Learn OCI Network Firewall in Oracle Cloud Infrastructure with Examples

Troy Levin, Consulting Member of Technical Staff
January 2025, version 1.0

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Revision History

The following revisions have been made to this document.

DATE	REVISION
January 2025	Initial publication

Table of Contents

Introduction

The Oracle Cloud Infrastructure (OCI) Network Firewall service is a cornerstone of OCI's network security offering, designed to protect modern cloud workloads while ensuring seamless network functionality. Oracle has partnered with Palo Alto Networks to offer the OCI Network Firewall service, a cloud native, fully managed next-generation firewall service for protecting OCI workloads. OCI Network Firewall delivers a range of advanced security features, capabilities and seamlessly integrates with various native OCI services.

This technical paper provides an in-depth exploration of the OCI Network Firewall service, emphasizing its role in securing network traffic, detecting and preventing threats, and enforcing security policies. It highlights the core functionalities of the firewall with a focus on common design scenarios and use cases where the OCI network firewall enhances security within OCI cloud networks. Structured to guide network architects, security engineers, cloud administrators, and technical business decision-makers, the paper covers the firewall's capabilities and practical applications.

The guide begins with an overview of the firewall's features, showcasing the capabilities that make it a robust solution for cloud security. It then explores the creation of firewall policies, explaining how to utilize the policy model to define and implement rules that govern traffic flows and enhance security postures. Finally, the paper examines common routing scenarios for firewall insertion, demonstrating how to strategically place the firewall within different network architectures to maximize its effectiveness. The goal is to help readers implement the OCI network firewall effectively in their environments and fully utilize its potential for secure and efficient cloud operations.

The content presented is based on the capabilities and configurations available at the time of publishing. As OCI and the OCI Network Firewall service continue to evolve, new features and improvements are introduced that can affect the information provided. For up-to-date information, we encourage you to consult the OCI Network Firewall documentation because this document might require periodic updates so that it accurately reflects the most recent developments in the OCI Network Firewall service.

OCI Network Firewall Features Overview

This section provides a comprehensive overview of key firewall features that are essential for building a robust network security strategy. Understanding its core features is critical for effectively using the firewall to control traffic flow and enforce security policies. The firewall includes the following key features:

- **Stateful network filtering:** Dynamically monitors traffic to allow or block connections based on their state
- **Custom URL filtering:** Enables precise control over web traffic access
- **Intrusion detection and prevention:** Identifies and blocks threats in real-time
- **Secure Sockets Layer (SSL) inspection:** Decrypts and analyzes encrypted traffic to uncover hidden risks.

By grasping how these features work individually and together, you can better design security strategies that align with their specific needs. These features form the building blocks for creating policies that define and manage traffic behavior, from blocking unauthorized access to ensuring secure data flow across the network. With this foundational understanding, you can construct policies that translate these advanced capabilities into precise, actionable controls.

Stateful Network Filtering

Stateless rules evaluate each packet individually, focusing only on the header of a single packet traveling in one direction. No state information is retained. Because stateless rules involve less traffic processing, they offer better performance and scale. Stateful rules keep track of active connection state within the context of a complete communication flow retaining information about each packet, enabling the inspection of packet flows in both directions. This feature allows the system to make more informed decisions about whether to allow or block traffic.

OCI Networking provides both stateless and stateful security lists and network security groups (NSGs) for virtual cloud networks (VCNs), which you use to secure workloads. These security lists and NSGs follow an allow list model, permitting traffic based on defined protocols and ports while implicitly denying nonmatching traffic. However, you often require more scalable and flexible security solutions, especially as infrastructure grows.

With OCI Network Firewall, you can implement stateful filtering rules that either permit or block traffic based on IPv4, IPv6 source or destination address, protocol and port. The OCI Network Firewall strengthens your security posture with advanced stateful network filtering, making it ideal for enterprises requiring scalability and flexibility. It supports the creation of both allow lists and deny lists, offering greater control, scale and adaptability compared to service lists and NSGs, effectively addressing diverse and complex security requirements.

Stateful security rules track the state of network connections, such as transmission control protocol (TCP) sessions and user diagram protocol (UDP) flows, to allow or deny traffic based on connection context rather than individual packets. Client-to-server (c2s) and server-to-client (s2c) refer to the directions of data flow between a client-initiated flow and a server. The firewall monitors both c2s and s2c flows within each session, checking incoming packets against existing sessions and applying the original security policies. When defining policies, only the c2s direction is considered, simplifying configuration by focusing on incoming traffic to protected resources, while the s2c flow is automatically managed. This approach ensures efficient traffic filtering and connection tracking by monitoring details like IP addresses, ports, protocols, and sequence numbers.

When a session is established and packets arrive at the firewall, the traffic is initially allowed to pass through to determine the application type. The firewall processes the traffic according to the most permissive security rule, which is evaluated from top to bottom and left to right. If the traffic is incomplete or insufficient, it indicates that the application couldn’t be determined, or the TCP handshake didn’t complete successfully. Because the traffic was initially allowed to pass for application identification and no further processing occurred (as it was permitted), it appears as “allowed” in the traffic logs.

The firewall uses security rules to determine whether to allow or deny traffic. Each rule is based on parameters, such as source and destination IP addresses, service, port, and protocol (TCP or UDP). If the traffic matches a security rule, the firewall applies the corresponding action: Allow, drop, reject, intrusion detection or intrusion prevention. No further rules are processed. For TCP, the firewall tracks the three-way handshake and flags connections based on packet sequence numbers, TCP flags, and connection termination. For other stateless protocols like UDP, which are connectionless, the firewall tracks flows based on timing and communication patterns to approximate a session. Any traffic that doesn’t match a security rule and isn’t part of an established session is implicitly denied. For the action drop, the traffic is dropped silently, and no notification of reset is sent. If the action is rejected, for TCP, a reset is sent in both directions to client and server. For UDP, an ICMP Type 3 - Destination Unreachable, Code 13 - Communication Administratively Prohibited is sent to the client.

The session is only fully analyzed if routing is symmetrical, as required by the nature of stateful security rules. Incomplete sessions can’t protect against threats on asymmetrical paths because without a server response, application aspects can’t be identified.

Custom URL Filtering

Custom URL filtering on the OCI Network Firewall enables administrators to manage and monitor access to specific websites. Actions includes restricting inbound and outbound HTTP and HTTPS traffic to a predefined list of fully qualified domain names (FQDNs), with support for wildcards, subdomains, and custom URLs. Administrators can create custom URL lists to block or allow specific URLs or domains. By blocking access to restricted or nonwork-related sites, custom URL filtering enhances network security and enforces compliance with an organization’s acceptable use policies.

You can apply custom URL filtering to both clear text HTTP and encrypted HTTPS web traffic, enabling policy enforcement across the following scenarios:

- **Clear text HTTP transactions**: The URL filtering policy inspects the HTTP host and URL path headers in the client's request to enforce its rules.
- **Encrypted HTTPS transactions**: The policy examines the server name indication (SNI) field in the TLS client hello handshake to determine the URL, provided the TLS version is 1.2 or earlier. For TLS version after1.3, you can only use the SNI field if it's not encrypted.
- **Encrypted HTTPS matches policy decryption rule**: The URL filtering policy inspects the HTTP host and URL path headers in the decrypted request. The SNI field in the TLS client hello handshake is ignored.

Intrusion Detection and Prevention

Intrusion detection and intrusion prevention are two crucial security features in the OCI Network Firewall that help protect networks from malicious activities. The intrusion detection system (IDS) monitors network traffic and analyzes it for suspicious patterns or known threats, generating alerts when potential intrusions are detected; however, it does not take action to stop the threat. In contrast, an intrusion prevention system (IPS) not only detects suspicious activity but also actively blocks or mitigates threats in real time, preventing them from causing harm to the network. While IDS focuses on visibility and alerting, IPS emphasizes proactive defense and automated response. Together, they enhance the firewall's ability to safeguard the network. The OCI Network Firewall includes Palo Alto's industry-leading intrusion detection and prevention system that identifies and blocks malware, exploits of vulnerabilities, and command-and-control (C2) activities across all ports and protocols, which works for both encrypted and nonencrypted traffic.

The threat signatures that the OCI Network Firewall uses are classified into the following categories:

- **Antivirus:** Identifies different forms of malware and viruses, such as worms, trojans, and spyware downloads.
- **Antispyware**: Monitors compromised hosts for C2 spyware attempting to connect or beacon to an external C2 server.
- **Vulnerability:** Designed to detect and exploit system vulnerabilities.

The OCI Network Firewall service receives signature updates in the form of two update packages, the antivirus content and application and threats content updates. The packages are automatically updated as part of the service. The antivirus content updates include antivirus signatures and DNS (C2) signatures used by antivirus and antispyware security profiles, respectively. The application and threats content updates include vulnerability and antispyware signatures, used by the vulnerability and antispyware security profiles, respectively. Palo Alto provides a table of all possible signature categories by type—antivirus, spyware, and vulnerability—and content update (applications and threats or antivirus) that provides the signatures in each category. For more information, see their Threat Signature Categories documentation. With a free Palo LIVEcommunity account, you have access to Palo Alto's threat vault, a database that contains the latest threats, such as vulnerabilities, exploits, viruses, and spyware, that Palo Alto Networks next-generation firewalls can detect and prevent.

Each threat signature has an internal severity level and default action as defined in Palo Alto's threat vault. Every OCI Network Firewall includes predefined security profiles for antivirus, antispyware, and vulnerability protection, which are attached to either intrusion detection or prevention security policy rule actions. Security profiles work in conjunction with intrusion security policy rules to scan traffic flows for threats like viruses, malware, and spyware attacks and take actions based on security recommendations from OCI. When using IPS, the action is to block threats of severity level critical Medium or High. When using IDS, the action is to only send alerts to the OCI Network Firewall threat logs. The OCI Network Firewall contains threat logs for viewing both blocked and detected threats.

Intrusion detection and prevention system is enabled in the security policy when a security rule action is configured as Intrusion detection or intrusion prevention. The OCI Network Policy Building and Creation Overview section later in this document covers policy building, including intrusion detection and prevention. For more information on configuration of intrusion and detection, refer to the security rule section of the Create a Security Rule documentation.

Secure Sockets Layer (SSL) Inspection

SSL inspection on firewalls plays a crucial role in enhancing security by decrypting and inspecting encrypted traffic for both inbound and outbound communications. By using SSL certificates, firewalls can intercept and analyze encrypted data, identifying potential threats hidden within secure connections. For inbound traffic, SSL inspection ensures that incoming requests to internal servers are safe. For outbound traffic, it allows you to monitor and secure connections initiated by internal users or applications.

SSL and its successor, Transport Layer Security (TLS), are widely used to encrypt communications by encrypting data between clients and servers. Malicious actors can also exploit encryption to hide threats from conventional security measures. The OCI Network Firewall addresses this challenge through inbound and outbound SSL inspection, enabling you to decrypt, inspect, and reencrypt SSL traffic. This process helps ensure that encrypted communications are not a blind spot in an organization's security posture, providing enhanced visibility and protection against potential threats.

Both inbound and forward proxy SSL inspection are crucial for identifying threats hidden within SSL-encrypted traffic, all while maintaining the integrity and security of data. The main difference between SSL inbound inspection and forward proxy SSL inspection lies in the direction and purpose of the SSL traffic being inspected. This section provides an in-depth overview of both inbound and forward proxy SSL inspection, explaining the process to establish trust, decrypt, inspect, and reencrypt traffic securely.

To better understand how SSL inspection strengthens security, it is essential to examine its application in two critical contexts: inbound SSL inspection and forward proxy SSL inspection. Each approach addresses unique challenges in handling encrypted traffic, helping ensure comprehensive protection. The OCI Network Firewall is purpose-built for this capability, using its advanced SSL inspection features to provide seamless decryption, inspection, and reencryption of encrypted traffic, helping ensure robust security without compromising performance or data integrity. The following sections delve into these methods, highlighting their roles, processes, and the security benefits they bring to your network infrastructure.

