な保護を確実に行うことができます。この機能に特化したOCI Network Firewallは、高度なSSL検査機能を使用して、暗号化されたトラフィックのシームレスな復号、検査、再暗号化を実現し、パフォーマンスやデータの整合性を損なうことなく堅牢なセキュリティを確保しています。この後の項では、これらの手法について掘り下げ、それぞれの役割とプロセス、およびネットワーク・インフラストラクチャにもたらすセキュリティ上の利点を明らかにします。

本書では、SSLという用語を使用して通信の暗号化という概念を表します。現在、セキュア接続を設定する際のプロトコルとしては、TLSの方が広く使用されています。

インバウンドSSL検査

SSLインバウンド検査とは、VCNに入ってインスタンスやロード・バランサなどのリソースに向かう、SSLで暗号化されたトラフィックの復号と検査を意味します。この検査は、有効なSSL証明書と秘密鍵を持つVCN内でホストされているリソースが所有するFQDNのトラフィックに適用されます。OCI Network Firewallでは、内部サーバーに向かうトラフィックを復号し、データに潜在的な脆弱性や脅威、マルウェアがないか検査してから、データを再暗号化して内部の宛先に送ることに重点を置いています。トラフィックを復号することで、ファイアウォールはセキュリティ・ポリシーを適用して、暗号化された接続であってもセキュリティ・リスクがないか十分に検査されることを保証できます。インバウンドSSL検査がクライアント、OCI Network Firewall、サーバーの間で機能するためには、OCI Network FirewallにサーバーとSSL証明書と秘密鍵がインストールされている必要があります。

次のシナリオは、SSLで暗号化された単純なWebアプリケーションをホストする典型的なOCI環境を表したものです。このアプリケーションは、パブリック・サブネットでホストされているFQDN `https://www.oracle.com`を通じて外部ユーザーに公開されます。ファイアウォールは、インターネット・ゲートウェイとパブリック・サブネットの間に位置し、インバウンド・トラフィックのセキュリティ・レイヤーの役割を果たしています。インバウンド・トラフィックは、セキュリティ検査のためにOCI Network Firewallを経由します。外部ユーザーがHTTPSリクエストを開始すると、OCI Network Firewallは暗号化されたトラフィックを復号して検査することで、インバウンドSSLを検査します。

このステップにより、悪意のあるコンテンツやセキュリティ上の脅威が内部OCI Webサーバーに到達する前に識別して軽減し、環境内でプライバシーとセキュリティの両方を確保することができます。

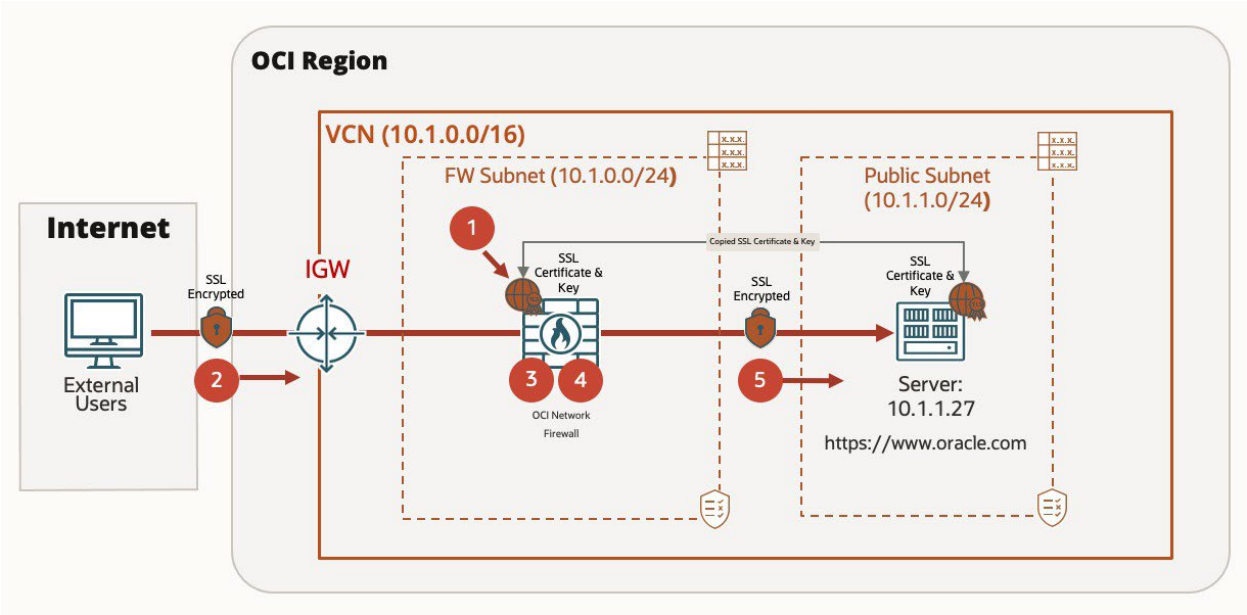

図1: インバウンドSSL検査のトポロジ

SSLインバウンド検査は、次のステップに従って行われます。

1. 管理者がOCI Vaultサービスを使用して、保護対象サーバーの証明書と秘密鍵のコピーをインポートします。
2. 外部クライアントがサーバーとのSSLセッションを開始し、内部OCIサイト(`https://www.oracle.com`)にリクエストを送信します。
3. トラフィックが、OCI Network Firewallで構成されている復号ポリシーに一致します。
4. OCI Network FirewallのSSL検査エンジンがSSLセッションを捕捉し、アップロードされた証明書と鍵のペアを使用してトラフィックを復号します。
5. 検査されたトラフィックがポリシーによって許可されると、トラフィックは再暗号化されて転送されます。

SSLハンドシェイクの一部である当初のSSLリクエストは、プロキシされずにWebサーバーに転送されます。リクエストは変更されません。SSLハンドシェイク中、OCI Network FirewallはServer Helloメッセージを検査して、Webサーバーによって提供された証明書がステップ1で使用した証明書と一致するかどうかを確認します。証明書が一致した場合、復号プロセスが開始され、セッションの残りの部分が正常に復号されます。証明書が一致しない場合、復号は失敗します。サーバーの戻りトラフィックは、サーバー・サブネットのルート表を使用して、OCI Network Firewall経由で送信されます。このルート表には、ルート・ルールとファイアウォールの次のホップが含まれています。

フォワード・プロキシSSL検査

SSLフォワード・プロキシ検査とは、VCN内のクライアントによって開始され、OCIの内部または外部にあるサーバーに向かう、暗号化されたトラフィックの復号を意味します。このプロセスにより、暗号化されたチャネルを介して悪意のあるコンテンツの送受信(データの流出やマルウェアのダウンロードなど)が行われないことを保証できます。OCI Network Firewallは、アウトバウンド・トラフィックに脅威がないか検査し、セキュリティ・ポリシーを施行してから、トラフィックを再暗号化して宛先に送ることができます。

従来のクライアント/サーバーSSLハンドシェイクとは異なり、SSLフォワード・プロキシ・モードでは、ファイアウォールはメディエータとして機能し、クライアントとサーバーの間の通信を捕捉します。ファイアウォールはクライアントからのSSL接続を終端し、サーバーへの新しい接続を確立します。サーバーにはファイアウォールがクライアントのように見え、クライアントにはファイアウォールがサーバーのように見えます。

ファイアウォールがメディエータ・モードで機能するためには、インバウンドSSL検査のユース・ケースで使用した証明書とは異なる証明書が必要です。この証明書は、ファイアウォールがクライアントへの提示に使用できる、認証局によって発行されたCA証明書か、ファイアウォールにインポートされた自己署名証明書です。クライアントは、サーバーの証明書を信頼して、ブラウザの警告やエラーを回避する必要があります。

次のシナリオは、典型的なOCI環境を表したものです。外部Webサイトにアクセスする内部ユーザーから発生したトラフィックを保護するように、フォワード・プロキシSSL検査が構成されています。サブネット内のユーザーが外部サイト(`https://www.oracle.com`など)にアクセスしようとすると、トラフィックはまず、プロキシの役割を果たすOCI Network Firewallを経由します。ファイアウォールはSSLトラフィックを捕捉して復号し、マルウェアやデータ流出などの潜在的な脅威がないかトラフィックの内容を検査します。検査が完了すると、ファイアウォールはトラフィックを再暗号化して、目的の宛先に転送します。このステップにより、OCI環境を離れる機微データをモニタリングしてコンプライアンスとセキュリティを維持しながら、転送中の暗号化を通じてプライバシーを確保することができます。

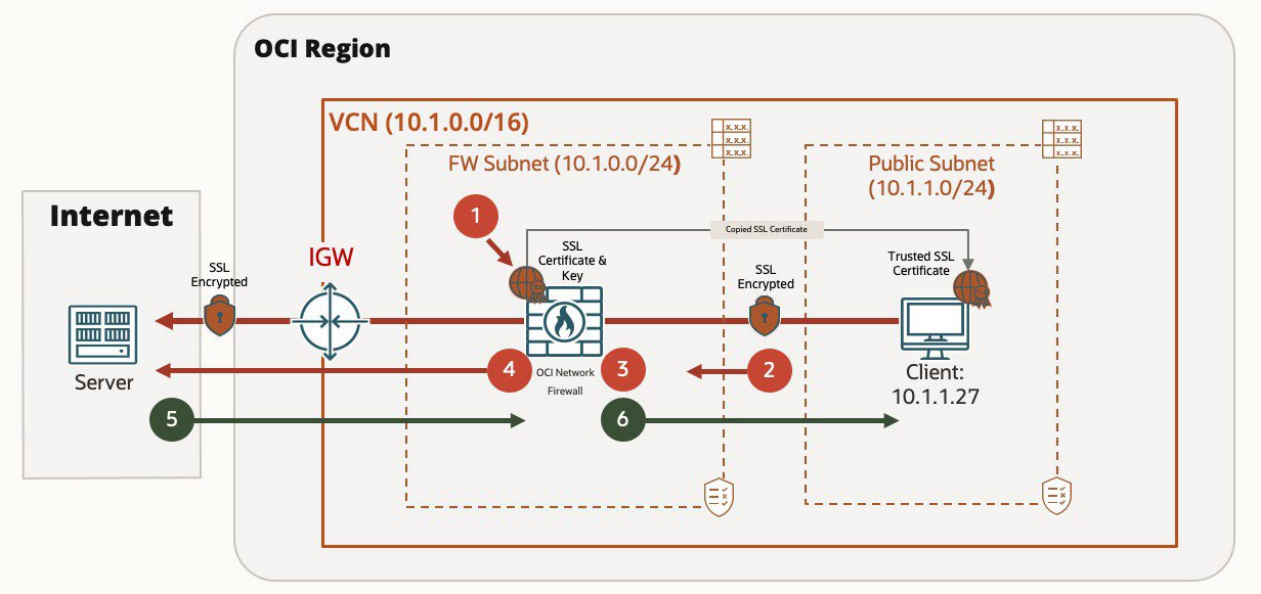

図2: フォワード・プロキシSSL検査のトポロジ

SSLフォワード・プロキシ検査は、次のステップに従って行われます。

1. 管理者がOCI Vaultサービスを使用して、認証局によって発行された証明書または自己署名証明書と秘密鍵のコピーをインポートします。
2. クライアントがサーバーとのSSLセッションを開始し、`https://www.oracle.com`にリクエストを送信します。トラフィックが、OCI Network Firewallで構成されているフォワード・プロキシSSLの復号ポリシーに一致します。
3. ファイアウォールのSSLProxyEngineがトラフィックを捕捉し、内部公開鍵インフラストラクチャ(PKI)とCA証明書によって署名された証明書を使用して、`www.oracle.com`の証明書を生成します。クライアントにはファイアウォールが外部サーバーのように見えますが、セキュア・セッションは、本物のサーバーではなく、ファイアウォールとの間に確立されます。
4. ファイアウォールがクライアントのSSL証明書リクエストをサーバーに送信し、別のセッションを開始します。サーバーからはファイアウォールがクライアントのように見えるため、サーバーはメディエータを意識せずに証明書の確認に進みます。
5. サーバーが署名付き証明書をクライアント向けのOCI Network Firewallに送信します。
6. ファイアウォールがサーバーの証明書を分析します。サーバーの証明書が、構成されているポリシーとプロファイルに適合すると、ファイアウォールがサーバーの証明書のSSLコピーを生成してクライアントに送信します。

SSL証明書

OCI Network Firewallは、インバウンドとフォワード両方のSSL検査用のSSL証明書をセキュアに格納および管理するために、OCI Vaultサービスとシームレスに統合されています。ネットワーク・ファイアウォールでSSL証明書を利用する場合、OCI Vaultサービスは提供された証明書を検証して信頼のルートに格納し、トラフィックの復号中にセキュアに使用できるようにします。検証を成功させるには、すべての中間証明書、ルート証明書、秘密鍵を含む、完全なSSL証明書チェーンを指定します。証明書は、事前定義済のJSONテンプレート内にラップして、.pem形式でアップロードする必要があります。オラクルは、SSL証明書チェーンを生成して適切な形式に変換するスクリプトを作成しました。これは、公式のOracle GitHubリポジトリからダウンロードできます。次のブロックは、JSON形式のSSL証明書チェーンの例です。

```
{
"caCertOrderedList" :
    [ "ROOT_CERT01_PEM_CONTENT",
    "INTERMEDIATE_CERT01_PEM_CONTENT",
    "INTERMEDIATE_CERT02_PEM_CONTENT",
 ],

"certKeyPair": {
    "cert" : "LEAF_CERT_01_PEM_CONTENT",
    "key": "PRIVATE_KEY_01_PEM_CONTENT"
 }
}
```

OCI Network FirewallでのSSL復号のすべてのユース・ケースに、証明書と属性に関連した特定の要件があります。

インバウンドSSL検査のSSL証明書

SSLインバウンド検査の場合、certKeyPairにパブリック証明書と秘密鍵が必要です。この場合、認証局(CA)フラグをtrueに設定する必要はありません。

証明書のCAフラグを確認するには、次のOpenSSLコマンドを使用して、SSLインバウンド検査の証明書を確認します。

```
 openssl x509 -in ssl-inb.pem -noout -text | grep -E -A 1 "Issuer:|Subject:|Basic
Constraints|Netscape Cert Type|X509v3 Key Usage"

         Subject Public Key Info:
--
            X509v3 Basic Constraints:
                CA:FALSE
          Netscape Cert Type:
                SSL Server
--
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
```

このコマンドには次のパラメータがあります。

- **Basic Constraints**: CA:FALSEは、証明書が他の証明書を発行できないことを示します。この特性は、リーフ証明書の鍵となります。
- **Netscape Cert Type**: “SSL Server”は、証明書がSSLサーバーとして使用するためのものであることを示します。通常はこれがリーフ証明書の役割です。
- **X509v3 Key Usage**: このセクションには、Digital Signature , Key Encipherment と表示されます。セキュア通信用のSSLで使用されるリーフ証明書の場合は、これが標準です。

フォワード・プロキシSSL検査の証明書

SSLフォワード・プロキシSSL検査の場合、certKeyPairにパブリック証明書と秘密鍵が必要ですが、CAフラグをtrueに設定して、ファイアウォールが証明書を偽装してアウトバウンド・トラフィックを復号できるようになります。証明書のCAフラグを確認するには、次のOpenSSLコマンドを使用して、フォワード・プロキシSSL検査の証明書を確認します。

```
 openssl x509 -in ssl-fwd.pem -noout -text | grep -E -A 1 "Issuer:|Subject:|Basic
Constraints|Netscape Cert Type|X509v3 Key Usage"

        Subject Public Key Info:
--
            X509v3 Basic Constraints: critical CA:TRUE,
                pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

このコマンドには次のパラメータがあります。

- **Basic Constraints**: CA:TRUEは、この証明書がCAの役割を果たし、他の証明書を発行できることを意味します。pathlen:0は、発行できるのはリーフ証明書のみで、他の中間証明書は発行できないことを示します。これは、中間証明書の典型的な設定です。
- **X509v3 Key Usage**: Certificate Signが含まれます。これは、他の証明書に署名する証明書に必要であり、この証明書が中間証明書であることを示すもう1つの要素です。

このプロセスにより、証明書がOCI Network FirewallでのSSL検査のユース・ケースをサポートするように正しく構成されていることを保証できます。

高可用性

機能の概要で取り上げる最後のトピックは高可用性です。高可用性は、クラウド・サービスが連続稼働を実現し、ダウンタイムを最小限に抑え、データ損失を削減し、ビジネス継続性を維持するために不可欠です。OCI Network Firewallサービスの高可用性は、サービスに組み込まれた暗黙的な機能です。OCI Network Firewallは、本質的に可用性が高く、水平方向のスケーラビリティとフォルトトレランスに優れているため、ロード・バランサなどのインフラストラクチャや複雑な構成を追加して高可用性を手動で構成する必要はありません。OCIネットワーク・ファイアウォールを導入する際には、デプロイメントの範囲を2つのオプションから選択できます。複数の可用性ドメインにまたがるリージョナル・デプロイメントと、1つの可用性ドメイン内で複数のフォルト・ドメインにまたがるデプロイメントです。クリティカルなアプリケーションに推奨されるデフォルト・オプションはリージョナルであり、1つ以上の可用性ドメインで障害が発生しても継続的な保護を保証します。
可用性ドメイン専用のデプロイメントは、1つの可用性ドメイン内で1つ以上のフォルト・ドメインにまたがる冗長性を提供し、高可用性と低レイテンシの組合せを必要とするアプリケーションに有効です。この利点は、インフラストラクチャや複雑な構成を追加せずに得ることができます。

高可用性の構成は、「ネットワーク・ファイアウォールの作成」ワークフローの「拡張オプション」セクションで確認できます。高可用性の構成の詳細は、「Create a Firewall」ドキュメントのファイアウォールの作成の項を参照してください。

次の項では、以上の知識を基に、効果的なネットワーク・ポリシーを設計して実装し、OCI Network Firewallの堅牢な機能セットの価値を最大化する方法を見ていきます。このように進めることで、ツールを理解する段階から、ツールを応用してセキュリティとトラフィックを実際に管理する段階へとシームレスに移行できます。

OCIネットワーク・ポリシーの作成とファイアウォールの概要

ネットワーク・ポリシーは効果的なセキュリティ戦略の基盤であり、ネットワーク・ポリシーを使用すると、体系的かつ予測可能な方法でワークロードを保護し、コンプライアンスを徹底し、トラフィックのフローを制御することができます。正規のトラフィックのみがネットワークを移動することを保証しながら、潜在的に悪意のある活動や不正な活動をブロックするには、ポリシーが不可欠です。
データの取り扱いとアクセスについて明確で施行可能なルールを定義して規制要件に対応するためにも、ポリシーは重要です。

正しく作成されたポリシーは、ルール(トラフィックを許可または拒否するための特定の条件)、条件(IPアドレス、サービス、アプリケーション、URLなどの基準)、アクション(許可やブロックなど、トラフィックとルールとの照合の結果)などの主要コンポーネントで構成されます。これらの要素が連係して、ネットワーク・トラフィックのきめ細かな制御を実現します。

このような体系的アプローチでポリシーを作成することにより、セキュリティ・ルールは実行可能なだけでなく、ファイアウォールの機能に即したものとなります。まずポリシーとそのコンポーネントの重要性を理解することで、セキュアでコンプライアスに優れ、管理の行き届いたクラウド環境を効果的に実現できます。ポリシー・モデルの転換とパフォーマンスにおけるOCI Network Firewallのスケール、制限、最近の向上点の詳細は、ブログ記事「OCI Network Firewall: Unveiling Policy Model Transformations and Performance Advances」を参照してください。

この項では、ポリシー作成の基本を順に確認した後、実際のアプリケーションを例に取り、ポリシーがどのようにネットワーク・トラフィック・フローを保護し、最適化するかを説明します。

アプリケーション

OCI Network Firewallのアプリケーションは、レイヤー7検査を使用し、ポートやIPアドレスのみに頼るのではなく、アプリケーションの動作とプロトコルに基づいてトラフィックを識別および分類することで、高度なトラフィック制御を可能にします。この機能は、最新のネットワーク環境の正確な制御と強力なセキュリティを実現します。

ファイアウォールは、トラフィックのパターンと動作を分析することで、アプリケーションを識別します。アプリケーションは、そのアプリケーションに関連付けられた特定のプロトコルと動作を表す、一意のシグネチャによって定義されます。ポートベースのフィルタリングとは異なり、アプリケーションは固有のプロパティによって認識されるため、検知の精度が向上します。このアプローチにより、ファイアウォールで次のことが可能になります。

- レイヤー7検査を実行し、アプリケーション・レイヤーでトラフィックを分析する。
- 複数のアプリケーションが同じポートまたはプロトコルを共有する場合でも、アプリケーションを正確に検知し、分析する。

アプリケーションは、次のパラメータによって特徴付けられます。

- **名前**: サービスの一意の識別子。
- **プロトコル**: ICMPまたはICMPv6
- **ICMPタイプ:** 0-Echo reply、3-Destination unreachable、5-Redirect、8-Echo。
- **ICMPコード:** ICMPを選択した場合に使用します。0-Net unreachable、1-Host unreachable、2-Protocol unreachable、3-Port unreachable

アプリケーションは、アプリケーション・リストに整理されます。アプリケーション・リストとは、ファイアウォール・ポリシー・ルールに含まれる、定義済アプリケーションのコレクションです。このリストを使用すると、アプリケーション自体に基づいてネットワーク・トラフィックを正確に制御できます。

OCI Network Firewallのアプリケーションは、従来のポートとプロトコルによるフィルタリングを超える、動作に基づいたきめ細かなトラフィック制御を可能にします。レイヤー7検査を使用して、正確で適応性に優れたセキュアなネットワーク・トラフィック管理を実現するアプリケーションは、アプリケーション主導の最新クラウド環境に不可欠なものとなっています。

現在、OCI Network FirewallはICMPとICMPv6のアプリケーションをサポートしており、他のタイプも追加される予定です。アプリケーションの最新の強化点については、OCI Network Firewallのドキュメントを参照してください。

サービス

OCI Network Firewallのサービスは、特定のネットワーク・プロトコルまたはアプリケーションを、それらに関連付けられたレイヤー4ポートによって定義します。サービスは特定のネットワーク・プロトコルまたはアプリケーションを表し、次の要素によって特徴付けられます。

- **名前**: サービスの一意の識別子。
- **プロトコル**: TCPまたはUDP。
- **ポート**: 1433などの特定のポート番号、または80-8080などの範囲で定義します。

各サービスに最大10のポート範囲を含めることができるため、複数のポートを使用するアプリケーションを柔軟に表現できます。サービスは、個別に作成することも、JSONファイルを使用して一括でインポートすることも可能なので、複雑な構成の設定が合理化されます。このモジュール式アプローチにより、ポリシー内の類似のルール間で定義を再利用できるため、管理が簡素化されます。

作成されたサービスは、サービス・リストに整理されます。サービス・リストは、同じファイアウォール・ポリシーに含まれるサービスのコレクションの役割を果たします。このリストは、次のアクションのためにポリシー・ルールで参照されます。

- 特定のトラフィックを許可または拒否する。
- 組織のセキュリティ要件へのコンプライアンスを確保する。
- ファイアウォール・ルールの読みやすさと再利用のしやすさを高める。

ポート443を使用したWeb-Servicesというサービスをルールに含めて、HTTPSトラフィックを許可することができます。別のアプリケーションで類似のルールが必要な場合は、同じサービス・リストを再利用して一貫性を維持できます。

OCI Network Firewallのサービスは、レイヤー4のプロトコルとポートの構成を再利用可能なエンティティに抽象化することで、効率的なトラフィック制御を可能にします。サービスはファイアウォール・ポリシーに統合されているため、管理性の向上とセキュリティの強化が実現し、動的なクラウド環境のスケーラビリティが保証されます。

JSONファイルを使用して複数のアプリケーションまたはサービスをインポートする方法については、「Bulk Import Firewall Policy Components」を参照してください。

リスト

リストとは、セキュリティ・ルールで使用するアドレス、アプリケーション、サービスまたはURLをグループ化できる、OCI Network Firewallポリシーの再利用可能なコンポーネントです。リスト内の項目をルールで適用する際には、すべての項目が同様に扱われます。たとえば、既知の悪意のあるWebサイトをブロックするには、「悪意のあるURL」というURLリストを作成し、リスト全体へのアクセスを同時に拒否するルールを適用します。

OCIファイアウォールは、IPアドレス・リストやアプリケーション・リストなど、様々なタイプのリストをサポートしています。効果的なトラフィック管理とセキュリティには、次のタイプのリストを使用します。

- **IPアドレス・リスト**: IPアドレス・リストは、ファイアウォール・ポリシー・ルールの作成時に使用するIPv4アドレスとIPv6アドレスのリストを作成するために使用します。IPアドレス・リストには、個々のIPv4アドレスまたはIPv6アドレス、CIDRブロック、あるいはその両方の組合せを含めることができます。
- **アプリケーション・リスト**: アプリケーション・リストは、作成したアプリケーションを選択してグループ化するために使用します。アプリケーション・リストを作成し、アプリケーションのグループのトラフィックを制御(許可またはブロック)します。
- **サービス・リスト**: サービス・リストは、サービス・リストに含めるサービスを選択してグループ化するために使用します。ファイアウォール・ポリシーのルールの作成に使用できるサービスのリストを作成します。サービス・リストを使用すると、サービスのグループのトラフィックを許可またはブロックできます。各サービスはポートベースのシグネチャによって識別され、レイヤー4検査がサービスの照合に使用されます。

URLリスト

URLフィルタリングは、管理者がWebサイトへのアクセスをURLに基づいて制御およびモニタリングできる、重要なセキュリティ機能です。この機能を使用すると、特定のWebトラフィックをブロックまたは許可するポリシーを施行でき、セキュリティの強化と内部ガイドラインへのコンプライアンスの確保が可能になります。OCIファイアウォールでは、URLリストはURLを整理して管理するためのツールの役割を果たします。これにより、フィルタリング・プロセスが合理化され、フィルタリング・プロセスの効率性とスケーラビリティも向上します。次の項では、URLリストを構成および適用してURLフィルタリングを微調整し、Webトラフィックの制御を強化する方法について概説します。

管理者は、特定のURLのグループへのアクセスを許可または拒否するURLリストを設定できます。このリストを構成するには、各URLを別々の行に入力します。アスタリスク(*)やカレット(^)などのワイルドカードを使用して、照合をカスタマイズすることもできます。URLを指定する際には、“http://”や“https://”などのプロトコル情報は省略します。

URLフィルタリングでワイルドカード照合を使用すると、管理者は、特定のFQDNへのトラフィックをブロックまたは許可する幅広いルールを柔軟に作成できます。その際に、ドメインのあらゆるバリエーションを考慮する必要はありません。このアプローチにより、大規模、動的あるいは予測不能なドメイン構造を扱う場合は特に、フィルタリング・ポリシーの管理が簡素化されます。

URLのホスト名の部分では、アルファベットおよび数字と、ピリオド、アンダースコア、チルダ(~)、各種句読点のような特殊記号など、特定の文字がサポートされます。これらの文字は、正確にフィルタリングできるように、有効なURL要素を形成するために使用します。

ピリオド、スラッシュ、疑問符、アンパサンド、等号、セミコロン、プラス記号などの特定の文字は、URL内のトークン・セパレータとして機能します。トークン・セパレータを使用すると、URLのセグメントを個別に定義できるため、パーサーがURL構造の各部分を効果的に解釈して管理するのが容易になります。

- **アスタリスク**: アスタリスク記号(*)は、任意の数の文字(文字なしを含む)を表します。ドメイン、サブドメインまたはパスの全体に一致させる場合に使用できます。
- **カレット**: カレット記号(^)は、1レベルのサブドメインのみに一致する機能を持ちます。

次の例は、ワイルドカード・フィルタの様々な組合せが、現在の所定の動作に従い、どのようにWebサイトに一致するか、一致しないかを示します。

- ***.oracle.com**: blog1.blog2.oracle.com.au.usに一致し、blog1.oracle.comに一致します。/文字がない場合、末尾に暗黙的な*があることになります。
- **^.oracle.com/**: blog.oracle.comに一致し、oracle.comとother.blog.oracle.comには一致しません。
- **oracle.^:** 右側のどのWebサイトにも一致します。oracle.com、oracle.com.au、oracle.com.au.usに一致します。
- **oracle.^.au/**: oracle.com.auとoracle.uk.auのみに一致し、oracle.comとoracle.com.au.website.infoには一致しません。
- ***.oracle.com/**: blog1.blog2.oracle.comに一致し、oracle.comとblog.oracle.com.auには一致しません。
- ***.oracle.com.***: blog1.blog2.oracle.com.au.usに一致し、blog1.oracle.comには一致しません。
- **oracle.com**: oracle.com.au、oracle.com.au.website、oracle.comに一致します。
- **oracle.com/**: oracle.comのみに一致します。

サブページは、特定のURLに対して復号が有効になっている場合にのみ、フィルタで照合できます。復号を使用しない場合、URLフィルタリングは、xyz.comへのトラフィックをすべてブロックまたは許可するなど、ドメインレベルの大まかなルールに限定されます。次の例について考えてみましょう。

- **oracle.com/***: oracle.com/word1とoracle.com/word2に一致します。
- **oracle.com/word.**: oracle.com/wordのみに一致します。

JSONファイルを使用して複数のサービス・リストとURLリストをインポートする方法については、「Bulk Import Firewall Policy Components」を参照してください。

ルール

ルールは、OCI Network Firewallの機能の要であり、ネットワーク・トラフィックの管理、検査、保護の方法を定義します。ルールを使用すると、トラフィック・フローを正確に制御し、正規のデータのみがネットワークを移動する一方で、潜在的な脅威や不正なアクセスの試みはブロックされることを保証できます。

トラフィックがルールに一致すると、OCI Network Firewallは、ルールのパラメータに基づいて、指定されたアクション(セッションの許可、ブロック、検査など)を実行します。セキュリティ・ルールには次の利点があります。

- **可視性の向上**: 詳細なパラメータに基づいてトラフィックを検査することで、管理者はネットワーク・アクティビティに関する深い洞察を得ます。
- **きめ細かな制御**: ルールによって特定のトラフィック・フローを正確に管理でき、不正なアクセスのリスクが軽減します。
- **カスタマイズ可能なポリシー**: セキュリティ要件に合わせてルールをカスタマイズし、コンプライアンスと効率性の両方を確保できます。

OCI Network Firewallは、次の種類の主要セキュリティ・ルールをサポートしており、各ルールが異なる目的を果たします。

- **復号ルール:** 復号ルールは、暗号化されたトラフィックの管理に不可欠です。復号ルールを使用することで、ファイアウォールはSSL/TLS通信を復号して、脅威やポリシー違反がないか検査できます。この機能は、悪意のある活動を隠すために使用されることの多いセキュア通信に対する可視性を高めます。復号ルールにより、管理者は、SSLのインバウンド・トラフィックまたはフォワード・プロキシ・トラフィックを検査し、セキュア通信が組織のポリシーに準拠していることを保証しながら、機微データを保護することができます。証明書の認証を設定し、マップされたシークレット、復号プロファイル、復号ルールを作成する手順については、「Create a Decryption Rule」ドキュメントを参照してください。
- **セキュリティ・ルール:** セキュリティ・ルールは、トラフィックを許可、ブロックまたは検査する、核となるアクセス制御ポリシーを定義します。このルールは、IPアドレス、ポート、プロトコル、URLなどのパラメータに基づいています。セキュリティ・ルールを作成する前に、アプリケーション・リスト、サービス・リスト、アドレス・リスト、URLリストなどの主要コンポーネントを設定する必要があります。セキュリティ・ルールが管理する特定のエンティティをこれらのリストで分類することにより、詳細で効率的なポリシー構成が可能になります。
- **トンネル検査ルール**: トンネル検査ルールは、VXLANでカプセル化された平文トンネルにおけるトラフィックの分析用に特別に設計されています。このルールにより、カプセル化されたデータに対してセキュリティ・ポリシーを施行して、コンプライアンスを確保するとともに、トンネル・トラフィックに隠れた潜在的な脅威を検知することができます。このユース・ケースの詳細は、ブログ記事「Announcing tunnel inspection for OCI Network Firewall」を参照してください。

これらのルールのタイプを理解し、実装することで、ネットワークのセキュリティを効果的に管理し、トラフィック・フローをポリシーに準拠させながら、高い可視性と脅威からの堅牢な保護を維持することができます。復号ルール、セキュリティ・ルール、トンネル検査ルールの詳しい構成手順については、「Firewall Policy Rules」ドキュメントを参照してください。

ルールの処理順序

OCI Network Firewallのトラフィック評価は、複数のレイヤーからなるプロセスです。OCIネットワーク・ファイアウォールは、3種類の主要セキュリティ・ルール(復号、セキュリティ、トンネル検査)を使用した体系的な処理順序に従って、トラフィックを処理します。

この評価は、トラフィックが次の検査レイヤーを進むにつれて、複数の段階で行われます。

1. セッションの設定とセッション前の施行の段階で、ファイアウォールはまず、レイヤー3とレイヤー4の条件を既存のセキュリティ・ルールに対して評価します。これにより、5タプル(ソースと宛先のIP、ソースと宛先のポート、プロトコル)に基づいてアクションをチェックし、既知の脅威をすばやく阻止して、それ以上の不要な処理(既知のIPのブロックなど)を回避します。
2. トラフィックがアプリケーションIDとコンテンツIDの検査を受け、アプリケーションのタイプとコンテンツがそれぞれ特定されます。
3. アプリケーションがSSLベースの場合、ファイアウォールは、復号ルールが定義されているかどうかをチェックし、必要なアクションを実行してから、トラフィックを再評価してアプリケーションIDとコンテンツIDの検査を行います。
4. ファイアウォールは、既存のセキュリティ・ルールに対してトラフィックを再評価します。
5. アプリケーションがVXLANトンネルの場合、ファイアウォールは、トンネル検査ルールを適用して、トラフィックをさらに評価します。一致するトンネル検査ルールが存在する場合、ファイアウォールは、内部パケットを検査し、既存のセキュリティ・ルールに対してトラフィックを評価します。

ルールの処理方法に関する次の重要な詳細事項を考慮してください。

- ルールはオプションですが、ファイアウォールで使用するポリシーにルールが少なくとも1つ指定されていないと、ファイアウォールはすべてのネットワーク・トラフィックを拒否します。
- ルールの評価は順番に行われます。つまり、ファイアウォールはルールを上から下へ処理します。このアプローチにより、最も限定的なルールが最初に適用されます。つまり、ルールが一致すると、他のルールはそれ以上評価されません。デフォルトでは、新しく作成したルールはそれぞれ優先順位リスト(上から下の順)の先頭に来ます。優先順位はいつでも変更できます。
- トンネル検査ルールを復号ルールと組み合せることはできません。

マップされたシークレットと復号プロファイル

OCI Network Firewallを使用したSSL復号を実装する際には、セキュアで効果的なトラフィック検査を保証する上で、マップされたシークレットと復号プロファイルが重要な役割を果たします。SSL復号により、ファイアウォールは、暗号化されたトラフィックに潜在的な脅威やポリシー違反がないか分析できます。悪意のある活動が暗号化された接続に隠れていることの多い今日のセキュリティ環境において、この機能は不可欠です。

マップされたシークレットは、SSL復号の主要コンポーネントです。OCI Vaultサービスで作成および管理されるこのシークレットは、インバウンドまたはフォワード・プロキシの復号に必要なSSL鍵にリンクしています。マップされたシークレットにより、ファイアウォールはこの鍵にセキュアにアクセスできるため、アウトバウンド・トラフィックのSSLフォワード・プロキシや着信トラフィックのSSLインバウンド検査などのシナリオで、暗号化されたトラフィックの復号と検査が可能になります。このシークレットを適切に構成することで、ファイアウォールは、機微データの整合性を損なうことなく、トラフィックをセキュアに復号できるようになります。

復号プロファイルは、SSL復号の実行方法を定義し、トラフィックが通過を許可される前にSSLセッションが満たす必要のあるセキュリティ基準を施行します。このプロファイルは、クリティカルなチェックを処理します。次に例を示します。

- **証明書の有効性**: SSL証明書が有効であり、信頼できる認証局によって発行されたことを保証します。
- **セッションの構成**: SSLセッション・パラメータが組織のセキュリティ・ポリシーに準拠していることを確認します。
- **失敗時のアクション**: 証明書の検証に失敗した場合のアクション(接続のブロック、管理者へのアラート送信など)を指定します。

復号プロファイルを使用することで、管理者は、厳密なセキュリティ基準を施行し、セキュアでない、あるいは基準を満たしていないSSL接続をブロックして、ネットワークに脆弱性が生じるのを防止できます。この精度の高さで、セキュリティ全般を強化しながら、正規のトラフィック・フローのみを許可することができます。SSLフォワード・プロキシ復号プロファイルとSSLインバウンド復号プロファイルの構成に使用できるオプションの詳しい概要は、「Firewall Policy Rules」ドキュメントの「Mapped Secrets and Decryption Profiles」の項を参照してください。

ポリシー作成例

この項では、前出のポリシー作成のトピックについてさらに詳しく説明し、Terraform OCIプロバイダを使用してHTTPSトラフィックを検査するネットワーク・ファイアウォール・ポリシーを作成する方法を示します。この架空のユース・ケースでは、従業員は、HTTPS経由でアクセスするクラウドベースの生産性およびコラボレーション・アプリケーションを利用しています。HTTPSは、暗号化された通信を保証する一方で、次のような脅威を隠すこともできます。

- フィッシング行為
- マルウェアの配布
- 不正なデータ流出

これらのリスクに対処するには、HTTPSトラフィックを復号して検査するようにポリシーを構成し、アプリケーションへの正規の安全なアクセスのみを保証します。

Terraform構成で、IPアドレス・リスト、URLリスト、サービスとサービス・リスト、復号プロファイル、HTTPSトラフィックのルールなど、ポリシーを作成するためのリソースを定義します。最後に、HTTPSトラフィックを検査するセキュリティ・ルールを構成し、正規のアクセスのみを許可します。このポリシー例は、Webアプリケーションを脅威から保護しながら、組織のセキュリティ基準を維持するためのベースラインとなります。

次のコード・ブロックは、簡略化したTerraform構成を示しています。

```
resource "oci_network_firewall_network_firewall_policy" "EXAMPLE-POLICY" { #Required
    compartment_id = var.compartment_id

    #Optional
    display_name = "EXAMPLE-POLICY"
}

resource "oci_network_firewall_network_firewall_policy_address_list" "CLIENT-IP-ADDRESS-LIST"
    { #Required
    name = "CLIENT-IPS"
    network_firewall_policy_id = oci_network_firewall_network_firewall_policy.EXAMPLE-POLICY.id
    type = var.network_firewall_policy_address_list_type

    #Optional
    addresses = ["10.0.0.0/8"]
}

resource "oci_network_firewall_network_firewall_policy_address_list" "APP-IP-ADDRESS-LIST"
    { #Required
    name = "APP-IPS"
    network_firewall_policy_id = oci_network_firewall_network_firewall_policy.EXAMPLE-POLICY.id
    type = var.network_firewall_policy_address_list_type