This document uses the term SSL to refer to the concept of encrypting communication. When setting up a secure connection today, TLS is the more widely used protocol in use.

Inbound SSL Inspection

SSL inbound inspection refers to the decryption and inspection of SSL encrypted traffic that is entering a VCN destined for a resource, such as an instance or load balancer. It applies to traffic for FQDNs owned by a resource hosted within your VCN that has a valid SSL certificate with private key. The OCI Network Firewall focuses on decrypting traffic destined for internal servers, inspecting the data for potential vulnerabilities, threats, or malware before re-encrypting and delivering it to the internal destination. By decrypting the traffic, the firewall can apply security policies and help ensure that even encrypted connections are thoroughly inspected for any security risks. For inbound SSL inspection to function between the client, OCI Network Firewall, and server, the OCI Network Firewall must have the same SSL certificate with private key installed as is on the server.

The following scenario illustrates a typical OCI environment hosting a simple SSL encrypted web application exposed to external users through the FQDN `https://www.oracle.com` hosted in a public subnet. The firewall is positioned between the internet gateway and the public subnet, acting as a security layer for inbound traffic. Inbound traffic is routed through the OCI Network Firewall for security inspection. When an external user initiates an HTTPS request, the OCI Network Firewall inspects the inbound SSL by decrypting and inspecting the encrypted traffic. This step helps ensure that any malicious content or security threats are identified and mitigated before reaching the internal OCI web server, maintaining both privacy and security in the environment.

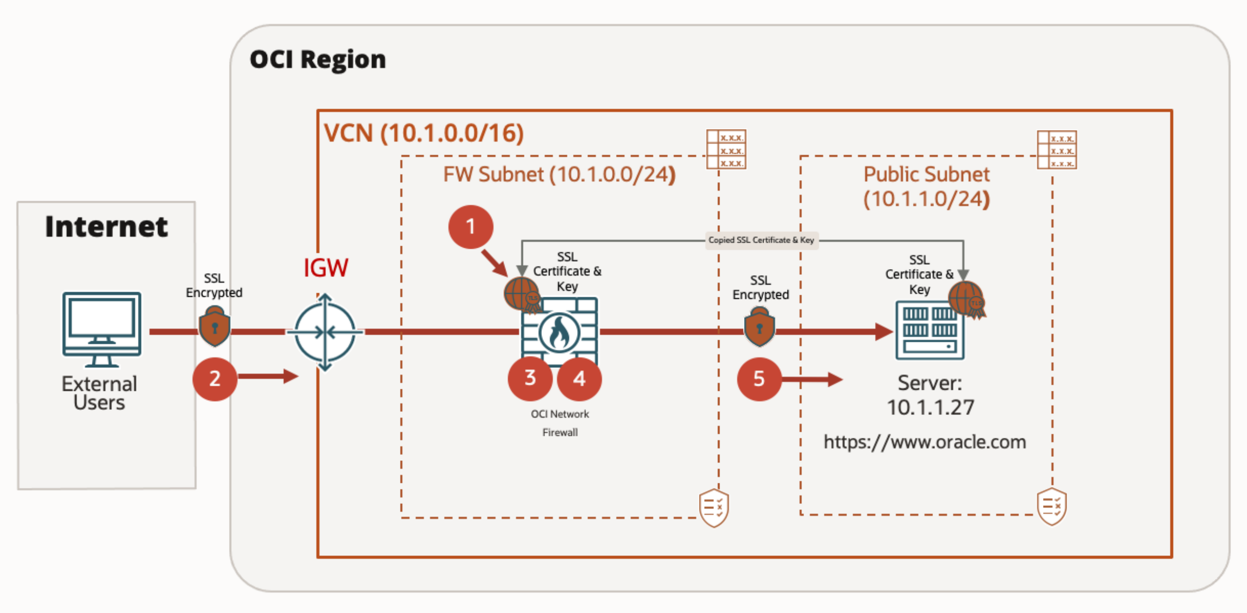


Figure 1: Topology for inbound SSL inspection

SSL inbound inspection moves through the following steps:

1. The administrator imports a copy of the protected server's certificate and private key using OCI Vault service.
2. An external client initiates an SSL session with the server, sends a request to the internal OCI site (`https://www.oracle.com`).
3. The traffic matches the decryption policy configured on the OCI Network Firewall.
4. The SSL Inspection Engine on the OCI Network Firewall intercepts the SSL session and, using the uploaded certificate key pair, decrypts the traffic.
5. If the inspected traffic is allowed by the policy, traffic is reencrypted and forwarded.

The initial SSL request as part of the SSL handshake is forwarded to the web server without being proxied. We don't change to the request. During the SSL handshake, the OCI Network Firewall inspects the server hello message to verify whether the certificate provided by the web server matches the one used in step 1. If the certificates match, the decryption process proceeds, allowing the rest of the session to be decrypted successfully. If the certificates don't match, the decryption fails. The server's return traffic is sent through the OCI Network firewall using the server subnet's route table, which contains a route rule with the next hop of the firewall.

Forward Proxy SSL Inspection

SSL forward proxy inspection refers to the decryption of encrypted traffic initiated by clients located within the VCN towards a server that can reside inside or outside of OCI. This process helps ensure that no malicious content is sent or received through encrypted channels, such as data exfiltration or malware downloads. The process allows the OCI Network Firewall to inspect outbound traffic for threats, enforcing security policies before reencrypting and sending the traffic to its destination.

Unlike the traditional client-server SSL handshake, in SSL forward proxy mode, the firewall acts as a mediator, intercepting communication between the client and server. The firewall terminates the SSL connection from the client and establishes a new connection to the server. To the server, the firewall appears as the client while, to the client, it appears as the server. For the firewall to function in mediator mode, it requires a different certificate than the one used for the inbound SSL inspection use case. This certificate is either a CA certificate issued by a certificate authority that the firewall can use to present to clients or a self-signed certificate imported into the firewall. Clients must trust the server certificate to avoid browser warnings and errors.

The following scenario illustrates a typical OCI environment. Forward proxy SSL inspection is configured to secure traffic originating from internal users accessing external websites. When a user in a subnet attempts to reach an external site, such as `https://www.oracle.com`, the traffic is first routed through the OCI Network Firewall, which acts as a proxy. The firewall intercepts the SSL traffic, decrypts it, and inspects the content for potential threats, such as malware or data exfiltration. When the inspection is complete, the firewall reencrypts the traffic and forwards it to the intended destination. This step helps ensure that sensitive data leaving the OCI environment is monitored for compliance and security while maintaining privacy through encryption during transit.

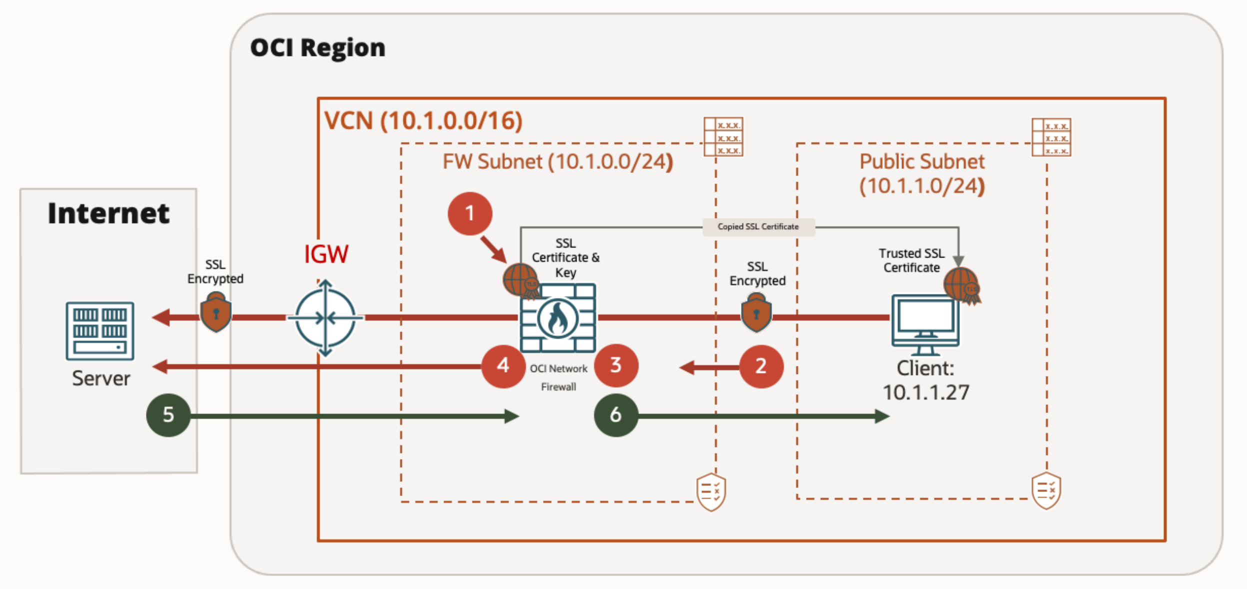


Figure 2: Topology for forward proxy SSL inspection

The SSL forward proxy inspection moves through the following steps:

1. The administrator imports a copy of a certificate issued by a certificate authority or a self-signed certificate and private key using the OCI Vault service.
2. The client initiates an SSL session with the server, sends request to `https://www.oracle.com`. The traffic matches the forward proxy SSL decryption policy configured on the OCI Network Firewall.
3. The SSLProxyEngine on the firewall intercepts the traffic and generates a certificate for `www.oracle.com` using the internal public key infrastructure (PKI), with the certificate signed by the CA certificate. For the client, the firewall appears as the external server, even though the secure session is established with the firewall rather than the real server.
4. The firewall sends the client's SSL certificate request to the server to initiate a separate session. From the server's perspective, the firewall appears to be the client, so the server is unaware of the mediator and proceeds to verify the certificate.
5. The server sends a signed certificate to the OCI Network Firewall intended for the client.
6. The firewall analyzes the server certificate. If the server certificate meets the policies and profiles you configure, the firewall generates an SSL copy of the server certificate and sends it to the client.

SSL Certificates

OCI Network Firewall seamlessly integrates with the OCI Vault service to securely store and manage SSL certificates for both inbound and forward SSL inspection. When utilizing SSL certificates with the network firewall, the service validates the provided certificate and stores it in the trust root for secure use during traffic decryption. To ensure successful validation, supply the complete SSL certificate chain, including all intermediate certificates, the root certificate, and the private key. Certificates must be uploaded in `.pem` format, wrapped within a predefined JSON template. Oracle has created a script to generate and convert the SSL certificate chain to the proper format. You can download it from the official Oracle GitHub repository. The following block is an example of an SSL certificate chain in JSON format:

```
{
"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"
 }
}
```

All SSL decryption use cases on the OCI Network Firewall have specific requirements related to certificates and attributes.

Inbound SSL Inspection SSL Certificates

SSL inbound inspection requires a public certificate and private key in the `certKeyPair`. In this case, the certificate authority (CA) flag doesn't need to be set to true.

To verify the CA flag in a certificate, use the following OpenSSL command to verify SSL inbound inspection certificate:

```
 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
```

The command has the following parameters:

- **Basic constraints**: `CA:FALSE` indicates that the certificate isn't allowed to issue other certificates. This characteristic is key in a leaf certificate.
- **Netscape cert type**: "SSL Server" indicates that the certificate is intended for use as an SSL server, which is typically the role of a leaf certificate.
- **X509v3 key usage**: This section shows `Digital Signature , Key Encipherment`, which is standard for a leaf certificate used in SSL for secure communication.