    #Optional
    addresses = ["192.168.0.0/16"]
}
```

```
resource "oci_network_firewall_network_firewall_policy_service" "HTTPS-SERVICE"
    { #Required
    name = "HTTPS-SERVICE"
    network_firewall_policy_id = oci_network_firewall_network_firewall_policy.EXAMPLE-POLICY.id
    port_ranges {
        #Required
        minimum_port = "443"
        #Optional
        maximum_port = "443"
    }
    type = "TCP_SERVICE"
}

resource "oci_network_firewall_network_firewall_policy_service_list" "HTTPS-SERVICE-LIST"
    { #Required
    name = HTTPS-SERVICE-LIST
    network_firewall_policy_id = oci_network_firewall_network_firewall_policy.EXAMPLE-POLICY.id.id
    services = ["HTTPS-SERVICE"]
}

resource "oci_network_firewall_network_firewall_policy_url_list" "URL-LIST" { #Required
    name = "URL-LIST"
    network_firewall_policy_id = oci_network_firewall_network_firewall_policy.EXAMPLE-POLICY.id
    urls {
        #Required
        pattern = "www.oracle.com"
        type = "SIMPLE"
    }
}

resource "oci_network_firewall_network_firewall_policy_mapped_secret" "SSL-MAPPED-SECRET"
    { #Required
    name = "SSL-MAPPED-SECRET"
    network_firewall_policy_id = oci_network_firewall_network_firewall_policy.EXAMPLE-POLICY.id
    source = "OCI_VAULT"
    type = "SSL_INBOUND_INSPECTION"
    vault_secret_id = oci_vault_secret.test_secret.id
    version_number = "1"
}

resource "oci_network_firewall_network_firewall_policy_decryption_rule" "SSL-DECRYPTION-RULE"
    { #Required
       name = "SSL-DECRYPT-RULE"
       action = "DECRYPT"
    condition {
        destination_address = []
        source_address = []
    }
    position {
        #Optional
        after_rule = []
        before_rule = []
    }
    network_firewall_policy_id = oci_network_firewall_network_firewall_policy.EXAMPLE-POLICY.id
```

```
    #Optional
       decryption_profile =
oci_network_firewall_network_firewall_policy_decryption_profile.DECRYPTION-PROFILE.name
       secret = oci_network_firewall_network_firewall_policy_mapped_secret.SSL-MAPPED-SECRET.name
}

resource "oci_network_firewall_network_firewall_policy_decryption_profile" "DECRYPTION-PROFILE"
    { #Required
    name = "DECRYPTION-PROFILE"
    network_firewall_policy_id = oci_network_firewall_network_firewall_policy.EXAMPLE-POLICY.id
    type = "SSL_INBOUND_INSPECTION"

    #Optional
    are_certificate_extensions_restricted =
var.network_firewall_policy_decryption_profile_are_certificate_extensions_restricted
    is_auto_include_alt_name =
var.network_firewall_policy_decryption_profile_is_auto_include_alt_name
    is_expired_certificate_blocked =
var.network_firewall_policy_decryption_profile_is_expired_certificate_blocked
    is_out_of_capacity_blocked =
var.network_firewall_policy_decryption_profile_is_out_of_capacity_blocked
    is_revocation_status_timeout_blocked =
var.network_firewall_policy_decryption_profile_is_revocation_status_timeout_blocked
    is_unknown_revocation_status_blocked =
var.network_firewall_policy_decryption_profile_is_unknown_revocation_status_blocked
    is_unsupported_cipher_blocked =
var.network_firewall_policy_decryption_profile_is_unsupported_cipher_blocked
    is_unsupported_version_blocked =
var.network_firewall_policy_decryption_profile_is_unsupported_version_blocked
    is_untrusted_issuer_blocked =
var.network_firewall_policy_decryption_profile_is_untrusted_issuer_blocked
}

resource "oci_network_firewall_network_firewall_policy_security_rule" "SECURITY-RULE"
    { #Required
    action = "INSPECT" name
    = "SECURITY-RULE"
    condition {
        application = []
        destination_address = ["APP-IP-ADDRESS-LIST"]
        service = ["HTTPS-SERVICE-LIST"]
        source_address = ["CLIENT-IP-ADDRESS-LIST"]
        url = ["URL-LIST"]
    }
    network_firewall_policy_id = oci_network_firewall_network_firewall_policy.EXAMPLE-POLICY.id

    #Optional
    inspection = "NTRUSION_PREVENTION"
    position {

        #Optional
        after_rule = var.network_firewall_policy_security_rule_position_after_rule
        before_rule = var.network_firewall_policy_security_rule_position_before_rule
    }
}
```

ファイアウォールを作成するには、関連付けられたファイアウォール・ポリシーが少なくとも1つ必要です。ファイアウォールはそれぞれ1つのファイアウォール・ポリシーにリンクされますが、1つのファイアウォール・ポリシーを複数のファイアウォールに関連付けることができます。ファイアウォールを作成し、そのファイアウォールにポリシーを関連付ける詳しい手順については、「Overview of Creating a Firewall」ドキュメントを参照してください。

OCIネットワーク・ファイアウォール挿入シナリオのルーティング・ユース・ケース

OCIでは、OCI Network Firewallサービスの統合は、VCN内のセキュリティとトラフィックの管理を強化する上できわめて重要です。ファイアウォール挿入により、ネットワーク・セキュリティをクラウド・アーキテクチャにシームレスに統合して、事前定義済のセキュリティ・ポリシーに従って着信と発信両方のトラフィックをすべて検査し、フィルタリングすることができます。このプロセスは、OCI Network Firewallとの間でトラフィックを送信する特定のルーティング構成を使用することで容易になります。

VCNがネットワーク・ファイアウォールを使用するように構成されている場合、トラフィック・フローがファイアウォール経由で宛先に到達するように、ルーティング表を慎重に設計する必要があります。このプロセスでは、ファイアウォールを特定のトラフィック・フローの次のホップとして指し示すルート・ルールを構成します。これにより、セキュリティ・ポリシーの検査、ロギング、適用が可能になります。ファイアウォールをルーティング・パスに戦略的に挿入することで、クラウド環境のモニタリングと制御を効果的に行い、幅広いサイバー脅威から保護しながら、高い可用性とパフォーマンス基準を維持することができます。

この項では、OCIにおけるファイアウォール挿入の様々なシナリオについて説明し、効果的なトラフィック管理に必要なルーティング構成、OCI Network Firewallを使用する利点、インテリジェントなルーティング戦略を通じてセキュリティを最適化するためのベスト・プラクティス設計を示します。

OCI Network Firewallをパブリック・サブネットまたはプライベート・サブネットにデプロイすることで、どちらのケースでもプライベートIPアドレスのみを受信できます。OCI Network Firewallは、トラフィック・ルーティング・パス内の「Bump in the Wire」として統合され、トラフィックが宛先に到達する前に、追加のセキュリティ処理を実行します。この設定では、VCNおよびサブネットのルート表のルート・ルールとして、OCI Network FirewallのプライベートIPを宛先CIDRのターゲットに設定することで、トラフィックがOCI Network Firewallに送られます。その後、OCI Network Firewallのサブネット・ルート表に従って、トラフィックが宛先に転送されます。2つの基本的なVCNルーティング機能がこのプロセスをサポートしています。VCN内ルーティングとVCNゲートウェイ・イングレス・ルーティングです。OCIでのVCNルーティングの詳細は、『Learn Routing in Oracle Cloud Infrastructure Networking with Examples』を参照してください。このドキュメントでは、VCN内ルーティングやVCNゲートウェイ・イングレス・ルーティングなどのVCNルーティングについて、シナリオとともに詳しく説明しています。

この後の項では、OCIネットワーク・ファイアウォールをトポロジに挿入する際にサポートされる、一般的なVCNルーティング・シナリオについて説明します。

パフォーマンス向上のため、ファイアウォール・サブネットにアタッチされたセキュリティ・リストにステートフル・ルールを追加したり、ステートフル・ルールを持つNSGにファイアウォールを含めたりしないでください。

ファイアウォール・サブネットと仮想ネットワーク・インタフェース・カード(VNIC)に関連付けられたセキュリティ・リストとNSGルールは、ファイアウォールの手間で評価されます。セキュリティ・リストやNSGルールではトラフィックがファイアウォールに入ることを必ず許可し、トラフィックを適切に評価できるようにしてください。

VCN内ルーティングを使用したOCIネットワーク・ファイアウォール挿入のルーティング・ユース・ケース

次のシナリオは、OCIネットワーク・ファイアウォールを同じVCN内のサブネット間に配置する場合に使用するVCN内ルーティング設計を表したものです。次の図は、OCIネットワーク・ファイアウォールを、同じVCNにあるアプリケーションのWeb層サブネットとアプリケーション層サブネットの間に配置する例を示しています。どちらの方向のトラフィックもOCIネットワーク・ファイアウォールを経由するように、VCN内サブネット・ルート・ルールが両方のサブネット・ルート表で定義されているため、トラフィックが宛先に直接到達することはありません。

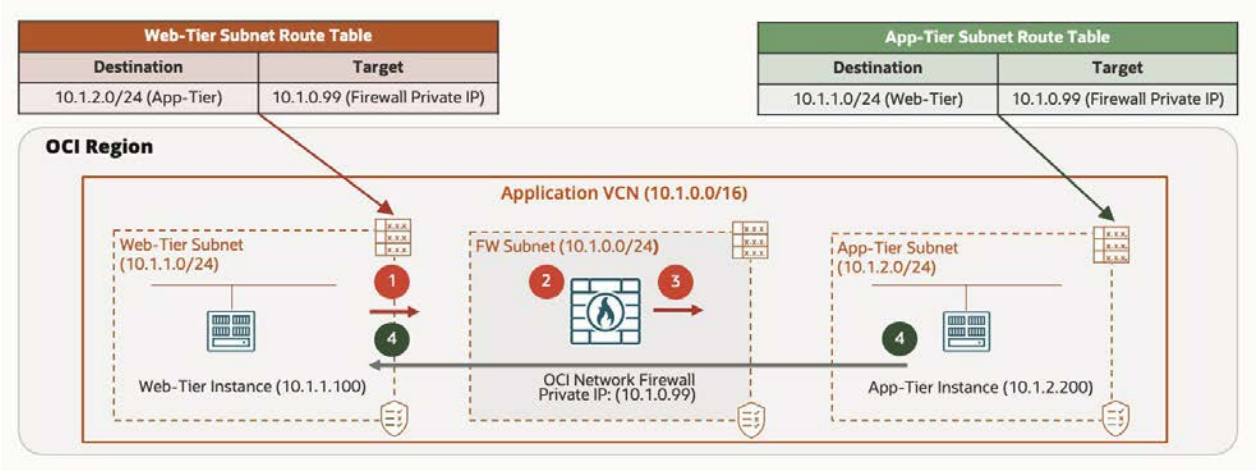

図3: OCIネットワーク・ファイアウォールと宛先へのVCN内サブネット・ルーティングのフロー。赤色の表は宛先に向かうイングレス・ルート・ルールを示し、緑色の表はソースへの戻りトラフィックのエグレス・ルート・ルールを示します。

トラフィック・フローは、次のステップに従って移動します。

1. Web層サブネット内のソース10.1.1.100から発生したトラフィックは、サブネット・ルート表のエントリを使用して、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.1.0.99に送られます。
2. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
3. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、サブネット・ルート表を使用して、トラフィックを宛先10.1.2.200に転送します。
4. 戻りトラフィックは同じパスをたどり、OCIネットワーク・ファイアウォールを通ってソース10.1.1.100に戻ります。

OCIのルーティングでは、最長接頭辞一致を用いて転送に関する決定を下します。静的デフォルト・ルートの0.0.0.0/0を使用する際には注意してください。VCN内のサブネット間でのルーティングに使用されるサブネット・ルート表に含まれている既存のルートより、静的デフォルト・ルートの方が限定的になるようにする必要があります。

OCIゲートウェイを使用したOCIネットワーク・ファイアウォール挿入のルーティング・ユース・ケース

OCIでは、ネットワーク通信を容易にし、トラフィックを保護する上で、いくつかのゲートウェイ・タイプが重要な役割を果たします。インターネット・ゲートウェイを使用すると、パブリック・サブネットがインターネットに直接接続できるため、インターネット・ゲートウェイはインバウンドおよびアウトバウンドのトラフィック検査での一般的な挿入ポイントとなっています。NATゲートウェイを使用すると、プライベート・サブネットのインスタンスがインターネットにさらされることなく、アウトバウンド・トラフィックを開始できます。動的ルーティング・ゲートウェイ(DRG)は、ハイブリッドのマルチクラウド接続の中心となり、VCN、オンプレミス・ネットワーク、OCIの間でトラフィックをルーティングします。OCIローカル・ピアリング・ゲートウェイ(LPG)を使用すると、同じリージョン内の複数のVCNを従来の方法で接続できますが、DRGほどの柔軟性とスケールは得られません。サービス・ゲートウェイは、インターネットを経由せずにOracleサービスにプライベートにアクセスできるセキュア・パスを提供します。これらのゲートウェイはいずれも、OCI Network Firewallと連係して、様々なネットワーク・シナリオでセキュリティと可視性を強化し、トラフィックのきめ細かな制御と保護を可能にします。

インターネット・ゲートウェイが同じVCN内の宛先ではなくOCIネットワーク・ファイアウォールにトラフィックを送信する

このユース・ケースでは、OCIネットワーク・ファイアウォールはOCIインターネット・ゲートウェイと連係して、インバウンドおよびアウトバウンドのトラフィックのセキュリティを強化します。OCIネットワーク・ファイアウォールがトラフィックを検査できるようにするために、インターネット・ゲートウェイはイングレス・ルート表に関連付けられています。イングレス・ルート表は、OCIネットワーク・ファイアウォールのプライベートIPアドレスにトラフィックを送信する転送ルールで構成されている必要があります。トラフィックがOCIネットワーク・ファイアウォールに到達すると、ファイアウォールのセキュリティ・ポリシー(脅威の有無の検査、アクセス制御の施行、その他の構成済ルールの適用など)に従って処理されます。

ファイアウォールは、トラフィックを処理した後、トラフィックを宛先に転送し、セキュリティ基準を満たすトラフィックのみが通過を許可されるようにします。

受信側では、VCNの宛先サブネットが自身のルート表を使用して戻りトラフィックを転送します。サブネット・ルート表を構成して、戻りトラフィックをOCIネットワーク・ファイアウォールのプライベートIPアドレスに送信するための転送ルールを含めます。このアプローチでは、アウトバウンド・トラフィックが保護されるだけでなく、セキュリティ管理が一元化されるため、インターネット・ゲートウェイを通過するすべてのトラフィックが、インターネットに転送される前に、OCIネットワーク・ファイアウォール・ポリシーの対象となります。

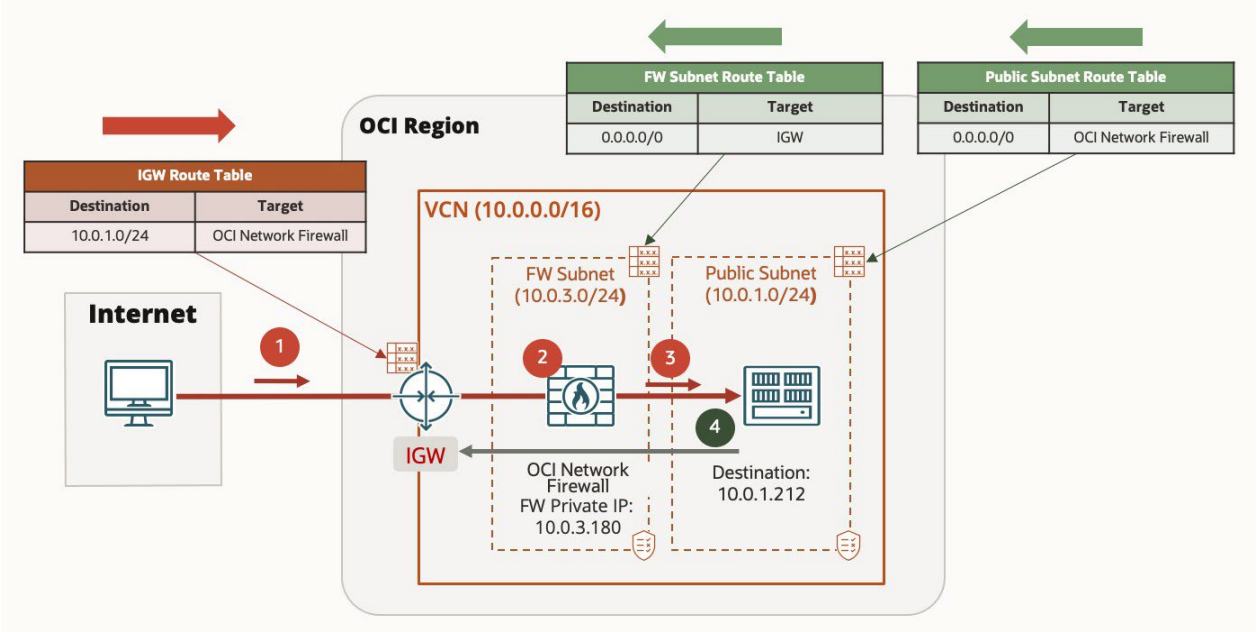

図4: インターネット・ゲートウェイからOCIネットワーク・ファイアウォールと宛先へのインバウンド・トラフィックのフロー。赤色の表と線は宛先に向かうイングレス・ルート・ルールとトラフィック・フローを示し、緑色の表と線はソースへの戻りトラフィックのルート・ルールとフローを示します。

トラフィック・フローは、次のステップに従って移動します。

1. インターネット・ソースから発生し、インターネット・ゲートウェイに到着したトラフィックは、イングレス・ルート表のエントリを使用して、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.3.180に転送されます。
2. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
3. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、サブネット・ルート表を使用して、トラフィックを宛先10.0.1.212に転送します。
4. 戻りトラフィックは同じパスをたどり、OCIネットワーク・ファイアウォールを通ってインターネット上のソースに戻ります。

NATゲートウェイが同じVCN内の宛先ではなくOCIネットワーク・ファイアウォールにトラフィックを送信する

このユース・ケースでは、OCIネットワーク・ファイアウォールはOCIネットワーク・アドレス変換(NAT)ゲートウェイと連係して、プライベート・サブネットから発生したアウトバウンド・トラフィックのセキュリティを強化します。OCIネットワーク・ファイアウォールが戻りトラフィックを検査できるようにするために、NATゲートウェイはイングレス・ルート表に関連付けられています。イングレス・ルート表は、OCIネットワーク・ファイアウォールのプライベートIPアドレスにトラフィックを送信する転送ルールで構成されている必要があります。

トラフィックがOCIネットワーク・ファイアウォールに到達すると、ファイアウォールのセキュリティ・ポリシー(脅威の有無の検査、アクセス制御の施行、その他の構成済ルールの適用など)に従って処理されます。ファイアウォールは、トラフィックを処理した後、トラフィックを宛先に転送し、セキュリティ基準を満たすトラフィックのみが通過を許可されるようにします。

戻りトラフィックについては、VCN内の宛先サブネットがルート表を使用して戻りトラフィックをOCIネットワーク・ファイアウォールに送り、継続的な検査が行われるようにします。このアプローチでは、アウトバウンド・トラフィックが保護されるだけでなく、セキュリティ管理が一元化されるため、NATゲートウェイを経由するすべてのトラフィックが、VCNを離れる前に、OCIネットワーク・ファイアウォール・ポリシーに確実に準拠します。

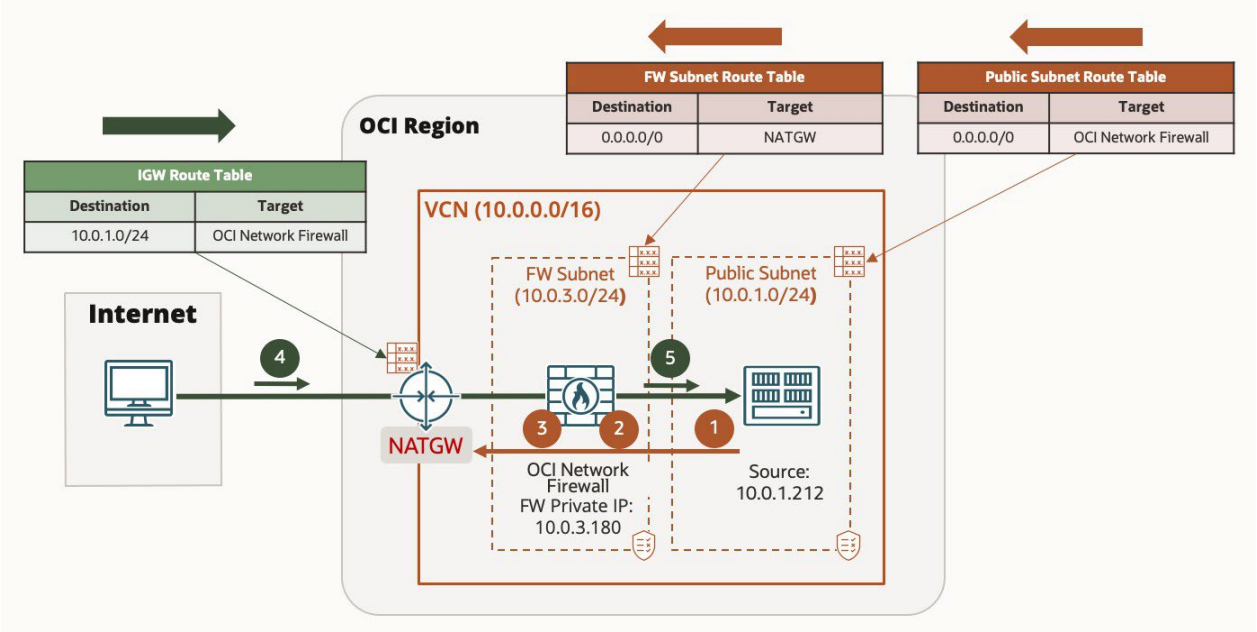

図5: NATゲートウェイからOCIネットワーク・ファイアウォールと宛先への戻りトラフィックのフロー。緑色の表と線はソースへの戻りトラフィックのイングレス・ルート・ルールとトラフィック・フローを示し、赤色の表と線はルート・ルールと開始されて宛先に向かうフローを示します。

トラフィック・フローは、次のステップに従って移動します。

1. OCIクライアントから発生したトラフィックは、サブネット・ルート表のエントリを使用して、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.3.180に転送されます。
2. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
3. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、サブネット・ルート表のエントリを使用して、トラフィックをNATゲートウェイに転送します。
4. NATゲートウェイに到着した戻りトラフィックは、イングレス・ルート表のエントリを使用して、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.3.180に転送されます。
5. OCIネットワーク・ファイアウォールは、サブネット・ルート表を使用して、トラフィックを宛先10.0.1.212に転送します。

DRGを使用した、中央で共有されているVCNとOCIネットワーク・ファイアウォール経由のリージョン内ルーティング

リージョン内VCNルーティングでは、同じリージョン内の異なるVCNに存在するネットワーク・リソース間でトラフィックをルーティングします。リージョン内VCNルーティングとは、リージョン内でのVCN間ルーティングを意味します。リージョン内でのVCN間接続にはDRGを使用するのが、シンプルさとスケーラビリティが得られる推奨アプローチです。

OCIネットワーク・ファイアウォールを中央のサービス・ハブVCNにデプロイし、一元化されたファイアウォールを共有する複数のスポークVCNにアプリケーションを分散させることができます。これは、ファイアウォールのデプロイメントを1つしか必要としないため、コスト効果が高く、運用しやすいと見なされることの多いアプローチです。この設計シナリオでは、サービス・ハブVCNとアプリケーション・スポークVCNがDRG経由で接続されます。アプリケーションのWeb層とアプリケーション層は、同じVCN内の2つのサブネットに配置されます。DRGをターゲットとして使用し、2つのサブネットの間にVCN内サブネット・ルート・ルールが構成されます。DRGは、検査のために、アプリケーション・トラフィックをサービス・ハブVCN内のOCIネットワーク・ファイアウォールに送ります。