Forward Proxy SSL Inspection Certificates

SSL forward proxy SSL inspection requires a public certificate and private key in the `certKeyPair`, but the CA flag must be set to true, allowing the firewall to impersonate the certificate and decrypt outbound traffic. To verify the CA flag in a certificate, use the following OpenSSL command to verify the forward proxy SSL inspection certificate:

```
 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
```

The command has the following parameters:

- **Basic constraints**: `CA:TRUE`, which means that this certificate can act as a CA and issue other certificates. The `pathlen:0` indicates that it can only issue leaf certificates, not other intermediate certificates. This setting is typical for an intermediate certificate.
- **X509v3 key usage**: Includes `Certificate Sign`, which is required for a certificate that signs other certificates, another indication that this is an intermediate certificate

This process helps ensure that the certificates are properly configured to support the SSL inspection use cases on the OCI Network Firewall.

High Availability

The final topic covered in the feature overview is high availability, which is essential for cloud services to provide uninterrupted operation, minimize downtime, reduce data loss, and maintain business continuity. High availability for the OCI Network Firewall service is built-in and implicit to the service. It’s inherently highly available, horizontally scalable, and fault-tolerant, so you don’t need to manually configure high availability by adding more infrastructure, such as a load balancer, or complex configuration. You can choose between two deployment scope options when launching the OCI network firewall: either as a regional deployment across multiple availability domains or within a single availability domain across fault domains. Regional is the recommended and default option for critical applications and ensures continuous protection, even in the event of one or more availability domain failures. Availability domain-specific provides redundancy across one or more fault domains within a single availability domain and is useful for applications that require a combination of high availability and low latency. You can gain this benefit without the need for more infrastructure or complex configuration.

You can find high-availability configurations in the Advanced Options section of the Create Network Firewall workflow. For more information on configuration of high availability, refer to the firewall creation section of our Create a Firewall documentation.

In the next section, we build on this knowledge, exploring how to design and implement effective network policies to maximize the value of OCI Network Firewall’s robust feature set. This progression helps ensure a seamless transition from understanding the tools to applying them for real-world security and traffic management.

OCI Network Policy Building and Firewall Overview

Network policies are the backbone of any effective security strategy, enabling you to safeguard workloads, enforce compliance, and control the flow of traffic in a structured and predictable way. Policies are essential in helping ensure that only authorized traffic traverses your network while blocking potentially malicious or unauthorized activity. They're also critical for meeting regulatory requirements by defining clear, enforceable rules for data handling and access.

A well-constructed policy consists of several key components, including rules (specific conditions for allowing or denying traffic), conditions (criteria such as IP addresses, services, applications, and URLs), and actions (the result of matching traffic to a rule, such as permit or block). These elements work together to provide granular control over network traffic.

This structured approach to policy building helps ensure that security rules are both actionable and aligned with the firewall's capabilities. By first understanding the importance of policies and their components, you can effectively achieve a secure, compliant, and well-managed cloud environment. For detailed information on OCI Network Firewall's scale, limits, and recent advancements in policy model transformations and performance, refer to the blog post, OCI Network Firewall: Unveiling Policy Model Transformations and Performance Advances.

In this section, we walk through the essentials of policy creation and explore a real-world application to demonstrate how these policies protect and optimize network traffic flows.

Applications

Applications in OCI Network Firewall allow for advanced traffic control by using Layer-7 inspection to identify and classify traffic based on application behavior and protocols, instead of solely relying on ports or IP addresses. This capability provides precise control and enhanced security for modern network environments.

The firewall identifies applications by analyzing traffic patterns and behaviors. Applications are defined by their unique signatures, which represent the specific protocols and behaviors associated with the application. Unlike port-based filtering, applications are recognized by their intrinsic properties, ensuring better detection accuracy. This approach gives the firewall the following capabilities:

- Perform Layer-7 inspection to analyze traffic at the application layer.
- Detect and classify applications accurately, even when multiple applications share the same port or protocol.

Applications can be characterized by the following parameters:

- **Name**: A unique identifier for the service.
- **Protocol**: ICMP or ICMPv6
- **ICMP type:** 0-Echo reply, 3-Destination unreachable, 5-Redirect, 8-Echo.
- **ICMP code:** Used when you select ICMP. 0-Net unreachable, 1-Host unreachable, 2-Protocol unreachable, 3-Port unreachable

Applications are organized into application lists, collections of defined applications that you can find in firewall policy rules. These lists enable precise control over network traffic based on the application itself.

Applications in OCI Network Firewall enable granular, behavior-based traffic control that goes beyond traditional port and protocol filtering. By using Layer-7 inspection, applications provide precise, adaptable, and secure management of network traffic, making them indispensable for modern application-driven cloud environments.

Currently, the OCI Network Firewall supports ICMP and ICMPv6 applications, with plans to add more types. For recent enhancements to applications, consult the OCI Network Firewall documentation.

Services

Services in the OCI Network Firewall define specific network protocols or applications by their associated Layer-4 port. A service represents a specific network protocol or application, characterized by the following factors:

- **Name**: A unique identifier for the service.
- **Protocol**: TCP or UDP.
- **Ports**: Defined by a specific port number, such as 1433, or a range, such as 80–8080.

Each service can include up to 10 port ranges, allowing for flexibility in representing applications that use multiple ports. Services can be created individually or imported in bulk using a JSON file, streamlining setup for complex configurations. This modular approach simplifies management by enabling reusable definitions across similar rules in a policy.

After creation, services are organized into service lists, which serve as collections of services within the same firewall policy. These lists are then referenced in policy rules for the following actions:

- Permit or deny specific traffic.
- Ensure compliance with organizational security requirements.
- Enhance readability and reusability of firewall rules.

You can include a service called Web-Services with a port 443 in a rule to allow HTTPS traffic. If another application requires similar rules, you can reuse the same service list, maintaining consistency.

Services in OCI Network Firewall enable efficient traffic control by abstracting Layer-4 protocol and port configurations into reusable entities. Integrating services into firewall policies enhances manageability, enforces security, and helps ensure scalability for dynamic cloud environments.

For importing multiple applications or services using a JSON file, refer to Bulk Import Firewall Policy Components.

Lists

Lists are reusable components of an OCI Network Firewall policy that allow you to group addresses, applications, services, or URLs for use in a security rule. All items in a list are treated the same way when applied in a rule. For example, to block access to known malicious websites, you can create a URL list called "Malicious URLs" and apply a rule that denies access to the entire list at the same time.

The OCI firewall supports various types of lists, such as IP address lists, application lists, and more. Use the following list types for effective traffic management and security:

- **IP address lists**: IP Address lists are used to create a list of IPv4 addresses and IPv6 addresses for use in building firewall policy rules. You can include individual IPv4 or IPv6 addresses, CIDR blocks, or a combination of both within the IP address list.
- **Application lists**: Application lists are used to select and group the applications you created. Create application lists to control traffic for groups of applications, either allowing or blocking them.
- **Service lists:** Use service lists to select and group the services you want to include in a service list. Create a list of services that you can use to build rules in a firewall policy. Service lists enable you to allow or block traffic for groups of services. Each service is identified by its port-based signature, and Layer-4 inspection is used to match these services.

URL Lists

URL filtering is a crucial security feature that allows administrators to control and monitor access to websites based on their URLs. This functionality enables you to enforce policies that either block or allow specific web traffic, strengthening security, and ensuring compliance with internal guidelines. For the OCI firewall, URL lists serve as a tool for organizing and managing URLs, streamlining the filtering process and making it more efficient and scalable. The following section outlines how URL lists are configured and applied to fine-tune URL filtering, providing greater control over web traffic.

Administrators can set up URL lists to either allow or deny access to specific groups of URLs. To configure these lists, each URL should be entered on a separate line, with the option to use wildcards, such as asterisks (*) and carets (^), for customized matching. When specifying URLs, omit protocol information, such as "http://" and "https://."

Wildcard matching in URL filtering provides administrators with the flexibility to create broad rules that block or allow traffic to specific FQDNs without needing to account for every possible variation of a domain. This approach simplifies the management of filtering policies, especially when dealing with large, dynamic, or unpredictable domain structures.

Certain characters are supported in the hostname portion of a URL, including letters, numbers, and special symbols like periods, underscores, tildes (~), and various punctuation marks. These characters are used to form valid URL components, allowing precise filtering.

Specific characters function as token separators within URLs, including periods, slashes, question marks, ampersands, equals signs, semicolons, and plus signs. Token separators help define distinct segments of a URL, making it easier for parsers to interpret and manage each part of the URL's structure effectively.

- **Asterisk**: The asterisk symbol (*) represents any number of characters, including none. It can be used to match entire domains, subdomains, or paths.
- **Caret**: The caret symbol (^) serves to match single-level subdomains only.

The following examples show how various wildcard filter combinations match and don't match websites according to current expected behavior:

- ***.oracle.com**: Matches blog1.blog2.oracle.com.au.us and matches blog1.oracle.com. Without the / character, an implicit * is at the end.
- **^.oracle.com/**: Matches blog.oracle.com but doesn't match oracle.com or other.blog.oracle.com.
- **oracle.^:** Matches any website on the right. Matches oracle.com, oracle.com.au, oracle.com.au.us.
- **oracle.^.au/**: Matches only oracle.com.au and oracle.uk.au but doesn't match oracle.com or oracle.com.au.website.info.
- ***.oracle.com/**: Matches blog1.blog2.oracle.com but doesn't match oracle.com or blog.oracle.com.au.
- ***.oracle.com.***: Matches blog1.blog2.oracle.com.au.us and doesn't match blog1.oracle.com.
- **oracle.com**: Matches oracle.com.au and oracle.com.au.website and oracle.com.
- **oracle.com/**: Matches only oracle.com.

Subpages can match by filter only if decryption is enabled for specific URLs. Without decryption, URL filtering is limited to broad domain-level rules, such as blocking or allowing all traffic to xyz.com. Consider the following examples:

- **oracle.com/***: Match oracle.com/word1 and oracle.com/word2.
- **oracle.com/word.**: Only matches oracle.com/word.

For importing multiple service and URL lists using a JSON file, see Bulk Import Firewall Policy Components.

Rules

Rules are at the heart of the OCI Network Firewall's functionality, defining how network traffic is managed, inspected, and secured. These rules enable you to enforce precise controls over traffic flows, helping ensure that only authorized data traverses the network while potential threats or unauthorized access attempts are blocked.

When traffic matches a rule, the OCI Network Firewall enforces the specified action, such as allowing, blocking, or inspecting the session, based on the rule's parameters. Security rules deliver the following benefits:

- **Enhanced visibility**: By inspecting traffic based on detailed parameters, administrators gain deep insights into network activity.
- **Granular control**: Rules allow precise management of specific traffic flows, reducing the risk of unauthorized access.
- **Customizable policies**: You can tailor rules to match your security requirements, ensuring both compliance and efficiency.

OCI Network Firewall supports the following primary types of security rules, each serving a distinct purpose:

- **Decryption rules:** Decryption rules are essential for managing encrypted traffic, enabling the firewall to decrypt and inspect SSL/TLS communications for threats or policy violations. This capability enhances visibility into secure communications, which are often used to conceal malicious activities. Decryption rules allow administrators to inspect SSL inbound or forward proxy traffic, ensuring that secure communications are compliant with organizational policies while protecting sensitive data. For steps to set up certificate authentication, create a mapped secret, decryption profile and decryption rules, see the Create a Decryption Rule documentation.
- **Security rules:** Security rules define the core access control policies that allow, block, or inspect traffic. These rules are based on parameters, such as IP addresses, ports, protocols, and URLs. Before creating a security rule, you must set up key components like application lists, service lists, address lists, and URL lists. These lists categorize the specific entities that the security rules manage, enabling detailed and efficient policy configuration.
- **Tunnel inspection rules**: Tunnel inspection rules are specifically designed for analyzing traffic within VXLAN-encapsulated clear-text tunnels. These rules help enforce security policies on encapsulated data, ensuring compliance and detecting potential threats hidden within tunnel traffic. You can learn more about this use case in the blog post, Announcing tunnel inspection for OCI Network Firewall.

By understanding and implementing these rule types, you can effectively manage network security, ensuring that traffic flows align with their policies while maintaining high visibility and robust threat protection. For detailed instructions on configuring decryption, security, and tunnel inspection rules, refer to the Firewall Policy Rules documentation.

Rules Order of Operations

Traffic evaluation for OCI Network Firewall is a multilayered process. The OCI network firewall processes traffic through a structured order of operations that involves three primary types of security rules: decryption, security, and tunnel inspection. This evaluation occurs at multiple stages as the traffic moves through the following layers of inspection:

1. During session setup and presession enforcement, the firewall first evaluates Layer-3–Layer-4 conditions against existing security rules, which checks for actions based on the 5-tuple (source and destination IP, source and destination port, and protocol) to quickly rule out known threats and avoid unnecessary further processing, such as blocking known IPs.
2. Traffic undergoes app ID and content ID inspection to determine the application type and content, respectively.
3. If the application is SSL-based the firewall then checks whether decryption rules are in place, performing any necessary actions before reevaluating it for app ID and content ID inspection.
4. The firewall then reevaluates the traffic against existing security rules.
5. If the application is a VXLAN tunnel, the firewall applies tunnel inspection rules to evaluate the traffic further. If a matching tunnel inspection rule exists, the firewall inspects the inner packet and evaluates the traffic against existing security rules.

Consider the following important details about how rules operate:

- Rules are optional, but if the policy that you use with a firewall doesn’t have at least one rule specified, the firewall denies all network traffic.
- Rule evaluation is sequential, meaning the firewall processes rules from top to bottom. This approach helps ensures that the most specific rule is applied first, meaning that when a rule is matched, no other rules are further evaluated. By default, each new rule that you create becomes the first in the priority list from top to bottom. You can change the priority order at any time.
- Tunnel Inspection rules can’t be combined with decryption rules.

Mapped Secrets and Decryption Profiles

When implementing SSL decryption with OCI Network Firewall, mapped secrets and decryption profiles play a critical role in ensuring secure and effective traffic inspection. SSL decryption allows the firewall to analyze encrypted traffic for potential threats or policy violations, which is essential in today’s security landscape where malicious activity is often hidden within encrypted connections.

Mapped secrets are a key component of SSL decryption. These secrets, created and managed in the OCI Vault service, link to the SSL keys required for inbound or forward proxy decryption. By enabling the firewall to access these keys securely, mapped secrets allow for the decryption and inspection of encrypted traffic in scenarios, such as SSL forward proxy for outbound traffic or SSL inbound inspection for incoming traffic. Properly configuring these secrets ensures the firewall can securely decrypt traffic without compromising the integrity of sensitive data.

Decryption profiles define how SSL decryption is performed and enforce the security standards that SSL sessions must meet before traffic is allowed to pass. These profiles handle critical checks, including the following example:

- **Certificate validity**: Helps ensure that SSL certificates are valid and issued by trusted authorities.
- **Session configuration**: Verifies that SSL session parameters meet organizational security policies.
- **Failure actions**: Specifies actions when certificates fail validation, such as blocking the connection or alerting administrators.

By using decryption profiles, administrators can enforce strict security criteria, blocking insecure or noncompliant SSL connections to prevent vulnerabilities from entering the network. This precision enhances the overall security posture while allowing legitimate traffic to flow. For a detailed overview of the options available for configuring SSL forward proxy and inbound decryption profiles, refer to the Mapped Secrets and Decryption Profiles section of the Firewall Policy Rules documentation.

Policy Building Example

This section expands on the previous topic of policy building, showing how to use the Terraform OCI provider to create a network firewall policy that inspects HTTPS traffic. For this hypothetical real-world use case, employees rely on a cloud-based productivity and collaboration application accessed over HTTPS. While HTTPS ensures encrypted communication, it can also conceal the following threats:

- Phishing attempts
- Malware distribution
- Unauthorized data exfiltration

To address these risks, the policy is designed is configured to decrypt and inspect HTTPS traffic, ensuring that only authorized and safe access to the application.

The Terraform configuration defines the following resources to build the policy: IP address lists, URL lists, a service and service list, a decryption profile, and rule for HTTPS traffic. Finally, it configures a security rule to inspect HTTPS traffic, allowing only authorized access. The policy example provides a baseline for securing web applications against threats while maintaining organizational security standards.

The following code block shows a simplified Terraform configuration:

```
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
    }
}
```

To create a firewall, you need at least one associated firewall policy. Each firewall is linked to a single firewall policy, but a single firewall policy can be associated with multiple firewalls. For detailed instructions for creating a firewall and associating a policy to it, see the Overview of Creating a Firewall documentation.

Routing Use Cases for OCI Network Firewall Insertion Scenarios

In OCI, the integration of the OCI Network Firewall service is crucial for enhancing security and traffic management within VCNs. Firewall insertion allows you to seamlessly integrate network security into your cloud architecture, ensuring that all incoming and outgoing traffic is inspected and filtered according to predefined security policies. This process is facilitated through specific routing configurations that direct traffic to and from the OCI network firewall.

When a VCN is configured to use a network firewall, the routing tables must be meticulously designed to ensure that traffic flows through the firewall before reaching its destination. This process involves configuring route rules that point to the firewall as the next hop for specific traffic flows, enabling inspection, logging, and application of security policies. By strategically inserting firewalls into the routing path, you can effectively monitor, control, and protect your cloud environments against a range of cyber threats, while maintaining high availability and performance standards.

In this section, we explore various scenarios for firewall insertion within OCI, including the routing configurations required for effective traffic management, the benefits of using the OCI network firewall, and best practice designs for optimizing security posture through intelligent routing strategies.

You can deploy the OCI Network Firewall in either a public or private subnet, receiving only a private IP address in both cases. It integrates as a "bump in the wire" within the traffic routing path to perform more security processing before the traffic reaches its destination. In this setup, traffic is directed to the OCI network firewall by setting its private IP as the target for a destination CIDR as a route rule for VCN and subnet route tables. The OCI Network Firewall's subnet route table then forwards traffic onto its destination. Two essential VCN routing features support this process: Intra-VCN routing and VCN gateway ingress routing. To learn more about VCN routing in OCI, refer to Learn Routing in Oracle Cloud Infrastructure Networking with Examples, which describes VCN routing including Intra-VCN routing and VCN gateway ingress routing in detail along with scenarios.

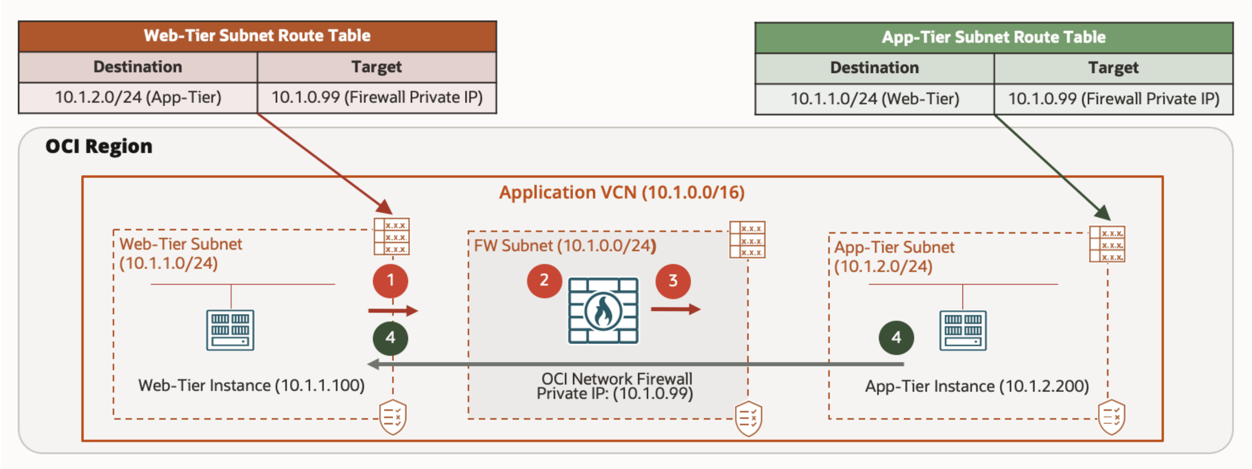
The following sections describe common VCN routing scenarios supported when inserting the OCI network firewall into the topology.

For better performance, Oracle recommends that you don’t add stateful rules to the security list attached to the firewall subnet or include the firewall in an NSG containing stateful rules.

Security list and NSG rules associated with the firewall subnet and virtual network interface cards (VNICs) are evaluated before the firewall. Ensure that any security list or NSG rules allow the traffic to enter the firewall so that it can be evaluated appropriately.

Routing Use Case for OCI Network Firewall Insertion with Intra-VCN Routing

The following scenario illustrates the intra-VCN routing design used to position the OCI network firewall between subnets within the same VCN. The following diagram shows an example where an OCI network firewall is placed between the web tier and app tier subnets of an application in the same VCN. Intra-VCN subnet route rules are defined in both subnet route tables to ensure that traffic in both directions is routed through the OCI network firewall, preventing it from reaching the destination directly.



Web-Tier Subnet Route Table	
Destination	Target
10.1.2.0/24 (App-Tier)	10.1.0.99 (Firewall Private IP)

App-Tier Subnet Route Table	
Destination	Target
10.1.1.0/24 (Web-Tier)	10.1.0.99 (Firewall Private IP)

OCI Region
Application VCN (10.1.0.0/16)
Web-Tier Subnet (10.1.1.0/24)
FW Subnet (10.1.0.0/24)
App-Tier Subnet (10.1.2.0/24)
1
2
3
4
4
Web-Tier Instance (10.1.1.100)
OCI Network Firewall Private IP: (10.1.0.99)
App-Tier Instance (10.1.2.200)

Figure 3: The flow of intra-VCN subnet routing to the OCI network firewall and destination. The red table indicates ingress route rules towards the destination and green tables indicate egress route rule towards for return traffic to the source.

The traffic flow moves through the following steps:

1. Traffic originating from the source 10.1.1.100 within the web tier subnet is directed to the private IP address 10.1.0.99 of the OCI network firewall using its subnet route table entry.
2. The OCI network firewall permits or denies the traffic based on the configured security policies.
3. If the traffic is permitted, the OCI network firewall forwards the traffic to the destination 10.1.2.200 using its subnet route table.
4. Return traffic follows the same path, passing through the OCI network firewall before being routed back to the source 10.1.1.100.

OCI routing employs longest prefix match to make forwarding decisions. Be careful when using a static default route of 0.0.0.0/0. You must ensure that the static default route is *not* less specific than any existing routes contained in the subnet route table used for routing between subnets within a VCN.