この構成では、Web層とアプリケーション層の間のすべてのトラフィックを一元化されたOCIネットワーク・ファイアウォールによって確実に検査し、複数のVCNでセキュリティ・ポリシーの一貫した施行を維持するとともに、アーキテクチャ全般を簡素化することができます。

次の図は、一元化されたOCIネットワーク・ファイアウォールがサービス・ハブVCN内にデプロイされ、複数のスポークVCNがファイアウォールへのアクセスを共有する様子を示しています。この設定は、各アプリケーションVCNのWeb層からのトラフィックが同じVCN内のアプリケーション層に到達する前に、そのトラフィックをサービス・ハブVCNのファイアウォールに送り、検査を行うことを目的としています。この図は、フォワード・ルーティング・パス(Web層からファイアウォール経由でアプリケーション層に至る)と、レスポンスが同じルートを戻るようにするためのリバース・ルーティング・パスの両方を示しています。また、Web層とアプリケーション層の間のVCN内サブネット・ルーティングではDRGをターゲットとして使用し、シームレスな接続を維持しています。

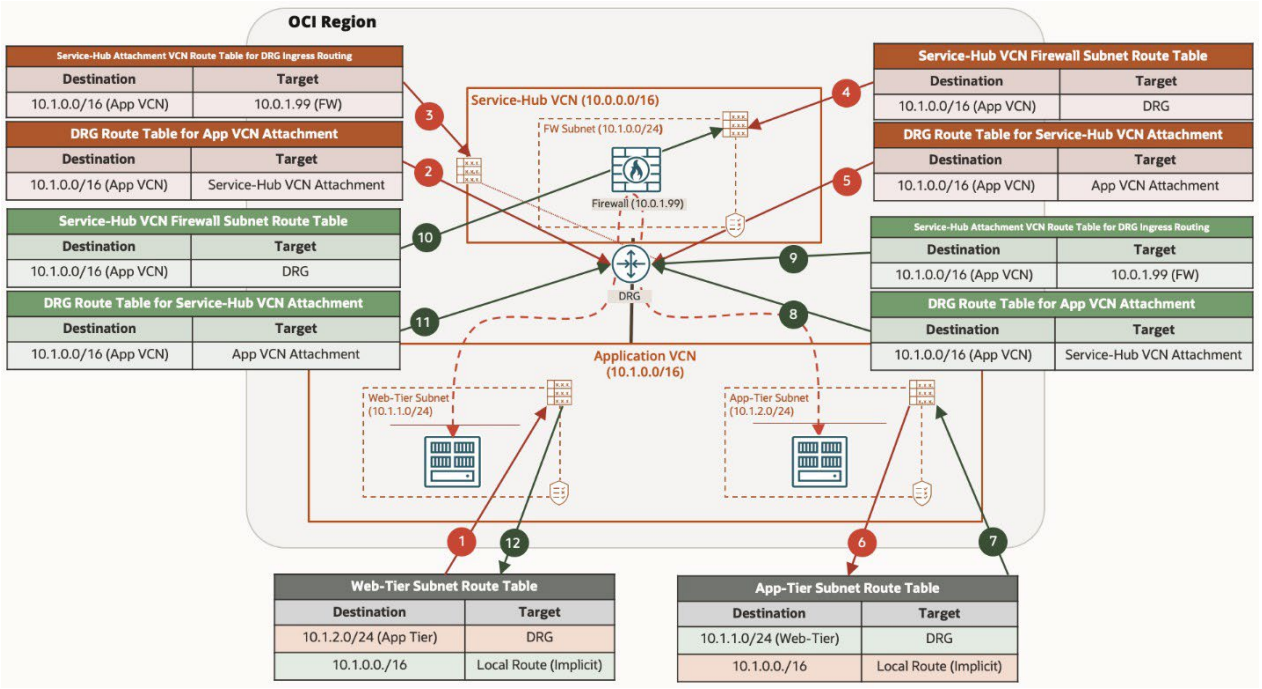

図6: 中央で共有されているVCN OCIネットワーク・ファイアウォールのルーティング・プロセスでは、DRGを使用してスポークVCN間のトラフィックをルーティングします。赤色の表は宛先に向かうイングレス・ルート・ルールを示し、緑色の表はソースへの戻りトラフィックのエグレス・ルート・ルールを示します。

トラフィック・フローは、次のステップに従って移動します。

1. Web層サブネット内のソース・インスタンスから発生したトラフィックは、アプリケーション層サブネットを宛先とするサブネット・ルート表のエントリを使用して、DRGに転送されます。
2. アプリケーションVCNアタッチメントのDRGルート表は、一元化されたOCIネットワーク・ファイアウォールがデプロイされているサービス・ハブVCNアタッチメントを使用して、トラフィックを転送します。
3. DRGイングレス・ルーティング用のサービス・ハブ・アタッチメントVCNルート表を使用して、トラフィックをアプリケーションVCN内のアプリケーション層サブネットに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.1.99に転送します。
4. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、サブネット・ルート表のエントリを使用して、トラフィックをDRGに転送します。
5. サービス・ハブVCNアタッチメントのDRGルート表は、アプリケーションVCNアタッチメントを使用して、トラフィックを転送します。
6. アプリケーションVCNアタッチメントのDRGルート表は、イングレス・ルーティング用のアプリケーション層VCNルート表を使用して、トラフィックを宛先に転送します。

ステップ7から12は、戻り方向の同じホップバイホップ・プロセスを示しています。

上の設計のバリエーションとして、ハブアンドスポーク設計のWeb層とアプリケーション層をそれぞれ専用のVCNに分離することもできます。

ローカル・ピアリング・ゲートウェイを使用した、中央で共有されているVCNとOCIネットワーク・ファイアウォール経由のリージョン内ルーティング

リージョン内でのVCN間接続にLPGを使用するのは従来のアプローチです。これは、特定のシナリオでは引き続き使用できますが、複雑でスケーラビリティが制限されるため、DRGほど好まれていません。

OCIネットワーク・ファイアウォールを中央のサービス・ハブVCNにデプロイし、一元化されたファイアウォールを共有する複数のスポークVCNにアプリケーションを分散させることができます。この設計シナリオでは、サービス・ハブVCNとアプリケーション・スポークVCNがLPG経由で接続されます。アプリケーションのWeb層とアプリケーション層は、同じVCN内の2つのサブネットに配置されます。LPGをターゲットとして使用し、2つのサブネットの間にVCN内サブネット・ルート・ルールが構成されます。LPGは、検査のために、アプリケーション・トラフィックをサービス・ハブVCN内のOCIネットワーク・ファイアウォールに送ります。この構成では、Web層とアプリケーション層の間のすべてのトラフィックを一元化されたOCIネットワーク・ファイアウォールによって確実に検査できます。

次の図は、一元化されたOCIネットワーク・ファイアウォールがサービス・ハブVCN内にデプロイされ、複数のスポークVCNがファイアウォールへのアクセスを共有する様子を示しています。この設定は、各アプリケーションVCNのWeb層からのトラフィックが同じVCN内のアプリケーション層に到達する前に、そのトラフィックをサービス・ハブVCNのファイアウォールに送り、検査を行うことを目的としています。次の図は、フォワード・ルーティング・パス(Web層からファイアウォール経由でアプリケーション層に至る)と、レスポンスが同じルートを戻るようにするためのリバース・ルーティング・パスの両方を示しています。また、Web層とアプリケーション層の間のVCN内サブネット・ルーティングではLPGをターゲットとして使用し、シームレスな接続を維持しています。

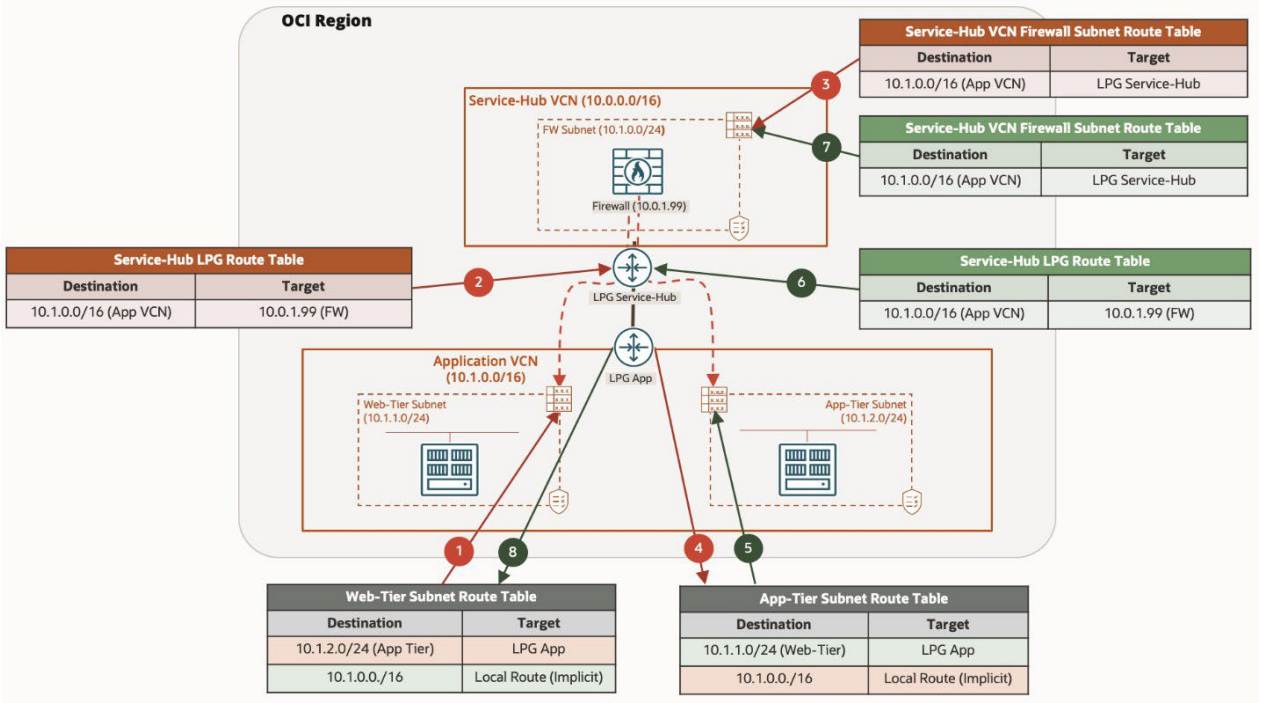

図7: 中央で共有されているVCN OCIネットワーク・ファイアウォールのルーティング・プロセスでは、LPGを使用してスポークVCN間のトラフィックをルーティングします。

トラフィック・フローは、次のステップに従って移動します。

1. Web層サブネット内のソース・インスタンスから発生したトラフィックは、アプリケーション層サブネットを宛先とするサブネット・ルート表のエントリを使用して、LPGに転送されます。
2. サービス・ハブVCN LPGルート表にはイングレス・ルーティングが構成されています。このルート表を使用して、トラフィックをアプリケーションVCN内のアプリケーション層サブネットに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.1.99に転送します。

3. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、サブネット・ルート表のエントリを使用して、トラフィックをLPGに転送します。
4. アプリケーションVCN LPGルート表にはローカル・イングレス・ルーティングが構成されています。このルート表を使用して、トラフィックを宛先に転送します。

ステップ5から8は、戻り方向の同じホップバイホップ・プロセスを示しています。

NATゲートウェイとDRGを使用したハブアンドスポーク

次のシナリオは、スポークVCNがDRG経由で中央のハブに接続する、OCIのハブアンドスポーク・ネットワーク・アーキテクチャを示しています。ハブは、接続されているすべてのスポークVCNからのネットワーク・トラフィックを管理および保護するための中心点として機能します。ハブは、OCI Network FirewallやNATゲートウェイなどの主要サービスをホストします。OCIネットワーク・ファイアウォールは、スポークからのアウトバウンド・トラフィックを検査、フィルタリング、保護し、すべてのエグレス・トラフィックをハブのセキュリティ・ポリシーに確実に準拠させます。NATゲートウェイにより、スポークVCN内のインスタンスは、インターネットに直接さらされることなくインターネットへのアウトバウンド接続を開始できるため、エグレスのみのインターネット・トラフィックのセキュアな中心点が得られます。このアーキテクチャは、セキュリティ管理を合理化し、トラフィック制御を一元化します。

NATゲートウェイに関するOCIのドキュメントによると、NATゲートウェイを使用できるのは専用VCN内のリソースのみです。VCNが別のVCNとピアリング接続している場合、他方のVCN内のリソースはNATゲートウェイにアクセスできません。

この設計では、OCIネットワーク・ファイアウォールはハブVCN内のローカル・リソースの役割を果たすため、ピアリング接続されたVCNのリソースがNATゲートウェイを利用できます。

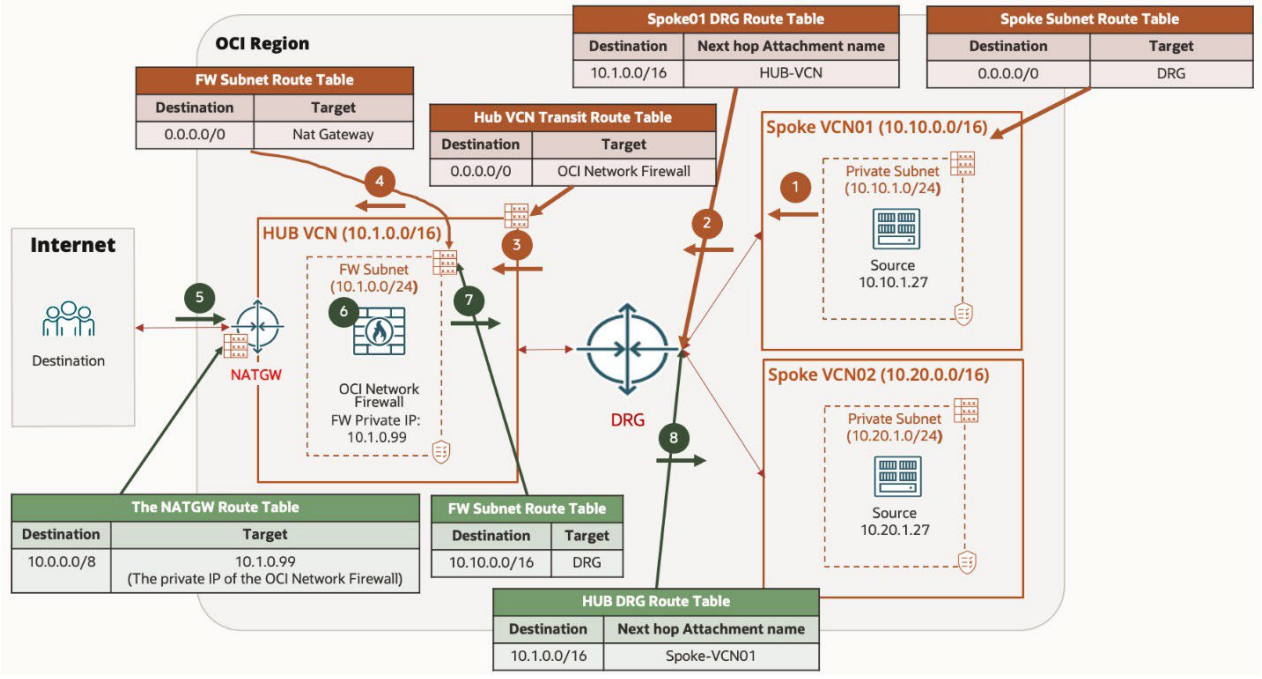

図8: NATとDRGを使用したハブアンドスポークのトポロジとホップバイホップ・ルーティング・プロセス。緑色の表と線はソースへの戻りトラフィックのイングレス・ルート・ルールとトラフィック・フローを示し、赤色の表と線はルート・ルールと開始されて宛先に向かうフローを示します。

トラフィック・フローは、次のステップに従って移動します。

1. スポークVCN01サブネット内のソース・インスタンスから発生したトラフィックは、インターネットを宛先とするサブネット・ルート表のエントリを使用して、DRGに転送されます。
2. スポークVCN01アタッチメントのDRGルート表は、一元化されたOCIネットワーク・ファイアウォールがデプロイされているハブVCNアタッチメントを使用して、トラフィックを転送します。

3. DRGイングレス・ルーティング用のサービス・ハブ・アタッチメントVCNルート表を使用して、トラフィックを同じVCN内のNATゲートウェイに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.1.99に転送します。
4. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、サブネット・ルート表のエントリを使用して、トラフィックをNATゲートウェイに転送します。
5. NATゲートウェイに到着した戻りトラフィックは、イングレス・ルート表のエントリを使用して、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.1.99に転送されます。
6. OCIネットワーク・ファイアウォールは着信トラフィックを検査します。
7. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、スポークVCN01を宛先とするサブネット・ルート表のエントリを使用して、トラフィックをDRGに転送します。
8. スポークVCN01アタッチメントのDRGルート表は、イングレス・ルーティング用のスポークVCN01ルート表を使用して、トラフィックを宛先に転送します。

DRGを使用した、OCIネットワーク・ファイアウォール経由のリージョン間ルーティング

異なるOCIリージョンにあるVCNのリソース間でトラフィックをルーティングしなければならない場合があります。異なるリージョンにあるDRG間でリモート・ピアリング接続(RPC)を使用できます。トラフィックはOCIバックボーン・ネットワークを通るので、セキュアで高パフォーマンスのデータ転送が保証されます。

セキュリティ向上のために、リモート・ピアリング接続に関係するリージョンの一方または両方の端にOCIネットワーク・ファイアウォールをデプロイできます。この設定により、きめ細かなトラフィック・フィルタリング・ポリシーの定義、アクセス制御、ネットワーク・トラフィックのモニタリングが可能になり、追加の保護レイヤーが得られます。リージョンの端にファイアウォールをデプロイすることで、トラフィックがVCNに入る前にセキュリティ・ポリシーを施行できるため、リージョン間のデータ・フローの制御を強化し、潜在的な脅威から保護することが可能になります。

次の図に示すシナリオについて考えてみましょう。このシナリオでは、Region-1内のVCN-1のSubnet-01にあるリソースが、Region-2内のVCN-2のSubnet-02にあるリソースと通信する必要があります。このリージョン間通信を容易にするために、Region-1のDRG-1とRegion-2のDRG-2の間にRPCが設定され、リージョンをまたがったシームレスなトラフィック転送を可能にしています。トラフィックのセキュリティを確保するために、両方のリージョンで、それぞれのVCNの端にOCIネットワーク・ファイアウォールがデプロイされています。この構成により、トラフィックがSubnet-02のターゲット・リソースに到達する前に、事前定義済のセキュリティ・ポリシーに従ってトラフィックを検査し、フィルタリングすることができるため、リージョン間のデータ・フローに対する追加の保護および制御レイヤーが得られます。

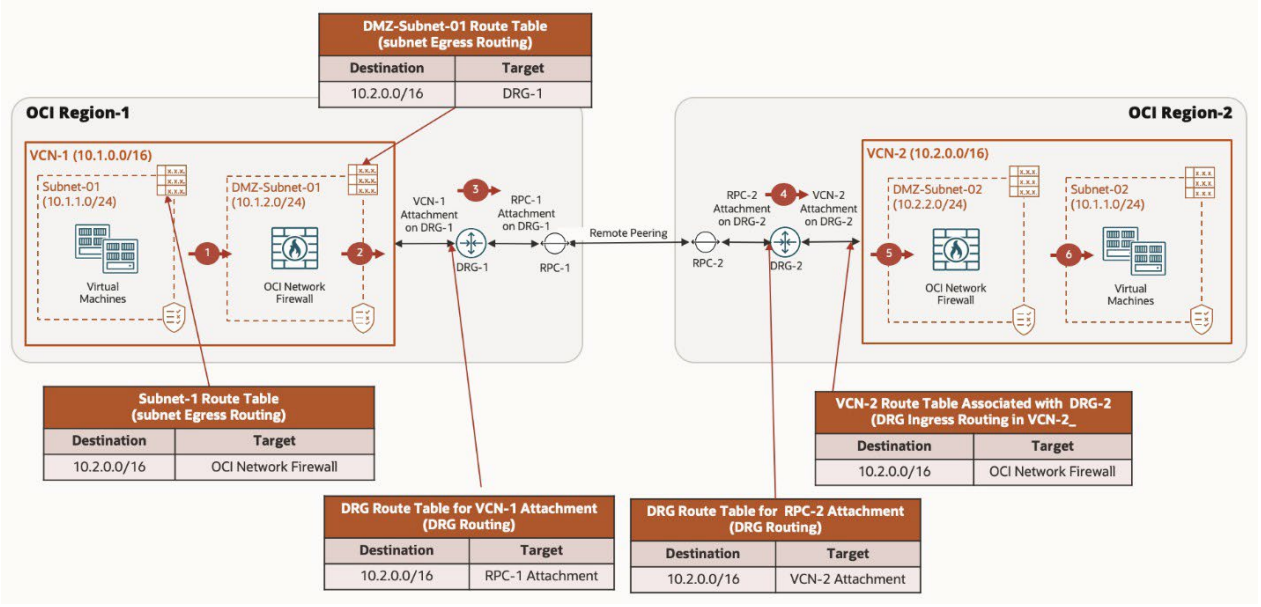

図9: セキュリティ向上のためにOCIネットワーク・ファイアウォールを通過する、2つのOCIリージョン間のトラフィックのトポロジとホップバイホップ・ルーティング・プロセス。赤色の表は宛先に向かうイングレス・ルート・ルールを示し、緑色の表はソースへの戻りトラフィックのエグレス・ルート・ルールを示します。

トラフィック・フローは、次のステップに従って移動します。

1. ソース・サブネット(VCN-1のSubnet-01)で、サブネット・ルート表に基づいてサブネット・エグレス・ルーティングが行われ、ローカルOCIネットワーク・ファイアウォールをターゲットとする宛先へのルートが解決されます。トラフィックは、ローカルOCIネットワーク・ファイアウォールに送られます。
2. ローカルOCIネットワーク・ファイアウォールは、サブネット・ルート表でルーティング・ルックアップ操作を実行します。これにより、DRGを次のホップとする宛先へのルートが解決されます。
3. ソースVCNアタッチメントに関連付けられたDRGルート表は、RPC-1アタッチメントを次のホップ・アタッチメントとする宛先へのルートを解決します。トラフィックは、RPC接続経由でリモート・リージョンのDRGに送られます。
4. リモートDRGは、RPC-2アタッチメントに関連付けられたDRGルート表でルーティング・ルックアップ操作を実行します。これにより、ローカルOCIネットワーク・ファイアウォールを次のホップとする宛先へのルートが解決されます。リモートDRGは、宛先のVCNイングレス・ルーティングを通じて、トラフィックをローカルOCIネットワーク・ファイアウォールのVCNに送ります。
5. ローカルOCIネットワーク・ファイアウォールは、サブネット・ルート表でルーティング・ルックアップ操作を実行します。これにより、Subnet-02を次のホップとする宛先への暗黙的ローカル・ルートを使用して、ルートが解決されます。
6. トラフィックが宛先に到着します。

戻りトラフィックは同じパスをたどり、ローカルOCIネットワーク・ファイアウォールを通って、Region-1のRPCとローカルOCIネットワーク・ファイアウォール経由でソースに戻ります。

サービス・ゲートウェイが宛先ではなくOCIネットワーク・ファイアウォールにトラフィックを送信する

OCIネットワーク・ファイアウォールをセキュアWebゲートウェイ(SWG)の手前に配置してレイヤー7 URLをフィルタリングするとともに、特定のサービスへのアクセスを制限し、サービスのセキュリティ・ポリシーに従ってトラフィックを検査することで、脅威からの高度な保護を実現できます。セキュアWebゲートウェイのイングレス・ルーティングを使用して、サービス・ゲートウェイを経由する転送パスにOCIネットワーク・ファイアウォールを挿入できます。

次のシナリオはこの設計を表したもので、サービス・ゲートウェイ経由でOCIサービスにアクセスするアプリケーション・サブネットからのトラフィックが、OCIネットワーク・ファイアウォールによって検査されます。サービス・ゲートウェイには、OCIネットワーク・ファイアウォールのプライベートIPアドレスをターゲットとする、宛先サブネットCIDRまたはVCN CIDRのルート・ルールを含む、ルート表があります。OCIネットワーク・ファイアウォールは、その構成に基づいてトラフィックのパケットを処理した後、トラフィックを宛先に向けて転送します。その後、VCNサブネットがルート表を使用して、トラフィックを宛先に送ります。

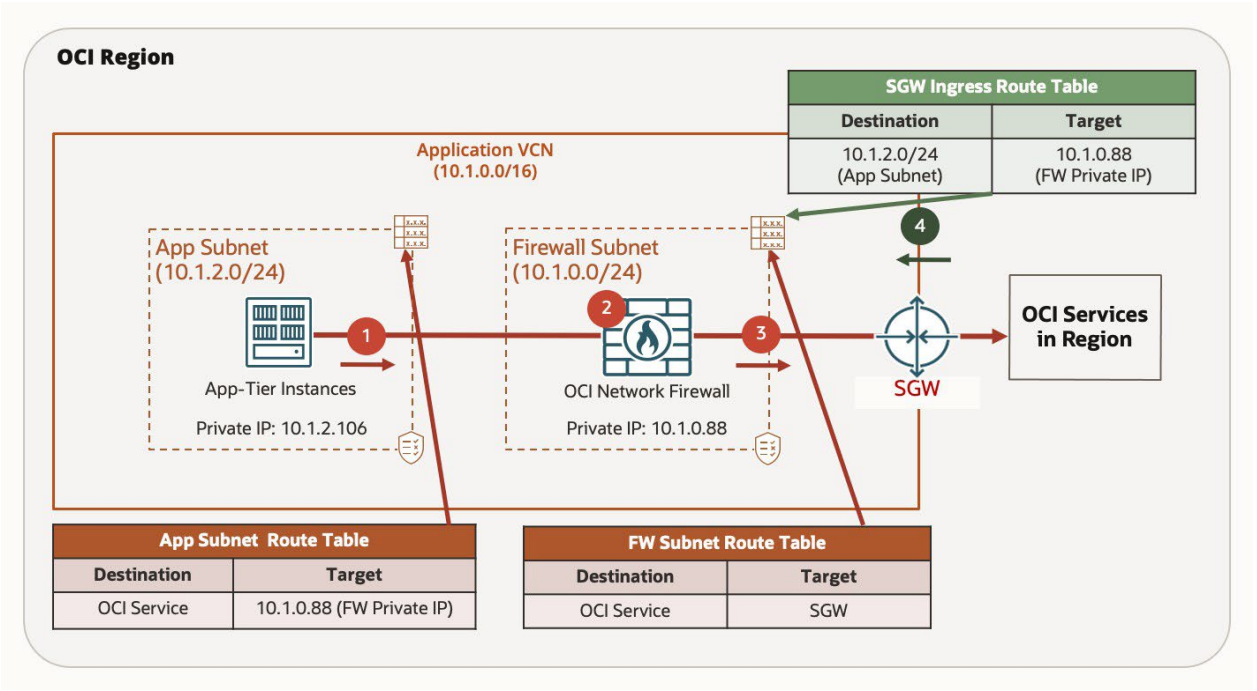

図10: サービス・ゲートウェイが宛先ではなくOCIネットワーク・ファイアウォールにトラフィックを送信するトポロジとホップバイホップ・ルーティング・プロセス。赤色の表は宛先に向かうイングレス・ルート・ルールを示し、緑色の表はソースへの戻りトラフィックのエグレス・ルート・ルールを示します。