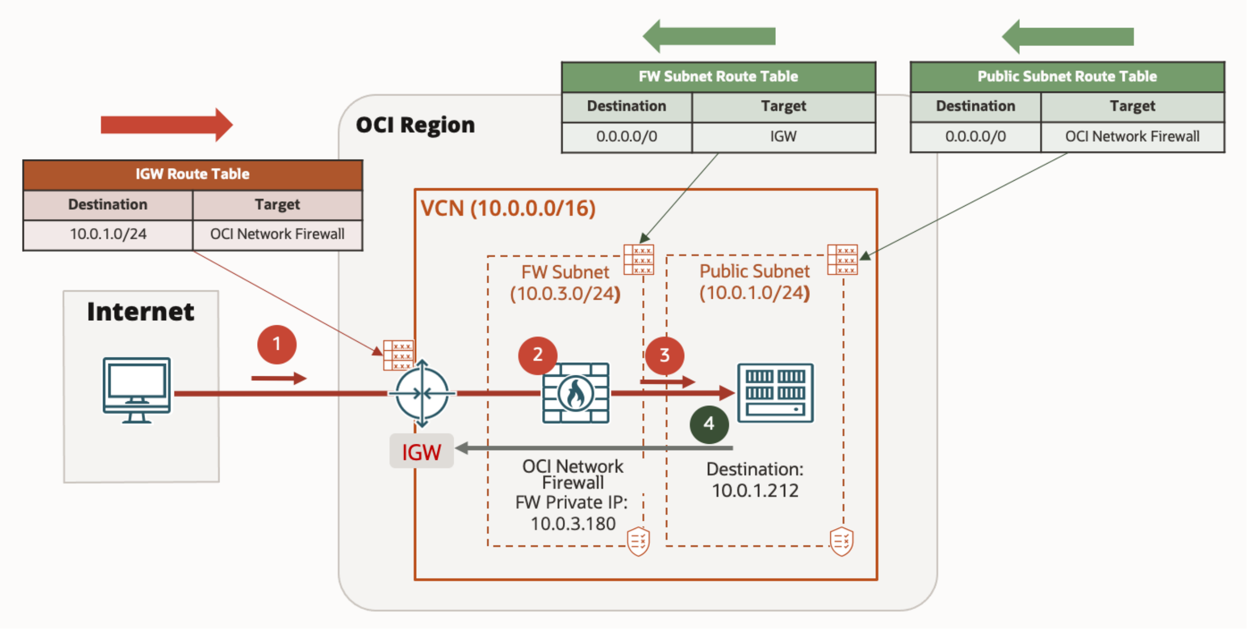
Routing Use Case for OCI Network Firewall Insertion with OCI Gateways

In OCI, several gateway types play crucial roles in facilitating network communication and securing traffic. The internet gateway enables direct internet connectivity for public subnets, making it a common insertion point for inbound and outbound traffic inspection. NAT gateways allow instances in private subnets to initiate outbound traffic without exposing themselves to the internet. Dynamic routing gateways (DRGs) are central to hybrid and multi-cloud connectivity, routing traffic between VCNs, on-premises networks, and OCI. OCI local peering gateways (LPGs) provide a traditional method for connecting VCNs within the same region with less flexibility and scale as compared to DRGs. Service gateways provide a secure path for private access to Oracle services without internet traversal. Each of these gateways work in conjunction with the OCI Network Firewall to enhance security and visibility across various network scenarios, enabling fine-grained traffic control and protection.

Internet Gateway Sends the Traffic to the OCI Network Firewall Instead of the Destination Within the Same VCN

In this use case, the OCI network firewall works in conjunction with an OCI internet gateway to enhance security for inbound and outbound traffic. To ensure that the OCI network firewall can inspect the traffic, the internet gateway is associated with an ingress route table that must be configured with a forwarding rule that sends traffic to the private IP address of the OCI network firewall. When the traffic reaches the OCI network firewall, it's processed according to the firewall's security policies, such as inspecting for threats, enforcing access controls, or applying any other configured rules. After the firewall processes the traffic, it forwards it to the destination, ensuring that only traffic that meets the security criteria is allowed through.

On the receiving end, the destination subnet in the VCN utilizes its own route table to forward the return traffic. Configure the subnet route table to include a forwarding rule for the return traffic to be sent to the private IP address of the OCI network firewall. This approach not only secures outbound traffic but also centralizes security management, ensuring that all traffic passing through the internet gateway is subject to OCI network firewall policies before being forwarded to the internet.



IGW Route Table	
Destination	Target
10.0.1.0/24	OCI Network Firewall

FW Subnet Route Table	
Destination	Target
0.0.0.0/0	IGW

Public Subnet Route Table	
Destination	Target
0.0.0.0/0	OCI Network Firewall

Figure 4: The flow of inbound traffic from the internet gateway to the OCI network firewall and destination. The red table and lines indicate ingress route rules and traffic flow toward the destination, and the green tables and lines indicate route rules and flow for return traffic to the source.

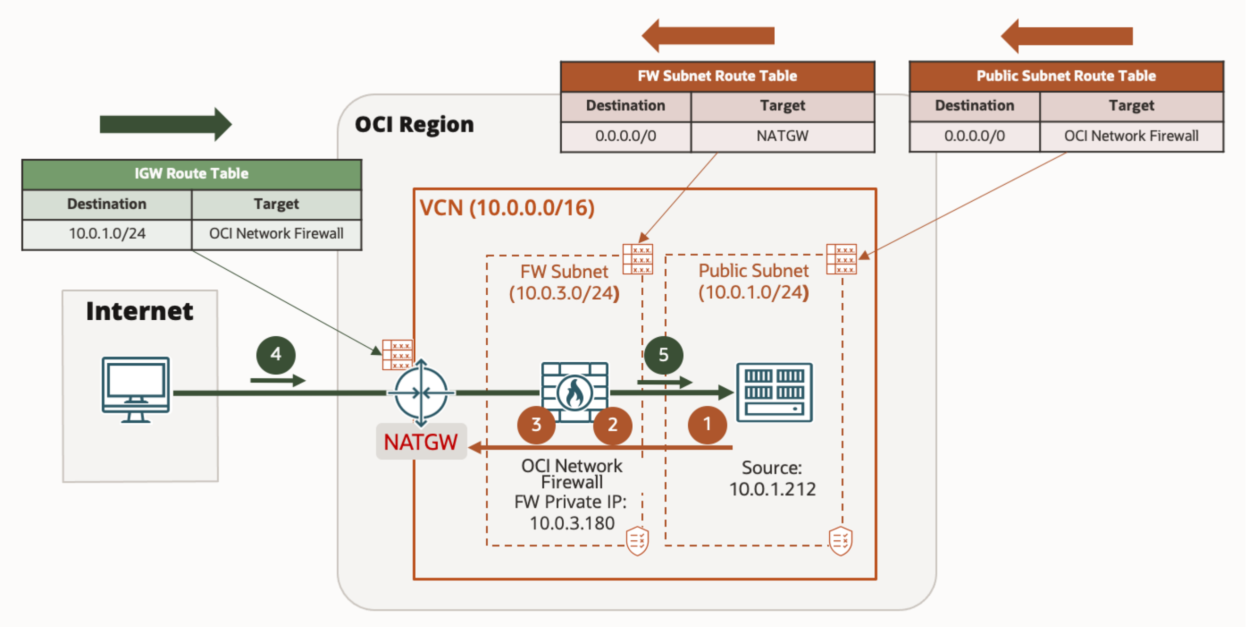
The traffic flow moves through the following steps:

1. Traffic originating from the internet source arriving at the internet gateway is forwarded to the private IP address 10.0.3.180 of the OCI network firewall using its ingress route table entry.
2. The OCI network firewall permits or denies the traffic based on the configured security policies.
3. If the traffic is permitted, the OCI network firewall forwards the traffic to the destination 10.0.1.212 using its subnet route table.
4. Return traffic follows the same path, passing through the OCI network firewall before being routed back to the source on the internet.

NAT Gateway Sends the Traffic to the OCI Network Firewall Instead of the Destination Within the Same VCN

In this use case, the OCI network firewall works in conjunction with an OCI network address translation (NAT) gateway to enhance security for outbound traffic originating from private subnets. To ensure that the OCI network firewall can inspect the return traffic, the NAT gateway is associated with an ingress route table that must be configured with a forwarding rule directing traffic to the private IP address of the OCI network firewall.

When the traffic reaches the OCI network firewall, it's processed according to the firewall's security policies, such as inspecting for threats, enforcing access controls, or applying other configured rules. After the firewall processes the traffic, it forwards it to the destination, ensuring that only traffic that meets the security criteria is allowed through. For return traffic, the destination subnet within the VCN uses its route table to direct it back to the OCI network firewall, ensuring continuous inspection. This approach secures outbound traffic while centralizing security management, making sure that all traffic routed through the NAT gateway adheres to OCI Network Firewall policies before exiting the VCN.



FW Subnet Route Table

Destination	Target
0.0.0.0/0	NATGW

Public Subnet Route Table

Destination	Target
0.0.0.0/0	OCI Network Firewall

IGW Route Table

Destination	Target
10.0.1.0/24	OCI Network Firewall

Figure 5: The flow of return traffic from the NAT gateway to the OCI network firewall and destination. The green table and line indicate ingress route rules and traffic flow for return traffic to the source, and the red tables and lines indicate route rules and initiated flow toward the destination.

The traffic flow moves through the following steps:

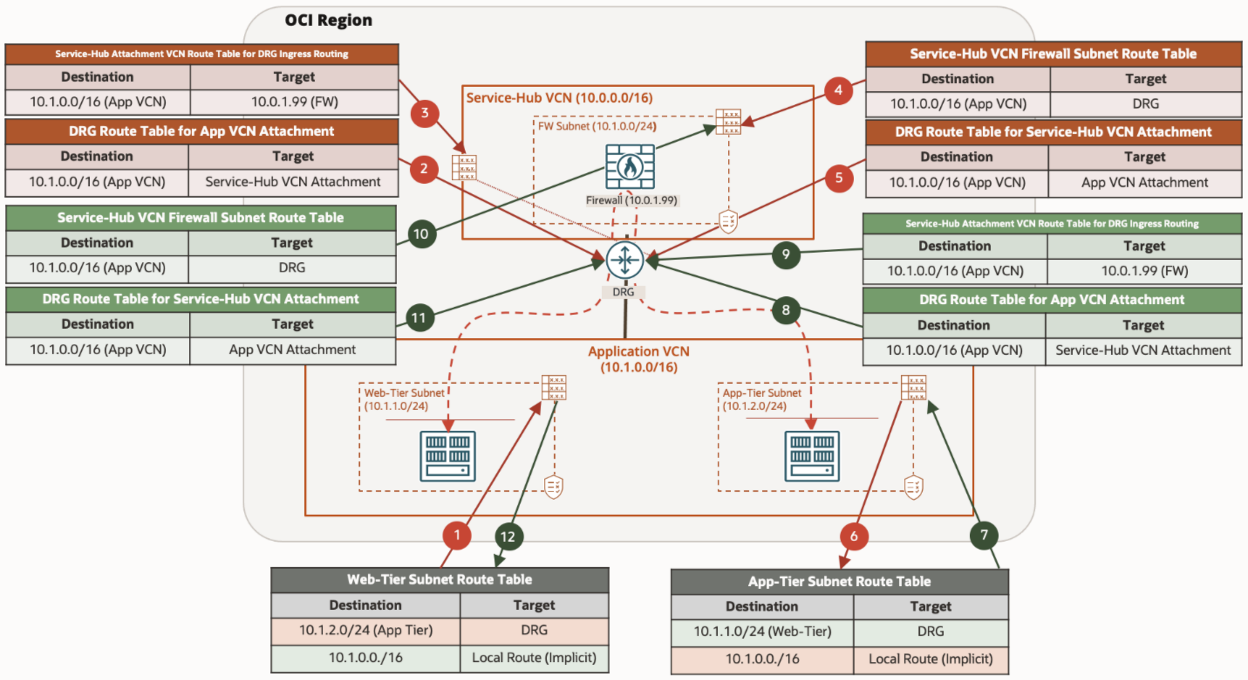
1. Traffic originating from the OCI client is forwarded to the private IP address 10.0.3.180 of the OCI network firewall using its subnet route table entry.
2. The OCI network firewall permits or denies the traffic based on the configured security policies.
3. If the traffic is permitted, the OCI network firewall forwards the traffic to the NAT gateway using its subnet route table entry.
4. Return traffic arriving at the NAT gateway is forwarded to the private IP address 10.0.3.180 of the OCI Network Firewall using its ingress route table entry.
5. The OCI network firewall forwards the traffic to the destination 10.0.1.212 using its subnet route table.

Intra-Region Routing Through a Centrally Shared VCN and OCI Network Firewall Using a DRG

Intra-regional VCN routing involves routing traffic between network resources located in different VCNs within the same region. It refers to inter-VCN routing within a region. Using a DRG for inter-VCN connectivity within a region is the recommended approach for its simplicity and scalability.

You can deploy an OCI network firewall in a central service hub VCN, with applications distributed across multiple spoke VCNs that share the centralized firewall. This approach is often seen as more cost-effective and operationally simpler, as it requires only a single firewall deployment. In this design scenario, the service hub VCN and the application spoke VCNs are connected through a DRG. The web tier and app tier of the application are placed in two subnets within the same VCN. Intra-VCN subnet route rules are configured between the two subnets, using the DRG as the target. The DRG routes application traffic to the OCI network firewall in the service hub VCN for inspection. This configuration helps ensure that all traffic between the web and app tiers is inspected by the centralized OCI network firewall, maintaining consistent security policy enforcement across multiple VCNs while simplifying the overall architecture.

The following diagram shows a centralized OCI network firewall deployed within a service hub VCN, where multiple spoke VCNs share access to the firewall. This setup is designed to route traffic from the web tier in each application VCN to the firewall in the service hub VCN for inspection before it reaches the app tier in the same VCN. The diagram highlights both the forward routing path (from the web tier through the firewall to the app tier) and the reverse routing path, which enables responses to follow the same route back. Additionally, intra-VCN subnet routing between the web and app tiers uses the DRG as a target to maintain seamless connectivity.



Service-Hub Attachment VCN Route Table for DRG Ingress Routing

Destination	Target
10.1.0.0/16 (App VCN)	10.0.1.99 (FW)

DRG Route Table for App VCN Attachment

Destination	Target
10.1.0.0/16 (App VCN)	Service-Hub VCN Attachment

Service-Hub VCN Firewall Subnet Route Table

Destination	Target
10.1.0.0/16 (App VCN)	DRG

DRG Route Table for Service-Hub VCN Attachment

Destination	Target
10.1.0.0/16 (App VCN)	App VCN Attachment

Service-Hub VCN Firewall Subnet Route Table

Destination	Target
10.1.0.0/16 (App VCN)	DRG

DRG Route Table for Service-Hub VCN Attachment

Destination	Target
10.1.0.0/16 (App VCN)	App VCN Attachment

Service-Hub Attachment VCN Route Table for DRG Ingress Routing

Destination	Target
10.1.0.0/16 (App VCN)	10.0.1.99 (FW)

DRG Route Table for App VCN Attachment

Destination	Target
10.1.0.0/16 (App VCN)	Service-Hub VCN Attachment

Web-Tier Subnet Route Table

Destination	Target
10.1.2.0/24 (App Tier)	DRG
10.1.0.0./16	Local Route (Implicit)

App-Tier Subnet Route Table

Destination	Target
10.1.1.0/24 (Web-Tier)	DRG
10.1.0.0./16	Local Route (Implicit)

Figure 6: The routing process for centrally shared VCN OCI network firewall routes traffic between spoke VCNs using a DRG. The red table indicates ingress route rules towards the destination, and the green tables indicate egress route rule toward for return traffic to the source.

The traffic flow moves through the following steps:

1. Traffic originating from the from a source instance in the web tier subnet is forwarded to the DRG using its subnet route table entry destined to the app tier subnet.
2. The DRG route table on the app VCN attachment forwards traffic using the service hub VCN attachment where the centralized OCI Network firewall is deployed.
3. The service hub attachment VCN route table for DRG ingress routing is used to forward the traffic to the private IP address 10.0.1.99 of the OCI network firewall instead of routing directly to the app tier subnet in the app VCN.
4. If the traffic is permitted, the OCI network firewall forwards the traffic to the DRG using its subnet route table entry.
5. The DRG route table on the service hub VCN attachment forwards traffic using the app VCN attachment.
6. The DRG route table on the app VCN attachment uses the app tier VCN route table for ingress routing to forward traffic to the destination.

Steps 7 through 12 highlight the same hop-by-hop process but in the return direction.

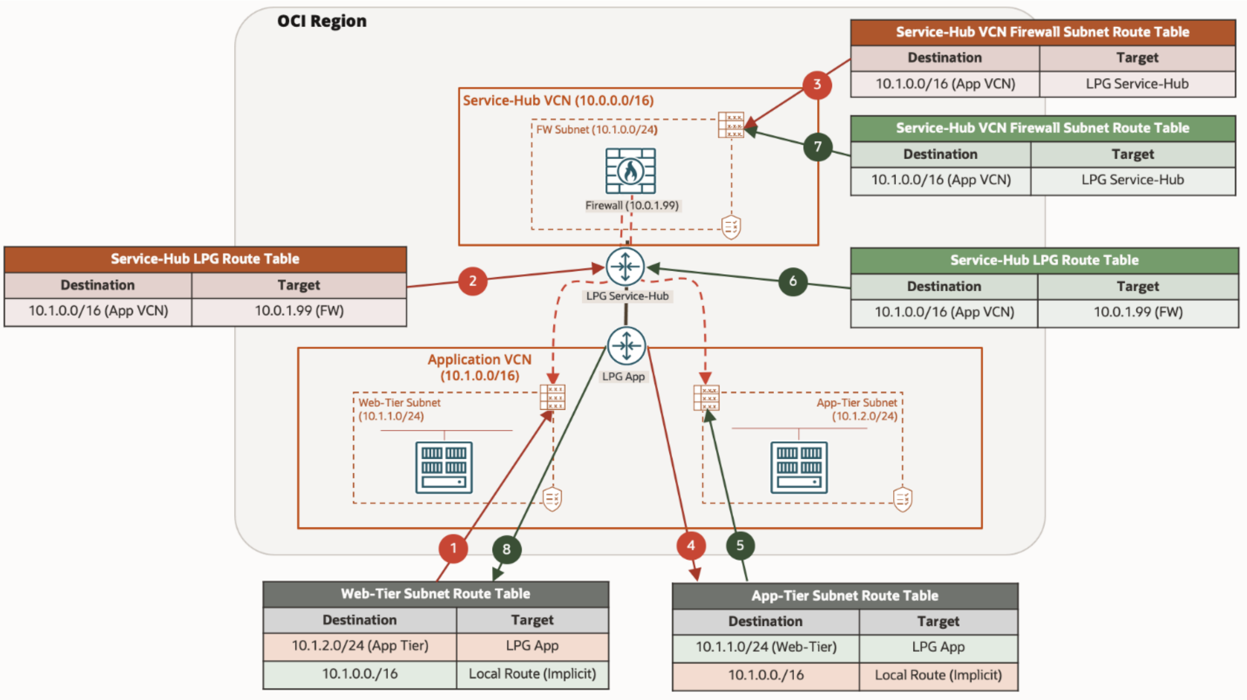
You can isolate the web tier and app tier into their own VCN in a hub-and-spoke design as a variation to the design above.

Intra-Region Routing Through a Centrally Shared VCN and OCI Network Firewall Using Local Peering Gateways

Using an LPG for inter-VCN connectivity within a region is a legacy approach, and while you can still use it in certain scenarios, it's less preferred compared to DRGs because of its increased complexity and limited scalability.

You can deploy an OCI network firewall in a central service hub VCN, with applications distributed across multiple spoke VCNs that share the centralized firewall. In this design scenario, the service hub VCN and the application spoke VCNs are connected by LPGs. The web tier and app tier of the application are placed in two subnets within the same VCN. Intra-VCN subnet route rules are configured between the two subnets, using the LPG as the target. The LPG routes application traffic to the OCI network firewall in the service hub VCN for inspection. This configuration helps ensure that all traffic between the web and app tiers is inspected by the centralized OCI Network firewall.

The following diagram shows a centralized OCI network firewall deployed within a service hub VCN, where multiple spoke VCNs share access to the firewall. This setup is designed to route traffic from the web tier in each application VCN to the firewall in the service hub VCN for inspection before it reaches the app tier in the same VCN. The following diagram highlights both the forward routing path (from the web tier through the firewall to the app tier) and the reverse routing path, which enables responses to follow the same route back. Additionally, intra-VCN subnet routing between the web and app tiers uses the LPG as a target to maintain seamless connectivity.


OCI Region
Service-Hub VCN (10.0.0.0/16)
FW Subnet (10.1.0.0/24)
Firewall (10.0.1.99)
LPG Service-Hub
LPG App
Application VCN (10.1.0.0/16)
Web-Tier Subnet (10.1.1.0/24)
App-Tier Subnet (10.1.2.0/24)
1
2
3
4
5
6
7
8

Service-Hub VCN Firewall Subnet Route Table

Destination	Target
10.1.0.0/16 (App VCN)	LPG Service-Hub

Service-Hub VCN Firewall Subnet Route Table

Destination	Target
10.1.0.0/16 (App VCN)	LPG Service-Hub

Service-Hub LPG Route Table

Destination	Target
10.1.0.0/16 (App VCN)	10.0.1.99 (FW)

Service-Hub LPG Route Table

Destination	Target
10.1.0.0/16 (App VCN)	10.0.1.99 (FW)

Web-Tier Subnet Route Table

Destination	Target
10.1.2.0/24 (App Tier)	LPG App
10.1.0.0./16	Local Route (Implicit)

App-Tier Subnet Route Table

Destination	Target
10.1.1.0/24 (Web-Tier)	LPG App
10.1.0.0./16	Local Route (Implicit)

Figure 7: The routing process for centrally shared VCN OCI network firewall routes traffic between spoke VCNs using an LPG.

The traffic flow moves through the following steps:

1. Traffic originating from the from a source instance in the web tier subnet is forwarded to the LPG using its subnet route table entry destined to the app tier subnet.
2. The service hub VCN LPG route table has ingress routing configured and is used to forward the traffic to the private IP address 10.0.1.99 of the OCI network firewall instead of routing directly to the app tier subnet in the app VCN.

3. If the traffic is permitted, the OCI network firewall forwards the traffic to the LPG using its subnet route table entry.
4. The app VCN LPG route table has local ingress routing configured and is used to forward the traffic to the destination.

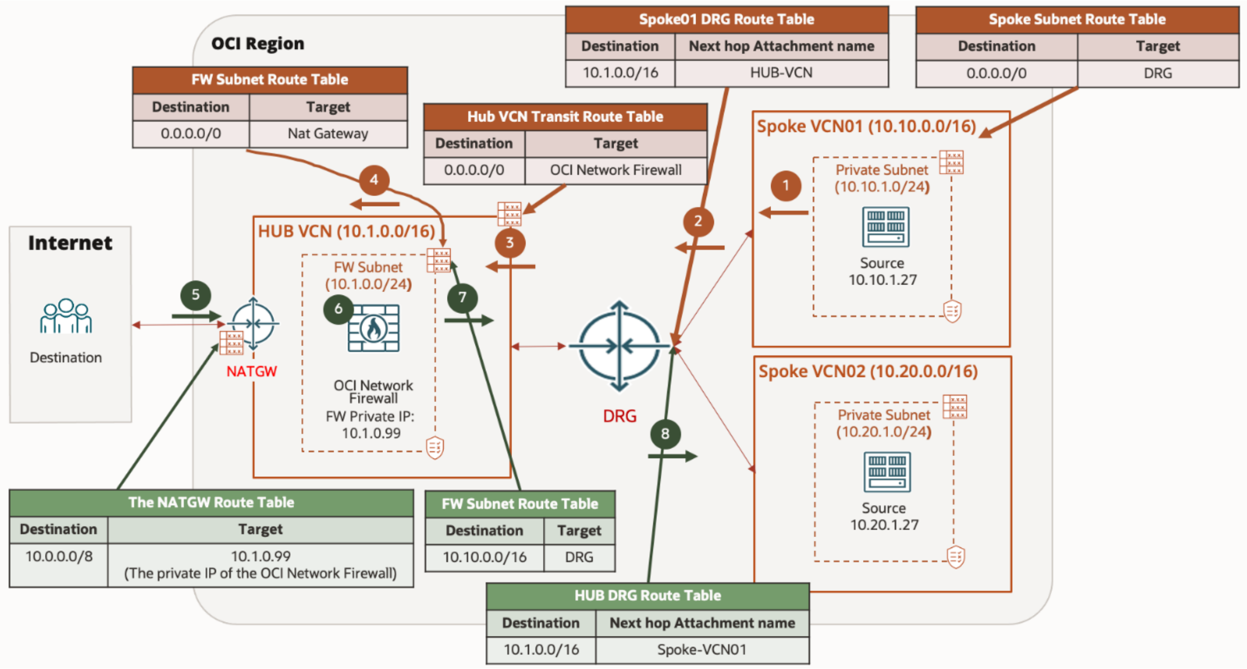
Steps 5 through 8 highlight the same hop-by-hop process but in the return direction.