トラフィック・フローは、次のステップに従って移動します。

1. アプリケーション層インスタンスから発生し、Oracle Services Network (OSN)のOracleサービスに向かうトラフィックは、SWGに直接転送されるのではなく、サブネット・ルート表のエントリを使用して、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.1.0.88に転送されます。
2. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
3. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、サブネット・ルート表のエントリを使用して、トラフィックをサービス・ゲートウェイに転送します。
4. 戻りトラフィックは同じパスをたどり、OCIネットワーク・ファイアウォールを通ってインターネット上のソースに戻ります。

オンプレミスへのOCIネットワーク・ファイアウォール挿入のルーティング・ユース・ケース

OCIネットワーク・ファイアウォールをネットワーク・アーキテクチャに挿入して、ハイブリッド・クラウド・デプロイメントからのトラフィック・フローを保護することができます。この後の項では、オンプレミス・ネットワークからのトラフィック・フローの検査に使用する、サポート対象のOCIネットワーク・ファイアウォール挿入シナリオについて説明します。

オンプレミス・インスタンスがOCIネットワーク・ファイアウォール経由でVCNにアクセスする

ハイブリッド・クラウド・デプロイメントがますます普及するのに伴い、オンプレミス・ネットワークとクラウド・ネットワークの間のシームレスな通信が必要になっています。DRGを使用すると、複数のVCNを1つのDRG経由でオンプレミス・ネットワークに接続できます。このオンプレミス・ネットワークは、VPNトンネルまたはFastConnect仮想回線で接続できます。図11に示すように、オンプレミス・ネットワークからOCI VCNへのトラフィックをOCI Network Firewall経由でルーティングし、セキュリティ・ポリシーを施行することができます。同様に、OCIからオンプレミス・ネットワークに戻るトラフィックは同じルーティング・パスをたどり、OCIネットワーク・ファイアウォールを通過します。

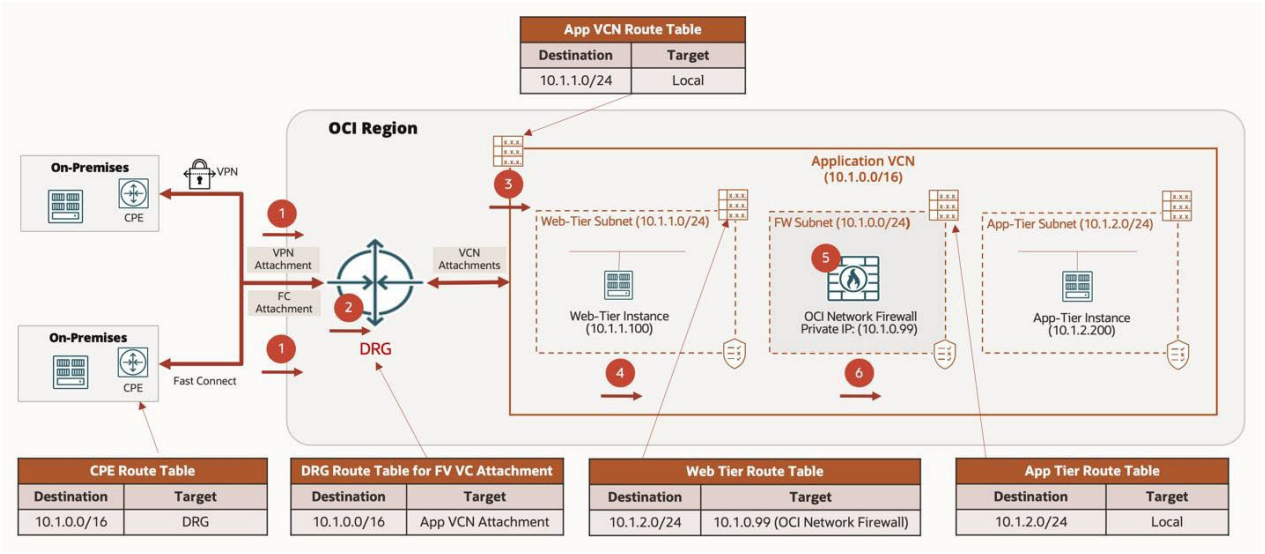

図11: オンプレミス・インスタンスがOCIネットワーク・ファイアウォール経由でVCNにアクセスするトポロジとホップバイホップ・ルーティング・プロセス。

トラフィック・フローは、次のステップに従って移動します。

1. オンプレミスから発生したトラフィックは、顧客構内設備(CPE)ルート表を使用します。このルート表には、次のホップとしてDRGを指し示すOCIネットワークのルートが含まれています。
2. DRGルート表のルックアップには、アプリケーションVCNアタッチメントの次のホップ・ターゲットが含まれています。
3. アプリケーションVCNアタッチメントには、イングレス・ルーティング用のデフォルトVCNルート表が含まれており、暗黙的ローカル・ルートを使用してトラフィックをWeb層サブネット内の宛先に送ります。
4. Web層サブネット・ルート表は、トラフィックを同じVCN内のアプリケーション層インスタンスに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.1.99に送ります。
5. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
6. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、サブネット・ルート表のエントリ(暗黙的ローカル・ルート)を使用して、トラフィックをアプリケーション層サブネットに転送します。

戻りトラフィックは同じパスを逆にたどります。OCIネットワーク・ファイアウォールを、この例のWeb層の手前に配置することもできます。

オンプレミス・インスタンスが中央で共有されているVCN OCIネットワーク・ファイアウォール経由でスポークVCNにアクセスする

DRGの最新機能を用いた一般的な設計では、DRGを中央のハブとして使用し、VCNの相互接続とオンプレミス・ネットワークへの直接接続を行います。次の図はそのようなネットワーク設計を示したもので、中央で共有されているVCN OCIネットワーク・ファイアウォールを組み合せて、トラフィックをスポークに送信する前に、オンプレミスからOCIネットワーク・ファイアウォールに送ります。

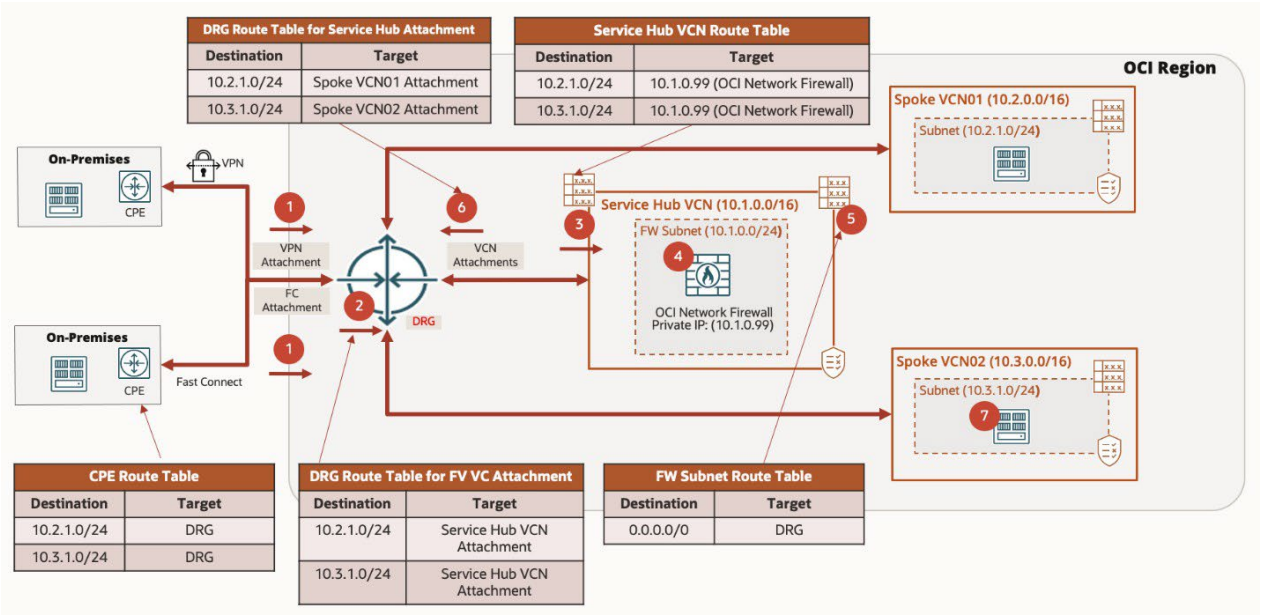

図12: オンプレミス・インスタンスが中央で共有されているVCN OCIネットワーク・ファイアウォール経由でスポークVCNにアクセスするトポロジとホップバイホップ・ルーティング・プロセス。

トラフィック・フローは、次のステップに従って移動します。

1. オンプレミスから発生したトラフィックは、CPEルート表を使用します。このルート表には、次のホップとしてDRGを指し示すOCIネットワークのルートが含まれています。
2. DRGルート表のルックアップには、サービス・ハブVCNアタッチメントの次のホップ・ターゲットが含まれています。
3. サービス・ハブVCNアタッチメントには、イングレス・ルーティング用のサービス・ハブVCNルート表が含まれており、トラフィックをスポークVCNに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.1.99を持つスポークVCN内の宛先に送ります。
4. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
5. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、デフォルト・ルールを含むサブネット・ルート表のエントリを使用して、トラフィックをDRGに転送します。
6. DRGルート表のルックアップには、スポークVCNアタッチメントの次のホップ・ターゲットが含まれています。
7. トラフィックがスポークVCNサブネットに到着します。

戻りトラフィックは同じパスを逆にたどります。サービス・ハブとOCIネットワーク・ファイアウォール経由でスポークVCN01を通ってスポークVCN02に移動するトラフィックがこのトポロジでサポートされています。

ロード・バランサを使用したOCIネットワーク・ファイアウォール挿入のルーティング・ユース・ケース

OCIネットワーク・ファイアウォールをOCI Load Balancerサービスと組み合せて、ネットワーク・アーキテクチャに挿入できます。OCI Load Balancerの詳細は、Load Balancerのドキュメントを参照してください。次のシナリオは、OCI Load Balancerとともに使用する、サポート対象のOCIネットワーク・ファイアウォール挿入を示しています。

OCIロード・バランサのフロントエンドとなるOCIネットワーク・ファイアウォール

VNCの境界にあるパブリック・ロード・バランサまたはプライベート・ロード・バランサの手前にOCIネットワーク・ファイアウォールを配置すると、特にセキュリティ、トラフィック管理、コンプライアンスに関連して、いくつかの利点が得られます。OCIネットワーク・ファイアウォールは第1の防御線の役割を果たし、不正なトラフィックをブロックするとともに、ロード・バランサとバックエンド・サーバーがインターネットまたはオンプレミスからの潜在的な脅威に直接さらされるのを防ぎます。この設定により、正規のトラフィックのみがロード・バランサに到達することを保証できます。

OCIネットワーク・ファイアウォールは、インターネットまたはプライベート・ネットワークに面したアプリケーションを保護し、コンプライアンスを確保し、パブリック・アクセスにさらされる組織に包括的なネットワーク・セキュリティを提供する上で、きわめて重要です。パブリック・ロード・バランサまたはプライベート・ロード・バランサの手前にOCIネットワーク・ファイアウォールを配置すると、脅威や悪意のある活動を検知して軽減できるため、セキュリティが大幅に向上します。

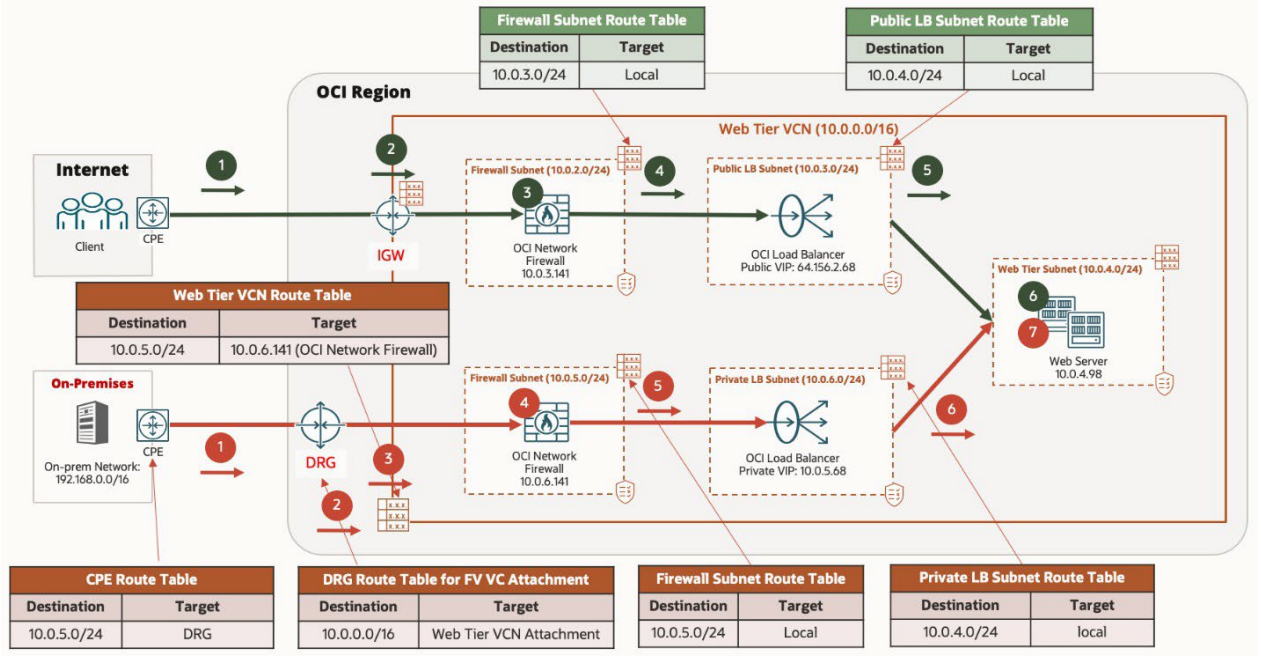

図13: ロード・バランサのフロントエンドとなるOCIネットワーク・ファイアウォールのトポロジ。赤色の線と番号はオンプレミスからのトラフィック・フローを表し、緑色の線と番号はインターネットからのトラフィック・フローを表します。

オンプレミスでは、トラフィック・フローは次のステップに従って移動します。

1. オンプレミスから発生し、プライベート・ロード・バランサのIPアドレス10.0.5.68に向かうトラフィックは、CPEルート表を使用します。このルート表には、次のホップとしてDRGを指し示すOCIネットワークのルートが含まれています。
2. DRGルート表のルックアップには、Web層ハブVCNアタッチメントの次のホップ・ターゲットが含まれています。
3. Web層VCNアタッチメントには、イングレス・ルーティング用のWeb層VCNルート表が含まれており、トラフィックをプライベート・ロード・バランサ・サブネットに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.6.141を持つ宛先プライベート・ロード・バランサ・サブネットに送ります。
4. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
5. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、Web層サブネットの暗黙的ローカル・ルートを含むサブネット・ルート表のエントリを使用して、トラフィックをプライベート・ロード・バランサ・サブネットに転送します。
6. プライベート・ロード・バランサは、トラフィックを受信し、Web層サブネットへの暗黙的ローカル・ルートを含むプライベート・ロード・バランサ・サブネットのサブネット・ルート表を使用します。
7. トラフィックがWeb層サーバーに到着します。

インターネット上では、トラフィック・フローは次のステップに従って移動します。

1. インターネット・ソースから発生し、パブリック・ロード・バランサのIPアドレス64.156.2.68に向かうトラフィックは、OCIパブリック・ロード・バランサ・サブネットのルートを含むCPEルート表を使用します。
2. インターネット・ソースから発生し、インターネット・ゲートウェイに到着したトラフィックは、イングレス・ルート表のエントリを使用して、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.3.141に転送されます。
3. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。

4. OCIネットワーク・ファイアウォールは、サブネット・ルート表を使用して、トラフィックをパブリック・ロード・バランサのプライベートIPアドレスに転送します。
5. パブリック・ロード・バランサは、トラフィックを受信し、Web層サブネットへの暗黙的ローカル・ルートを含むパブリック・ロード・バランサ・サブネットのサブネット・ルート表を使用します。
6. トラフィックがWeb層サーバーに到着します。戻りトラフィックは同じパスを逆にたどります。

OCIロード・バランサのバックエンドとなるOCIネットワーク・ファイアウォール

VCN内のパブリック・ロード・バランサまたはプライベート・ロード・バランサの背後にOCIネットワーク・ファイアウォールを配置すると、セキュリティを階層化しながらトラフィック・フローを最適化することによる戦略的利点が得られます。この構成では、ロード・バランサは着信トラフィックの分散を処理します。OCIネットワーク・ファイアウォールは、より集中的な第2の防御線の役割を果たし、ロード・バランサを通過したトラフィックの検査とフィルタリングを行います。この設定により、特に脅威を検査し、アプリケーション・レイヤーでのコンプライアンスを徹底する目的で、さらにきめ細かくトラフィックを管理し、保護することができます。

OCIネットワーク・ファイアウォールをロード・バランサの背後に置くことで、ロード・バランサは、正常なバックエンド・サーバーにトラフィックを分散するというコア機能を実行できます。一方、ファイアウォールは、正規のトラフィックにより深い脅威がないか検査することに専念します。この設定では、効率的なトラフィック管理と堅牢なセキュリティのバランスを取ることができます。

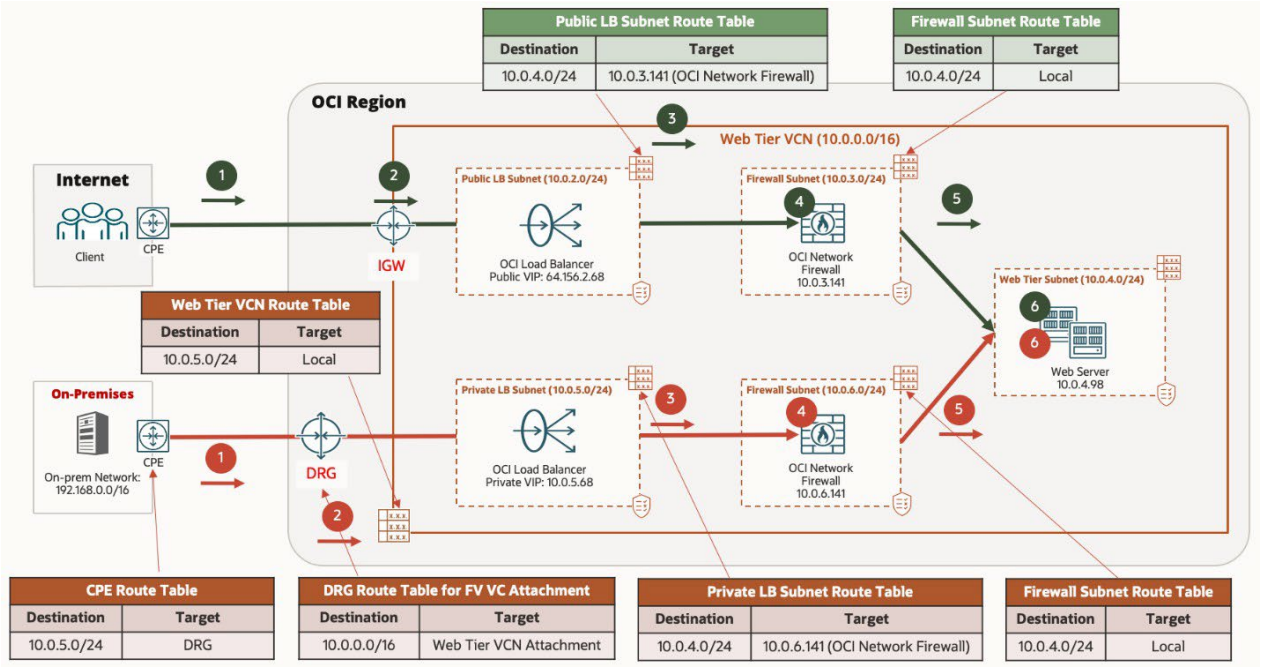

図14: OCIロード・バランサのバックエンドとなるOCIネットワーク・ファイアウォールのトポロジ。赤色の線と番号はオンプレミスからのトラフィック・フローを表し、緑色の線と番号はインターネットからのトラフィック・フローを表します。

オンプレミスでは、トラフィック・フローは次のステップに従って移動します。

1. オンプレミスから発生し、プライベート・ロード・バランサのIPアドレス10.0.5.68に向かうトラフィックは、CPEルート表を使用します。このルート表には、次のホップとしてDRGを指し示すOCIネットワークのルートが含まれています。
2. DRGルート表のルックアップには、プライベート・ロードバランサ・サブネットの暗黙的ローカル・ルートを含むWeb層ハブVCNアタッチメントの次のホップ・ターゲットが含まれています。
3. プライベート・ロード・バランサは、トラフィックを受信し、Web層サブネットに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.1.99を持つプライベート・ロード・バランサ・サブネットのサブネット・ルート表を使用します。

4. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
5. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、Web層サブネットの暗黙的ローカル・ルートを含むサブネット・ルート表のエントリを使用して、トラフィックをWeb層サブネットに転送します。
6. トラフィックがWeb層サーバーに到着します。

インターネット上では、トラフィック・フローは次のステップに従って移動します。

1. インターネット・ソースから発生し、パブリック・ロード・バランサのIPアドレス64.156.2.68に向かうトラフィックは、CPEルート表を使用します。このルート表には、OCIパブリック・ロード・バランサ・サブネットのルートが含まれています。
2. インターネット・ゲートウェイ・ルート表のルックアップには、パブリック・ロード・バランサ・サブネットの次のホップ・ターゲットが含まれています。
3. パブリック・ロード・バランサは、トラフィックを受信し、Web層サブネットに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.3.141を持つパブリック・ロード・バランサ・サブネットのサブネット・ルート表を使用します。
4. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
5. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、Web層サブネットの暗黙的ローカル・ルートを含むサブネット・ルート表のエントリを使用して、トラフィックをWeb層サブネットに転送します。
6. トラフィックがWeb層サーバーに到着します。

戻りトラフィックは同じパスを逆にたどります。

SSLモードのOCIロード・バランサを使用したOCIネットワーク・ファイアウォール挿入