Hub-and-Spoke with NAT Gateway and DRG

The following scenario demonstrates a hub-and-spoke network architecture in OCI, where spoke VCNs connect to a central hub through a DRG. The hub serves as the central point for managing and securing network traffic from all connected spoke VCNs. It hosts key services, such as OCI Network Firewall and NAT gateways. The OCI network firewall inspects, filters, and secures outbound traffic from the spokes, helping ensure that all egress traffic complies with the hub's security policies. The NAT gateway enables instances within the spoke VCNs to initiate outbound connections to the internet without being directly exposed, providing a secure, centralized point for egress-only internet traffic. This architecture streamlines security management and centralizes traffic control.

According to the OCI documentation on NAT gateways, a NAT gateway can only be used by resources within its own VCN. If the VCN is peered with another, resources in the other VCN can't access the NAT gateway.

In this design, the OCI network firewall acts as a local resource within the hub VCN, allowing peered VCN resources to utilize the NAT gateway.



Spoke01 DRG Route Table

Destination	Next hop Attachment name
10.1.0.0/16	HUB-VCN

Spoke Subnet Route Table

Destination	Target
0.0.0.0/0	DRG

FW Subnet Route Table

Destination	Target
0.0.0.0/0	Nat Gateway

Hub VCN Transit Route Table

Destination	Target
0.0.0.0/0	OCI Network Firewall

The NATGW Route Table

Destination	Target
10.0.0.0/8	10.1.0.99 (The private IP of the OCI Network Firewall)

FW Subnet Route Table

Destination	Target
10.10.0.0/16	DRG

HUB DRG Route Table

Destination	Next hop Attachment name
10.1.0.0/16	Spoke-VCN01

Figure 8: The topology and hop-by-hop routing process for hub-and-spoke with NAT and DRGs. The green table and line indicate ingress route rules and traffic flow for return traffic to the source, and the red tables and lines indicate route rules and initiated flow towards the destination.

The traffic flow moves through the following steps:

1. Traffic originating from the from a source instance in spoke VCN01 subnet is forwarded to the DRG using its subnet route table entry destined to the Internet.
2. The DRG route table on the spoke VCN01 attachment forwards traffic using the hub VCN attachment where the centralized OCI network firewall is deployed.

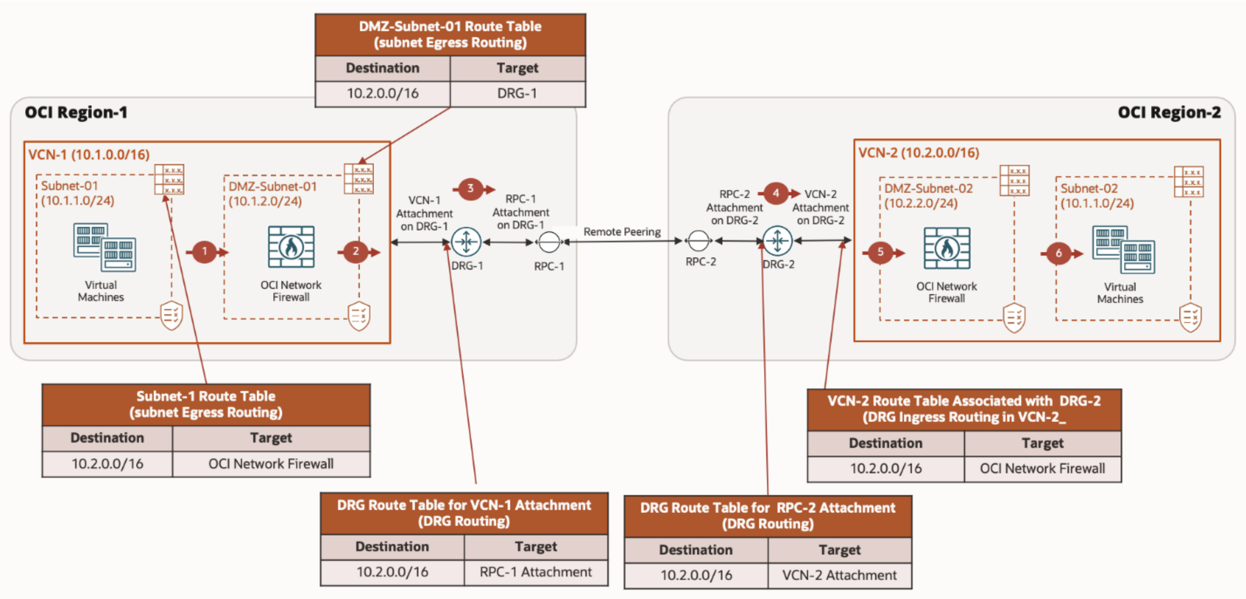
3. The service hub attachment VCN route table for DRG ingress routing is used to forward the traffic to the private IP address 10.0.1.99 of the OCI network firewall instead of routing directly to the NAT gateway in the same VCN.
4. If the traffic is permitted, the OCI network firewall forwards the traffic to the NAT gateway using its subnet route table entry.
5. Return traffic arriving at the NAT gateway is forwarded to the private IP address 10.0.1.99 of the OCI network firewall using its ingress route table entry.
6. The OCI network firewall inspects the incoming traffic.
7. If the traffic is permitted, the OCI network firewall forwards the traffic to the DRG using its subnet route table entry destined to spoke VCN01.
8. The DRG route table on the spoke VCN01 attachment uses the spoke VCN01 route table for ingress routing to forward traffic to the destination.

Inter-Region Routing Through the OCI Network Firewall Using a DRG

You might need to route traffic between resources in VCNs located in different OCI regions. You can use a remote peering connection (RPC) between the DRGs in the different regions. The traffic travels over the OCI backbone network, ensuring secure and high-performance data transfer.

For enhanced security, you can deploy the OCI Network Firewall at the edge of one or both regions involved in the remote peering connection. This setup adds an extra layer of protection by allowing you to define fine-grained traffic filtering policies, control access, and monitor network traffic. By deploying the firewall at the region’s edge, you can enforce security policies before traffic enters the VCNs, providing greater control over data flow between regions and safeguarding against potential threats.

Consider the scenario illustrated in the following figure, where resources in Subnet01 of VCN01 in Region01 must communicate with resources in Subnet02 of VCN02 in Region02. To facilitate this interregional communication, an RPC is established between DRG01 in Region01 and DRG02 in Region02, enabling seamless traffic transfer across the regions. To ensure that the traffic is secure, both regions have deployed an OCI Network Firewall at the edge of their respective VCNs. This configuration allows the traffic to be inspected and filtered according to predefined security policies before it reaches the target resources in Subnet02, adding an extra layer of protection and control over the inter-region data flow.



DMZ-Subnet-01 Route Table
(subnet Egress Routing)

Destination	Target
10.2.0.0/16	DRG-1

Subnet-1 Route Table
(subnet Egress Routing)

Destination	Target
10.2.0.0/16	OCI Network Firewall

DRG Route Table for VCN-1 Attachment
(DRG Routing)

Destination	Target
10.2.0.0/16	RPC-1 Attachment

DRG Route Table for RPC-2 Attachment
(DRG Routing)

Destination	Target
10.2.0.0/16	VCN-2 Attachment

VCN-2 Route Table Associated with DRG-2
(DRG Ingress Routing in VCN-2_

Destination	Target
10.2.0.0/16	OCI Network Firewall

Figure 9: The topology and hop-by-hop routing process for traffic between two OCI regions that passes through the OCI network firewall for enhanced security. The red table indicates ingress route rules towards the destination, and the green tables indicate egress route rule towards for return traffic to the source.

The traffic flow moves through the following steps:

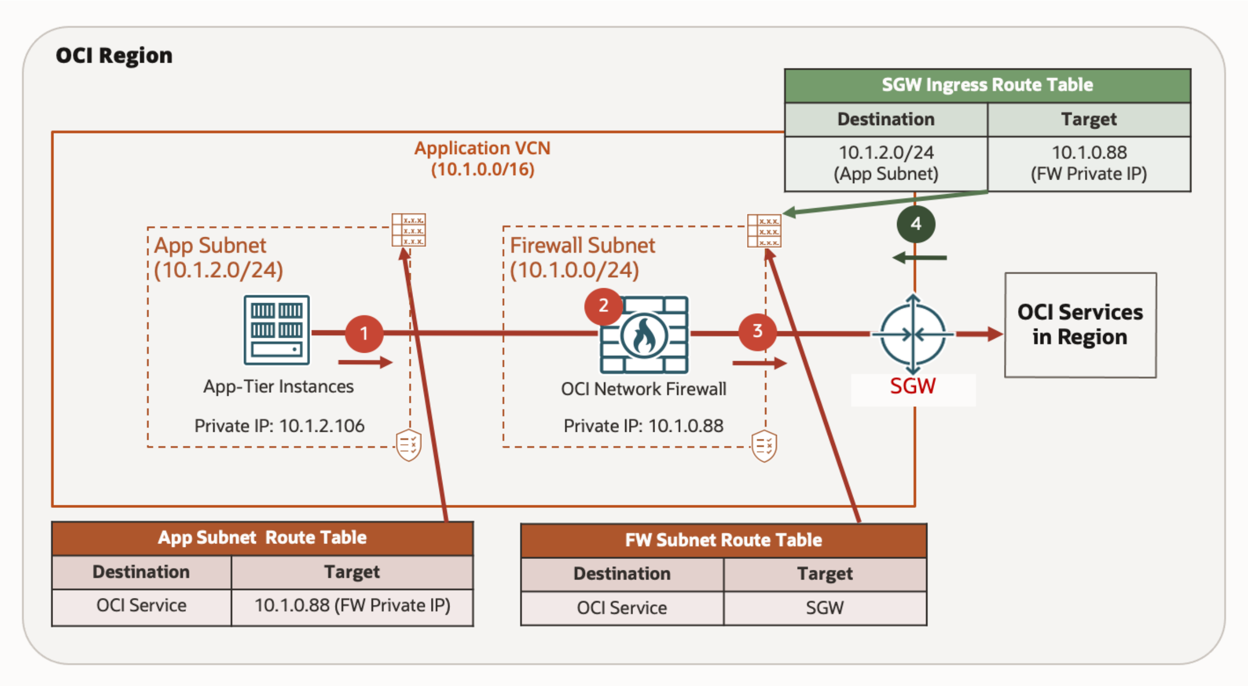
1. In the source subnet (Subnet-01 on VCN-1), subnet egress routing occurs based on the subnet route table, which resolves the route to the destination with the local OCI network firewall as the target. The traffic is routed to the local OCI network firewall.
2. The local OCI Network Firewall performs a routing lookup operation in the subnet route table. It resolves the route to the destination with the DRG as the next hop.
3. The DRG route table associated with the source VCN attachment resolves the route to the destination with the RPC-1 attachment as the next hop attachment. The traffic is routed to the DRG in the remote region over the RPC connection.
4. The remote DRG performs a routing lookup operation in the DRG route table associated with the RPC-2 attachment. It resolves the route to the destination with the local OCI Network Firewall as the next hop. The remote DRG routes the traffic to the local OCI network firewall VCN through the destination VCN ingress routing.
5. The local OCI network firewall performs a routing lookup operation in the subnet route table. It resolves the route using the implicit local route to the destination with Subnet-02 as the next hop.
6. Traffic arrives at the destination.