前の項では、OCIロード・バランサを使用してトラフィック・フローを効果的に保護する、OCIネットワーク・ファイアウォール・ルーティング挿入のユース・ケースを見てきました。この項では、それらのシナリオについてさらに詳しく説明し、特にロード・バランサでSSLモードを有効にするユース・ケースに焦点を当てます。ここでは、OCI Network Firewallサービスを使用してトラフィックを復号し、詳細な検査を実行して、セキュリティ・ポリシーを施行することで、OCIロード・バランサを含む暗号化されたネットワーク・パス全体でセキュリティと可視性を確実に強化する方法を確認します。

OCIでは、ロード・バランサを使用する際のセキュリティやパフォーマンスの要件に応じて、様々な方法でSSLを実装できます。これらの方法については、ブログ記事「Load Balancing SSL Traffic in OCI」を参照してください。主なユース・ケースの例として、次のものがあります。

- **SSL終端:** SSL接続がロード・バランサで終端するため、バックエンド・サーバーは暗号化されていないトラフィックを処理できます。
- **SSLトンネリング:** ロード・バランサでトラフィックを復号せずに、クライアントとバックエンド・サーバーの間のトランスポート・チャネル全体を保護します。
- **エンドツーエンドSSL:** ロード・バランサがクライアントのSSL接続を終端し、バックエンド・サーバーへの暗号化された接続を新たに開始します。この構成は、ロード・バランサがHTTPヘッダーを検査または変更しなければならない場合に便利です。

OCIネットワーク・ファイアウォールをOCIロード・バランサのパスにシームレスに統合してセキュリティを強化し、暗号化されたトンネルを中断せずにすべてのユース・ケースをサポートすることができます。終端モードでは、ファイアウォールは、ロード・バランサでのSSL終端の前にトラフィックを検査できるので、脅威からの高度な保護が実現し、トラフィック・フローのパブリック側でセキュリティ・ポリシーが施行されます。トンネリング・モードでは、セキュアで暗号化された通信がネットワーク・パス全体で保証されます。エンドツーエンド・モードでは、ファイアウォールは、ロード・バランサでのSSL終端の後にトラフィックを検査できるので、脅威からの高度な保護が実現し、トラフィック・フローのプライベート側でセキュリティ・ポリシーが施行されます。

OCIネットワーク・ファイアウォールでのインバウンドSSL検査に必要な証明書は、OCIロード・バランサの稼働時のSSLモードによって異なります。

次のシナリオは、トンネリング・モードまたはエンドツーエンドSSLモードのOCIロード・バランサを使用した、サポート対象のOCIネットワーク・ファイアウォール挿入を示しています。このシナリオでは、ネットワーク・インフラストラクチャは、ユーザーが内部(組織のプライベート・ネットワーク内に存在)か外部(インターネットからアクセス)かに基づいて、Webサーバーへの2つの異なるアクセス・パスを提供します。目的は、同じバックエンド・リソース(Webサーバー)へのセキュアで効率的なアクセスを提供しながら、堅牢なセキュリティ制御を実施することです。信頼できないインターネットからネットワークの境界を保護するには、OCIネットワーク・ファイアウォールをデプロイします。OCIネットワーク・ファイアウォールは、SSLが有効になっている2つのOCIロード・バランサ(パブリックとプライベート)の間に戦略的に配置します。

この設計では、外部ユーザーと内部ユーザーに別々のロード・バランサを使用するため、トラフィックをセキュアに分離できます。外部ユーザーが内部リソースに直接アクセスすることはできず、まずOCIネットワーク・ファイアウォールによるトラフィックの検査を受ける必要があります。この設計により、内部ユーザーは、プライベート・ロード・バランサの異なるSSL暗号化基準に従うことができます。OCIネットワーク・ファイアウォールは、外部トラフィックにセキュリティ・ポリシーを適用することで、悪意のある活動が広がるのを防止し、外部ユーザーからのトラフィックが内部サービスに到達する前に、潜在的な脅威がないか十分に検査されることを保証します。

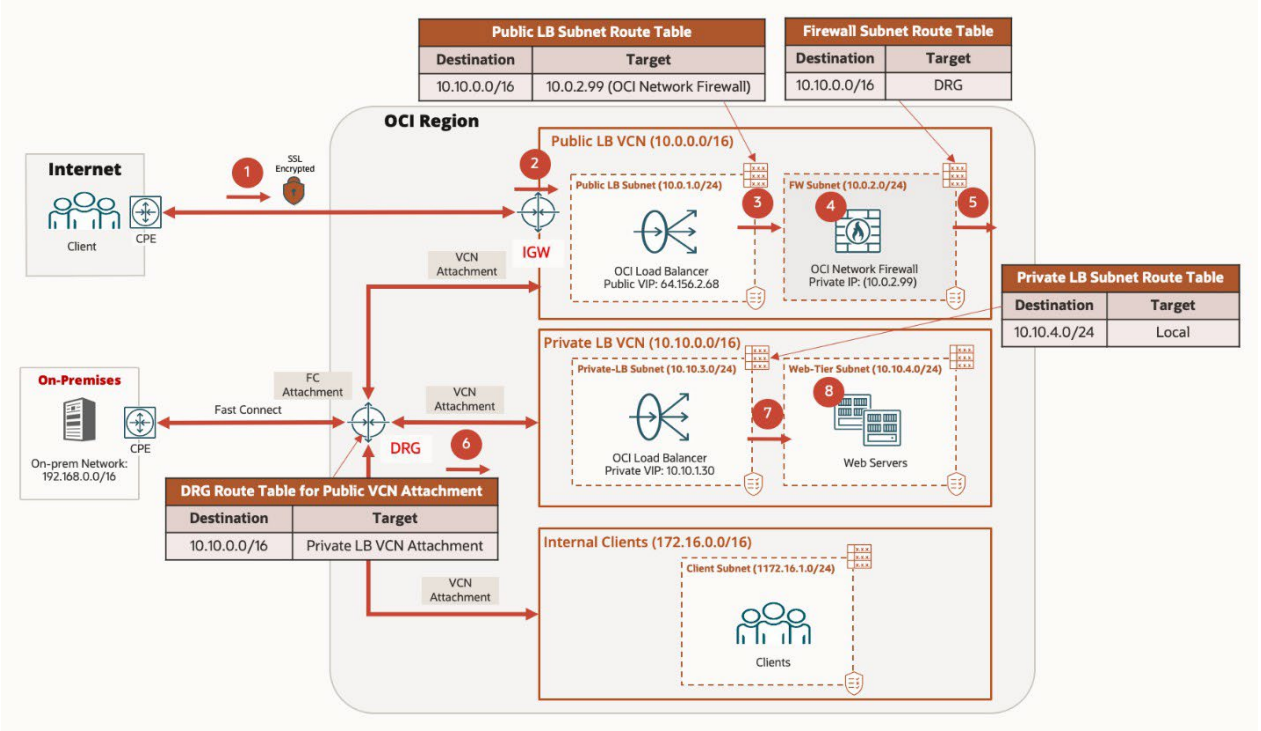

図15: OCIロード・バランサのSSLを使用したOCIネットワーク・ファイアウォール挿入のトポロジ

インターネット上では、トラフィック・フローは次のステップに従って移動します。

1. インターネット・ソースから発生し、パブリック・ロード・バランサのIPアドレスに向かうトラフィックは、CPEルート表を使用します。このルート表には、OCIパブリック・ロード・バランサ・サブネットのルートが含まれています。外部ユーザーは、パブリックSSL証明書を使用してパブリック・ロード・バランサに接続します。
2. インターネット・ゲートウェイ・ルート表のルックアップには、パブリック・ロード・バランサ・サブネットの次のホップ・ターゲットが含まれています。
3. パブリック・ロード・バランサがトラフィックを受信します。パブリック・ロード・バランサは、SSL接続を終端し、バックエンド・サーバー(プライベート・ロード・バランサのリスナーIPアドレス10.10.1.30)へのSSL接続を新たに開始します。パブリック・ロード・バランサ・サブネットのルート表には、プライベート・ロード・バランサに向かうトラフィックを、DRGに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIP 10.0.2.99経由で送信するためのプライベートIPルート・ルールが含まれています。

4. OCIネットワーク・ファイアウォールは、SSLインバウンド検査のルールを含む構成済のセキュリティ・ポリシーに基づいて、トラフィックを許可または拒否します。OCIネットワーク・ファイアウォールは、プライベート・ロード・バランサに一致するSSL証明書とキーで構成されています。
5. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、すべての10.10.0.0/16トラフィックをDRGに転送するルート・ルールを含むサブネット・ルート表を使用して、トラフィックを転送します。
6. DRGルート表のルックアップには、プライベート・ロードバランサ・サブネットの暗黙的ローカル・ルートを含むプライベート・ロード・バランサVCNアタッチメントの次のホップ・ターゲットが含まれています。
7. プライベート・ロード・バランサがトラフィックを受信します。プライベート・ロード・バランサは、SSL接続を終端し、バックエンド・サーバー(Webサーバー)へのSSL接続を新たに開始します。プライベート・ロード・バランサ・サブネットのルート表には、トラフィックをWebサーバーに直接送信するための暗黙的ローカル・ルート・ルールが含まれています。
8. トラフィックがWeb層サーバーに到着します。

戻りトラフィックは同じパスを逆にたどります。

ネットワーク・ロード・バランサを使用したOCIネットワーク・ファイアウォール挿入のルーティング・ユース・ケース

OCIネットワーク・ファイアウォールをOCIネットワーク・ロード・バランサと組み合せて、ネットワーク・アーキテクチャに挿入できます。ネットワーク・ロード・バランサは、NATモード、ソース保持モード、透過(ソースと宛先の保持)モードをサポートしています。これらのモードについては、ネットワーク・ロード・バランサのドキュメントの「Modes of Operation」に詳しい説明があります。各モードがトラフィック・フローのソースと宛先に与える影響を理解することは、セキュアで効率的なネットワークを設計する上できわめて重要です。フルNATモードのネットワーク・ロード・バランサは、NATゲートウェイ、インターネット・ゲートウェイ、DRGなどのOCIゲートウェイと組み合せて使用できます。一方、透過(ソースと宛先の保持)モードのネットワーク・ロード・バランサは、一緒に使用できるのがプライベート・ネットワーク・ロード・バランサのみであるため、DRGとの併用のみが可能です。

ネットワーク・ロード・バランサ向け仮想クラウド・ネットワーク・ルーティング

OCIの設定では、ネットワーク・ロード・バランサのトラフィックを、OCIネットワーク・ファイアウォールを含むVCNを経由するようにサブネット間でルーティングするのが、セキュリティとトラフィックの制御を強化するための一般的な設計パターンです。通常、この設定を行う際には、ネットワーク・ロード・バランサをプライベート・サブネットに配置し、VCNでルーティング・ルールを構成して、別のサブネットのOCIネットワーク・ファイアウォール経由でトラフィックを送信します。クライアントに面したサブネットとバックエンド・サブネットの間のトラフィックを検査および管理するセキュリティ・ポリシーでファイアウォールを構成し、必要なポートとプロトコルのみを許可することができます。この設定では、ネットワーク・ロード・バランサによってルーティングされるすべてのトラフィックがOCIネットワーク・ファイアウォールで確実にフィルタリングされるため、トラフィックがVCN内の宛先に到着する前にセキュリティを強化できます。

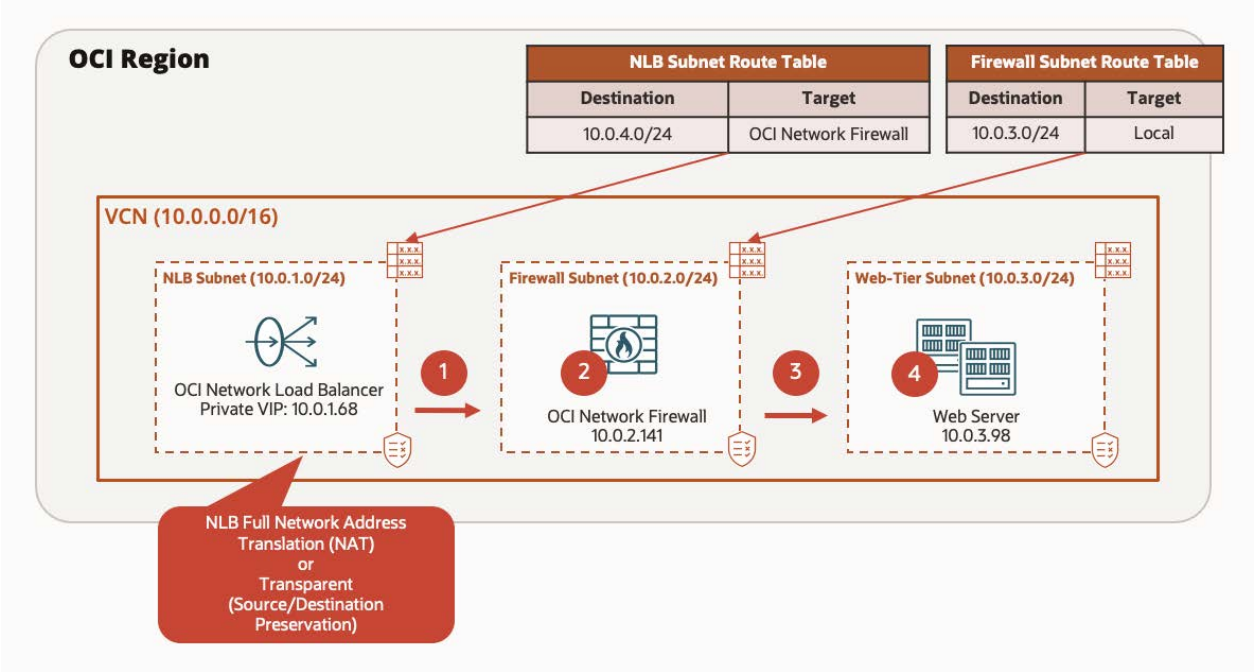

図16: フルNATモードまたは透過(ソースと宛先の保持)モードのプライベート・ネットワーク・ロード・バランサを経由し、検査のためにOCIネットワーク・ファイアウォールを通って、同じVCN内の宛先バックエンド・サーバーに到着するようにルーティングされるVCN内トラフィックのフロー。

トラフィック・フローは、次のステップに従って移動します。

1. プライベート・ネットワーク・ロード・バランサは、ソースからのトラフィックを受信し、Web層サブネットに直接送るかわりに、プライベート・ネットワーク・ロード・バランサ・サブネットのサブネット・ルート表を使用して、トラフィックをOCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.2.41に送ります。
2. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
3. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、Web層サブネットの暗黙的ローカル・ルートを含むサブネット・ルート表のエントリを使用して、トラフィックをWeb層サブネットに転送します。
4. トラフィックがWeb層サーバーに到着します。

戻りトラフィックは同じパスを逆にたどります。

ネットワーク・ロード・バランサ向けインバウンド・インターネット・トラフィックのインターネット・ゲートウェイ経由でのルーティング

次のインバウンド・インターネット・トラフィックのシナリオでは、トラフィックはパブリック・インターネットから発生し、インターネット・ゲートウェイ経由でOCIに送られます。ネットワーク・ロード・バランサは、ソース(パブリックIP)と宛先(ネットワーク・ロード・バランサ)の仮想IP (VIP)アドレスを変換することで着信インターネット・トラフィックを処理し、バックエンド・サーバーがインターネットに直接さらされないように保護します。

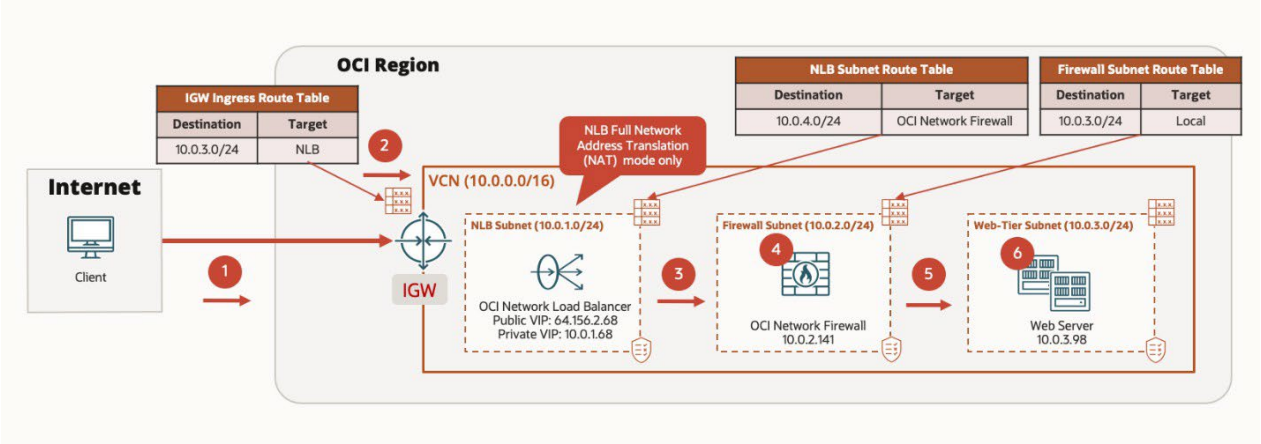

図17: インターネット・ゲートウェイ経由で、フルNATモードのネットワーク・ロード・バランサ、ネットワーク・ファイアウォール、バックエンド・サーバーに向かうインバウンド・インターネット・トラフィックのフロー。

インターネット上では、トラフィック・フローは次のステップに従って移動します。

1. インターネット・ソースから発生し、パブリック・ネットワーク・ロード・バランサのIPアドレスに向かうトラフィックは、CPEルート表を使用します。このルート表には、OCIパブリック・ネットワーク・ロード・バランサ・サブネットのルートが含まれています。
2. インターネット・ゲートウェイ・ルート表のルックアップには、パブリック・ネットワーク・ロード・バランサ・サブネットの次のホップ・ターゲットが含まれています。
3. パブリック・ネットワーク・ロード・バランサは、トラフィックを受信し、Web層サブネットに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.2.141を持つパブリック・ロード・バランサ・サブネットのサブネット・ルート表を使用します。
4. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
5. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、Web層サブネットの暗黙的ローカル・ルートを含むサブネット・ルート表のエントリを使用して、トラフィックをWeb層サブネットに転送します。
6. トラフィックがWeb層サーバーに到着します。

戻りトラフィックは同じパスを逆にたどります。

ネットワーク・ロード・バランサ向けインバウンド・オンプレミス・トラフィックのDRGを使用したルーティング

インバウンド・トラフィックがオンプレミス環境から発生してVPNまたはFastConnectを経由するシナリオの場合、OCIでは、DRGを経由してネットワーク・ロード・バランサに向かい、さらにOCIネットワーク・ファイアウォールを経由するセキュア・ルーティングが可能です。この設定は、オンプレミス・ネットワークからOCIでホストされているアプリケーションへの制御されたアクセスを保護するのに最適です。

この場合、オンプレミス環境からのトラフィックは、ネットワーク・ロード・バランサとファイアウォールが収容されているVCNに接続されたDRGに到達します。VCNのルーティング・ルールは、着信トラフィックをまずネットワーク・ロード・バランサ経由で送信するように構成されています。ネットワーク・ロード・バランサは、複数のバックエンド・リソースにトラフィックを分散して、スケーラビリティを確保します。トラフィックは、これらのリソースに到達する前に、OCIネットワーク・ファイアウォールによってフィルタリングされます。このとき、カスタム・セキュリティ・ポリシーを適用して、検査、脅威の検知、アクセス制御を行うことができます。このユース・ケースは、オンプレミスからクラウドへのワークロードのロード・バランシング、脅威の軽減、動的スケーラビリティの組合せにより、高セキュリティ要件をサポートします。

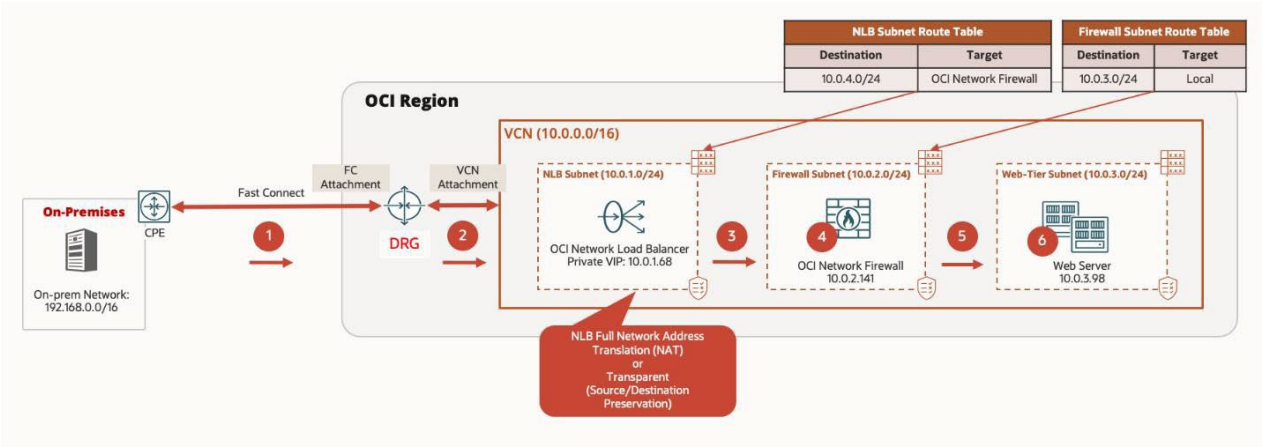

図18: オンプレミス・ネットワークからDRG経由でフルNATモードまたは透過モードのネットワーク・ロード・バランサに向かい、検査のためにOCIネットワーク・ファイアウォールを通って、同じVCN内の宛先バックエンド・サーバーに到着するインバウンド・トラフィックのフロー。

オンプレミスでは、トラフィック・フローは次のステップに従って移動します。

1. オンプレミスから発生し、プライベート・ネットワーク・ロード・バランサのIPアドレス10.0.1.68に向かうトラフィックは、CPEルート表を使用します。このルート表には、次のホップとしてDRGを指し示すOCIネットワークのルートが含まれています。
2. DRGルート表のルックアップには、プライベート・ネットワーク・ロードバランサ・サブネットの暗黙的ローカル・ルートを含むVCNアタッチメントの次のホップ・ターゲットが含まれています。
3. プライベート・ネットワーク・ロード・バランサは、トラフィックを受信し、Web層サブネットに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.2.41を持つプライベート・ネットワーク・ロード・バランサ・サブネットのサブネット・ルート表を使用します。
4. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
5. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、Web層サブネットの暗黙的ローカル・ルートを含むサブネット・ルート表のエントリを使用して、トラフィックをWeb層サブネットに転送します。
6. トラフィックがWeb層サーバーに到着します。

戻りトラフィックは同じパスを逆にたどります。

単一OCIネットワーク・ファイアウォール挿入のルーティング・ユース・ケース

North-South (インターネットバウンド)とEast-West (VCN間とオンプレミス)で別々のOCIネットワーク・ファイアウォールを管理すると、運用の複雑さとコストが増加します。チームは異なる構成やルール・セット、モニタリング・ツールを扱わなければならず、セキュリティ・ポリシーの一貫性が失われ、潜在的なセキュリティ・ギャップが生じる可能性があります。2つのファイアウォール・ソリューションのプロビジョニングとメンテナンスに多額のコストがかかる可能性もあります。OCIでは、パブリックおよびプライベートのサブネットとそれらに関連付けられたルート表の概念に基づき、リソースが内部的、外部的にどのように通信するかを決定します。さらに、OCIネットワーク・ファイアウォールなどのリソースをパブリック・サブネットとプライベート・サブネットのいずれかのみに割り当てる(同時に両方に割り当てない)こともできます。プライベート・サブネットのリソースはNATゲートウェイ経由でインターネットに出ることしかできず、インターネット・ゲートウェイは使用できないため、OCIネットワーク・ファイアウォールでNorth-SouthとEast-Westのトラフィック・フローを検査する必要がある場合は、North-South (インターネットバウンド)とEast-West (VCN間とオンプレミス)というトラフィックのパターンごとに、別々のOCIネットワーク・ファイアウォールをデプロイします。

次のシナリオは、OCIネットワーク・ファイアウォールを1つ使用してNorth-South (インターネットバウンド)とEast-West (VCN間とオンプレミス)の両方のトラフィック・パターンを管理できるようにする、サポート対象のOCIネットワーク・ファイアウォール挿入設計を表したものです。この設計では、OCIネットワーク・ファイアウォールを中央のハブVCN内にデプロイして、インターネットからのインバウンド・トラフィック・フロー、インターネットへのアウトバウンド・トラフィック・フロー、最後にオンプレミスからのトラフィック・フローを検査し、保護します。

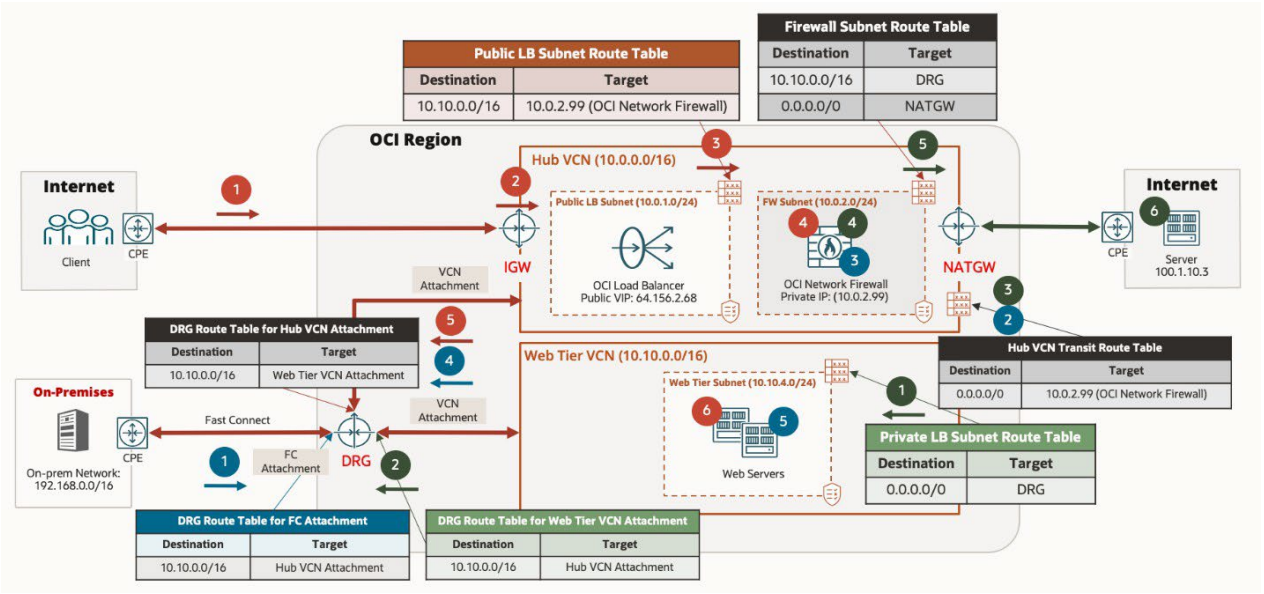

図19: 複数のトラフィック・フロー向け単一OCIネットワーク・ファイアウォールのルーティング挿入のトポロジとルーティング。赤色の線と番号は、インターネットからWebサーバーへのトラフィック・フローを表します。緑色の線と番号は、NATゲートウェイ経由でインターネットに向かうエグレス・トラフィック・フローを表します。青色の線と番号は、オンプレミスからWebサーバーへのトラフィック・フローを表します。黒色のルート表は、複数のタイプのトラフィック・フローに使用されます。

インターネットからのトラフィック・フローは、次のステップに従って移動します。

1. インターネット・ソースから発生し、パブリック・ロード・バランサのIPアドレスに向かうトラフィックは、CPEルート表を使用します。このルート表には、OCIパブリック・ロード・バランサ・サブネットのルートが含まれています。
2. インターネット・ゲートウェイ・ルート表のルックアップには、パブリック・ロード・バランサ・サブネットの暗黙的な次のホップ・ターゲットが含まれています。
3. パブリック・ロード・バランサがトラフィックを受信します。パブリック・ロード・バランサは、SSL接続を終端し、バックエンド・サーバー(Web層VCN内のWebサーバーのプライベートIPアドレス)へのSSL接続を新たに開始します。パブリック・ロード・バランサ・サブネットのルート表には、Webサーバーのプライベート IPアドレスに向かうトラフィックを、DRGに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIP 10.0.2.99経由で送信するためのプライベートIPルート・ルールが含まれています。
4. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
5. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、すべての10.10.0.0/16トラフィックをDRGに転送するルート・ルールを含むサブネット・ルート表を使用して、トラフィックを転送します。DRGルート表のルックアップには、Web層サブネットの暗黙的ローカル・ルートを含むWeb層VCNアタッチメントの次のホップ・ターゲットが含まれています。
6. トラフィックがWeb層サーバーに到着します。

NATゲートウェイ経由でインターネットに出るトラフィック・フローは、次のステップに従って移動します。

1. Web層VCNサブネット内のWeb層サーバーから発生したトラフィックは、サブネット・ルート表のエントリを使用して、DRGに転送されます。
2. Web層VCNアタッチメントのDRGルート表は、一元化されたOCIネットワーク・ファイアウォールがデプロイされているハブVCNアタッチメントを使用して、トラフィックを転送します。
3. DRGイングレス・ルーティング用のサービス・ハブ・アタッチメントVCNルート表は、トラフィックを同じVCN内のNATゲートウェイに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.2.99に転送します。

4. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
5. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、サブネット・ルート表のエントリを使用して、トラフィックをNATゲートウェイに転送します。
6. トラフィックがインターネット上のWeb層サーバーに到着します。

オンプレミスでは、トラフィック・フローは次のステップに従って移動します。

1. オンプレミスから発生したトラフィックは、CPEルート表を使用します。このルート表には、次のホップとしてDRGを指し示すOCIネットワークのルートが含まれています。DRGルート表のルックアップには、ハブVCNアタッチメントの次のホップ・ターゲットが含まれています。
2. ハブVCNアタッチメントには、イングレス・ルーティング用のトランジットVCNルート表が含まれており、トラフィックをWeb層VCNに直接送るかわりに、OCIネットワーク・ファイアウォールのプライベートIPアドレス10.0.2.99に送ります。
3. OCIネットワーク・ファイアウォールは、構成済のセキュリティ・ポリシーに基づいてトラフィックを許可または拒否します。
4. トラフィックが許可された場合、OCIネットワーク・ファイアウォールは、Web層VCNに向かうサブネット・ルート表のエントリを使用して、トラフィックをDRGに転送します。DRGルート表のルックアップには、Web層VCNアタッチメントの次のホップ・ターゲットが含まれています。
5. トラフィックがWeb層サーバーに到着します。

OCIネットワーク・ファイアウォール挿入でサポートされていないルーティング・ユース・ケース

OCIネットワーク・ファイアウォールをデプロイする際、特定のルーティング・シナリオはサポートされる構成の範囲に含まれません。こうしたサポート対象外の一般的なシナリオは、ネットワーク通信の問題やセキュリティ・ポリシーの施行ギャップ、パフォーマンス低下につながる可能性があります。制限事項を理解し、これらのルーティング構成を避けることは、ファイアウォールの最適なパフォーマンスを確保し、OCI環境内のトラフィック・フローを保護する上で、きわめて重要です。

ローカルVCN外部のインターネット・ゲートウェイ・ターゲットのリソース

OCIでは、インターネット・ゲートウェイはVCN内のパブリックIPアドレスとの間でトラフィックをルーティングするように設計されており、イングレス・トラフィックを別のVCNやプライベート・サブネットに送信することはできません。この制限が存在するのは、インターネット・ゲートウェイに関連付けられたルート表ルールがパブリック・サブネット外部のリソースをターゲットにできないためです。その結果、イングレス・インターネット・トラフィックを検査のために中央のOCIネットワーク・ファイアウォール経由でルーティングした後、別のVCNやプライベート・サブネットに転送する必要のあるシナリオはサポートされていません。

回避策として、OCIネットワーク・ファイアウォールをインターネットに面した各VCNに分散ソリューションとして実装できます。このアプローチでは、各VCNがインターネットバウンド・トラフィックを独立して処理できるため、VCN間ルーティングを必要としないセキュリティ検査が可能になります。

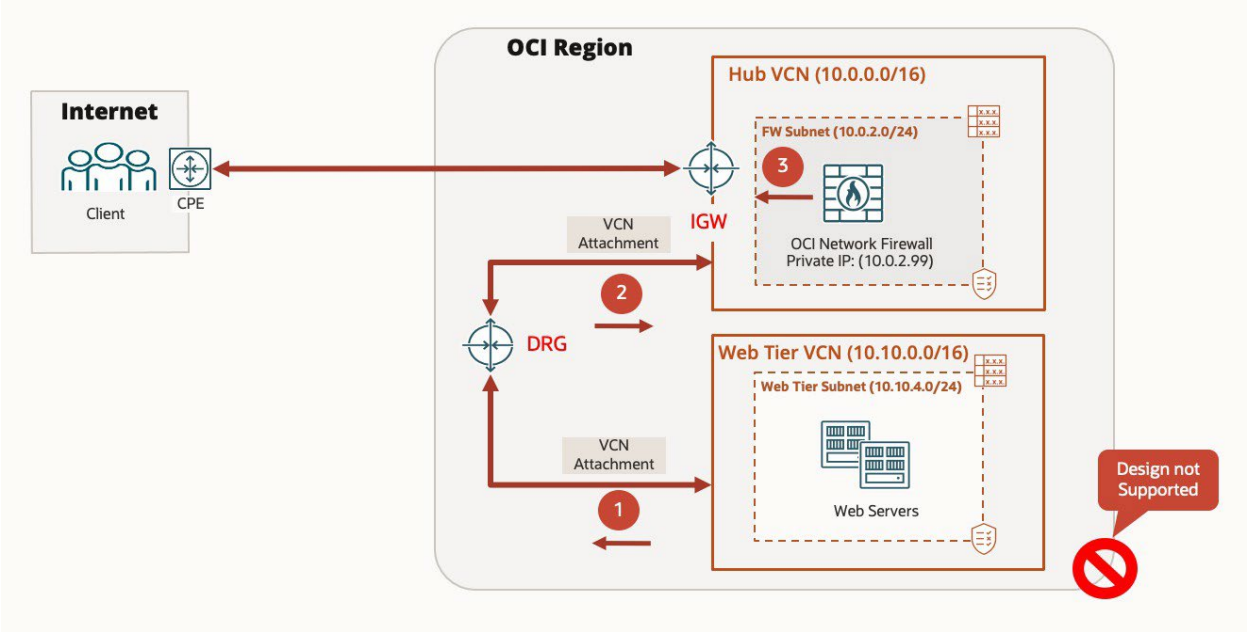

図20: ローカルVCN外部のリソースをターゲットとするインターネット・ゲートウェイのトポロジ

回避策として、OCIネットワーク・ファイアウォールをインターネットに面した各VCNに分散ソリューションとしてデプロイできます。

ネットワーク・ロード・バランサのソース保持モード

次の設計シナリオでは、OCIネットワーク・ロード・バランサがソース保持モードで動作します。このモードでは、ネットワーク・ロード・バランサは宛先NATを実行し、リスナーのVIPをバックエンド・サーバーのIPアドレスに変換する一方で、バックエンド・サーバーにトラフィックを転送する際には元のソースIPアドレスとポートの情報を保持します。この設定により、クライアントIPの可視性とセッションの永続性が維持されますが、これは特定のアプリケーションにとってきわめて重要です。

ただし、この構成では、戻りトラフィックがOCIネットワーク・ファイアウォールをバイパスするという重大な制限が生じます。ソース保持モードの場合、バックエンド・サーバーは、トラフィックをファイアウォール経由でルーティングするサブネット・ルート表ルールをバイパスするように構成されるためです。戻りトラフィックは、ファイアウォールを完全にバイパスして、ネットワーク・ロード・バランサに送られます。OCIネットワーク・ファイアウォールがセキュリティ・ポリシーを効果的に適用するには、インバウンドとアウトバウンド両方のトラフィックを検査する必要があります。このようなセキュリティ・ギャップがあるため、この設計は、包括的なトラフィック検査と施行を必要とするユース・ケースには適していません。

ネットワーク・ロード・バランサを使用したルーティング挿入のユース・ケースに関する前出の項で述べたように、現時点では特定のルーティング構成のみがサポートされています。OCIは、OCIネットワーク・ファイアウォール経由で送信元に戻す機能をサポートしていないため、本書発行の時点ではこの設計はサポート対象外と見なされます。

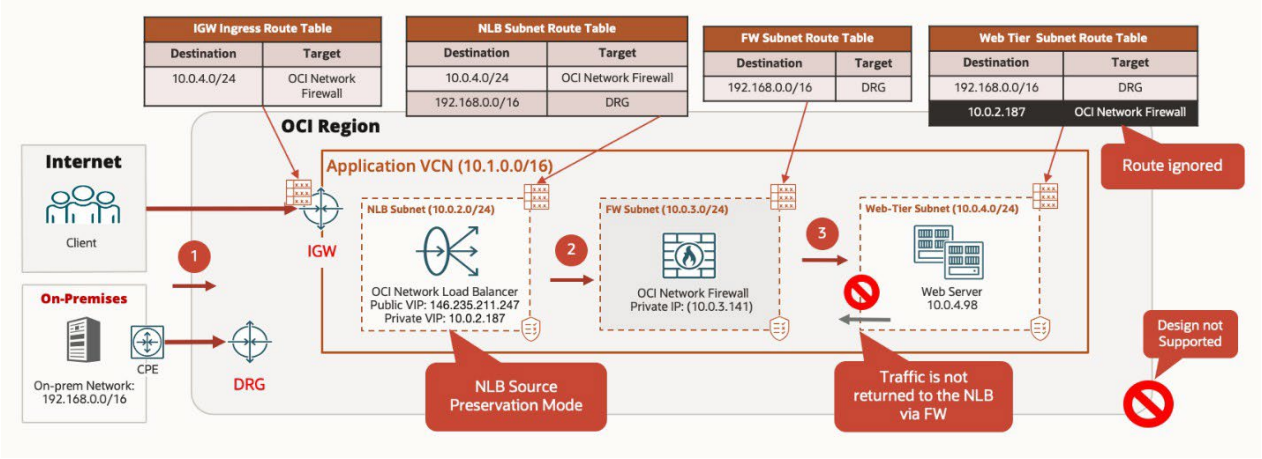

図21: ネットワーク・ロード・バランサのソース・ヘッダー(IPとポート)保持モードのトポロジ

ロード・バランサのOCIネットワーク・ファイアウォール・バックエンド

スケーラビリティ、パフォーマンス、高可用性を強化するために、OCIネットワーク・ファイアウォールをOCIネットワーク・ロード・バランサまたはOCIロード・バランサのバックエンド・セット内に配置することはサポートされていません。OCIネットワーク・ファイアウォールはネットワーク・ロード・バランサとロード・バランサのどちらのバックエンドとしても機能できないためです。この制限は、どちらのロード・バランサにも必須のOCIネットワーク・ファイアウォールによるヘルス・チェックがサポートされていないことに起因します。真の高可用性については、OCI Network Firewallサービスの組込みの高可用性機能について説明した、前出の「高可用性」の項を参照してください。この高可用性機能は、他のデプロイ済インフラストラクチャ(ロード・バランサなど)がなくてもシームレスなフェイルオーバーと信頼性を提供できるように設計されています。

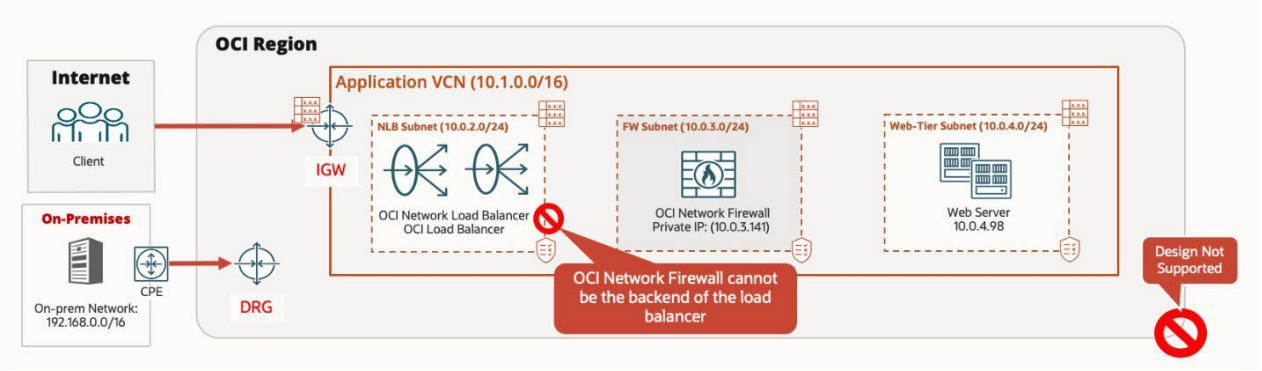

図22: ロード・バランサのOCIネットワーク・ファイアウォール・バックエンドのトポロジ

結論

OCI Network Firewallサービスは、クラウド環境の保護に不可欠な機能の堅牢なスイートを提供します。OCI Network Firewallサービスの高可用性、ステートフル・ネットワーク・フィルタリング、高度なセキュリティ対策(侵入検知やSSL検査など)を使用すれば、データとアプリケーションを効果的に保護できます。包括的なポリシー作成フレームワークにより、特定の運用ニーズを満たすカスタム構成が可能になるだけでなく、柔軟なルーティング挿入シナリオで既存のインフラストラクチャとのシームレスな統合が促進されます。これらの機能を理解し、活用することで、企業はセキュリティを強化し、クラウド・リソース全体で信頼性の高い接続を保証できます。この技術概要に集められた実際のネットワーク設計例は、OCI Network Firewallサービスのデプロイと管理の方法、および組織がOCI Network Firewallサービスを使用して最新クラウド・セキュリティの複雑さに自信を持って対処できるようにする方法について理解を深めたいと考えている方にとって、貴重なリソースとなります。

OCI Network Firewallと構成の詳細は、次のリソースを確認してください。

- OCI Network Firewallのクラウド・セキュリティ・サービス
- OCI Network Firewallのオンライン・ドキュメント
- OCI Network Firewallのリファレンス・アーキテクチャ
- Get Ready for Best-in-Class Security Built for Oracle Cloud Workloads
- Defense in Depth, Layering using OCI Network Firewall
- OCI Network Firewall: Unveiling policy model transformations and performance advances
- Announcing tunnel inspection for OCI Network Firewall
- Announcing Oracle Cloud Infrastructure Network Firewall
- Secure your workloads using Oracle Cloud Infrastructure Network Firewall Service
- Protect Websites and Applications with Oracle Cloud Infrastructure Network Firewall
- OCI Network Firewall - Concepts and Deployment
- OCI Network Firewall - NAT Gateway use case
- OCI Network Firewall - Hub and Spoke traffic inspection
- Use OCI Network Firewall for SSL forward proxy and inbound inspection using Decryption rule
- Using OCI Network Firewall for SSL decryption
- Create Fully Compatible JSON Templates from Custom PEM Certificates for OCI Network Firewall
- Learn Routing in Oracle Cloud Infrastructure Networking with Examples

Connect with us

+1.800.ORACLE1にお電話いただくか、**oracle.com**にアクセスしてください。北米以外のお客様は、**oracle.com/contact**でお近くの営業窓口を参照いただけます。

blogs.oracle.com facebook.com/oracle twitter.com/oracle