Return traffic follows the same path, passing through the local OCI network firewall before being routed back over the RPC, the local OCI Network Firewall in region-1, and to the source.

Service Gateway Sends the Traffic to the OCI Network Firewall Instead of the Destination

You might place the OCI network firewall in front of the secure web gateway (SWG) to filter Layer-7 URLs and provide advanced threat protection, restricting access to specific services and inspecting traffic according to their security policies. You can insert the OCI network firewall along the forwarding path through the service gateway using secure web gateway ingress routing.

The following scenario illustrates this design, where traffic from the app subnet accessing the OCI service through the service gateway is inspected by an OCI network firewall. The service gateway has a route table that contains a route rule for the destination subnet CIDR or the VCN CIDR with a private IP address of the OCI network firewall as the target. After processing the traffic packets based on its configuration, the OCI network firewall forwards the traffic toward the destination. The VCN subnet then uses its route table to route the traffic toward the destination.



SGW Ingress Route Table

Destination	Target
10.1.2.0/24 (App Subnet)	10.1.0.88 (FW Private IP)

App Subnet Route Table

Destination	Target
OCI Service	10.1.0.88 (FW Private IP)

FW Subnet Route Table

Destination	Target
OCI Service	SGW

Figure 10: The topology and hop-by-hop routing process for service gateway sends the traffic to the OCI network firewall instead of the destination. The red table indicates ingress route rules toward the destination, and the green tables indicate egress route rule towards for return traffic to the source.

The traffic flow moves through the following steps:

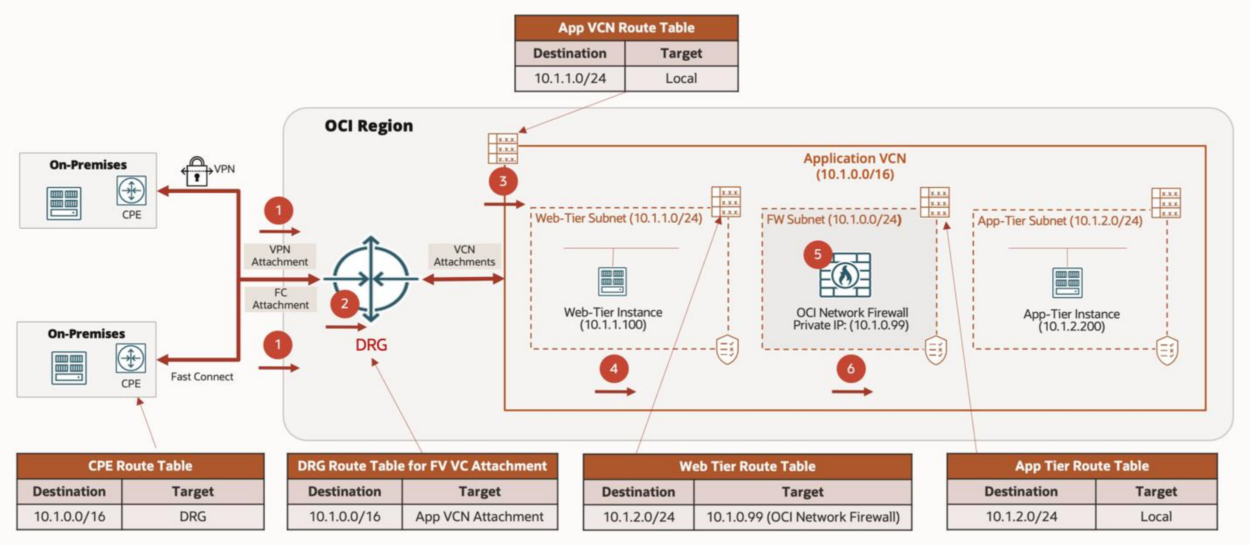
1. Traffic originating from the app tier instance destined to the Oracle service in the Oracle Services Network (OSN) is forwarded to the private IP address 10.1.0.88 of the OCI network firewall using its subnet route table entry instead of directly to the SWG.
2. The OCI network firewall permits or denies the traffic based on the configured security policies.
3. If the traffic is permitted, the OCI network firewall forwards the traffic to the service gateway using its subnet route table entry.
4. Return traffic follows the same path, passing through the OCI network firewall before being routed back to the source on the internet.

Routing Use Case for OCI Network Firewall Insertion to On-Premises

You can insert the OCI network firewall into a network architecture to secure traffic flows from hybrid cloud deployments. The following sections cover supported OCI network firewall insertion scenarios used to inspect traffic flows from on-premises networks.

On-Premises Instances Access VCN Through OCI Network Firewall

Hybrid cloud deployments are increasingly common, requiring seamless communication between on-premises and cloud networks. With a DRG, you can connect multiple VCNs to their on-premises networks through a single DRG. These on-premises networks can be connected by VPN tunnels or FastConnect virtual circuits. As shown in Figure 11, traffic from on-premises networks to an OCI VCN can route through the OCI Network Firewall to enforce security policies. Similarly, traffic from OCI back to on-premises networks follows the same routing path, passing through the OCI network firewall.



OCI Region
On-Premises
CPE
VPN
On-Premises
CPE
Fast Connect
1
VPN Attachment
FC Attachment
1
2
DRG
VCN Attachments
3
Application VCN (10.1.0.0/16)
Web-Tier Subnet (10.1.1.0/24)
Web-Tier Instance (10.1.1.100)
FW Subnet (10.1.0.0/24)
5
OCI Network Firewall Private IP: (10.1.0.99)
App-Tier Subnet (10.1.2.0/24)
App-Tier Instance (10.1.2.200)
4
6

App VCN Route Table	
Destination	Target
10.1.1.0/24	Local

CPE Route Table	
Destination	Target
10.1.0.0/16	DRG

DRG Route Table for FV VC Attachment	
Destination	Target
10.1.0.0/16	App VCN Attachment

Web Tier Route Table	
Destination	Target
10.1.2.0/24	10.1.0.99 (OCI Network Firewall)

App Tier Route Table	
Destination	Target
10.1.2.0/24	Local

Figure 11: The topology and hop-by-hop routing process for on-premises instances access VCN through the OCI network firewall.

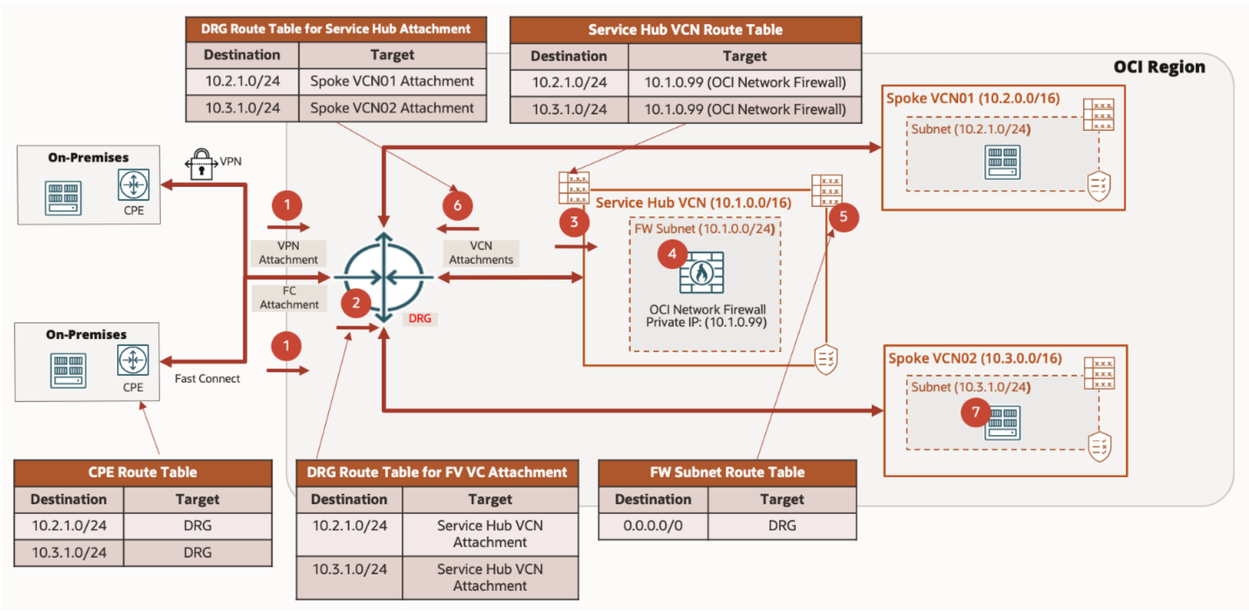
The traffic flow moves through the following steps:

1. Traffic originating from on-premises uses the customer premises equipment (CPE) routes table, which contains routes for OCI networks with the next hop pointing to the DRG.
2. The DRG route table lookup contains a next hop target for the app VCN attachment.
3. The app VCN attachment contains a default VCN route table for ingress routing to route the traffic towards the destination in web-tier subnet using an implicit local route.
4. The web-tier subnet route table routes traffic to the private IP address 10.0.1.99 of the OCI network firewall instead of routing directly to the app tier instance in the same VCN.
5. The OCI network firewall permits or denies the traffic based on the configured security policies.
6. If the traffic is permitted, the OCI network firewall forwards the traffic to the app tier subnet using its subnet route table entry which is an implicit local route.

Return traffic follows the same path in reverse. You can also place the OCI network firewall in front of the web-tier in the example.

On-Premises Instances Access Spoke VCN Through Centrally Shared VCN OCI Network Firewall

With the latest capability of a DRG, a common design uses the DRG as the central hub to interconnect VCNs and to connect them to the on-premises networks directly. The following diagram shows such a network design that combines the centrally shared VCN OCI network firewall to route traffic from on-premises to the OCI network firewall before sending traffic to the spoke.



DRG Route Table for Service Hub Attachment

Destination	Target
10.2.1.0/24	Spoke VCN01 Attachment
10.3.1.0/24	Spoke VCN02 Attachment

Service Hub VCN Route Table

Destination	Target
10.2.1.0/24	10.1.0.99 (OCI Network Firewall)
10.3.1.0/24	10.1.0.99 (OCI Network Firewall)

CPE Route Table

Destination	Target
10.2.1.0/24	DRG
10.3.1.0/24	DRG

DRG Route Table for FV VC Attachment

Destination	Target
10.2.1.0/24	Service Hub VCN Attachment
10.3.1.0/24	Service Hub VCN Attachment

FW Subnet Route Table

Destination	Target
0.0.0.0/0	DRG

Figure 12: The topology and hop-by-hop routing process for on-premises instances access spoke VCN through the centrally shared VCN OCI network firewall.

The traffic flow moves through the following steps:

1. Traffic originating from on-premises uses the CPE routes table, which contains routes for OCI networks with the next hop pointing to the DRG.
2. The DRG route table lookup contains a next hop target for the service hub VCN attachment.
3. The service hub VCN attachment contains a service hub VCN route table for ingress routing to route the traffic towards the destination in spoke VCN with the private IP address 10.0.1.99 of the OCI network firewall instead of routing directly to the spoke VCNs.
4. The OCI network firewall permits or denies the traffic based on the configured security policies.
5. If the traffic is permitted, the OCI network firewall forwards the traffic to the DRG using its subnet route table entry which contains a default route.
6. The DRG route table lookup contains a next hop target for the spoke VCN attachment.
7. Traffic arrives at the spoke VCN subnet.

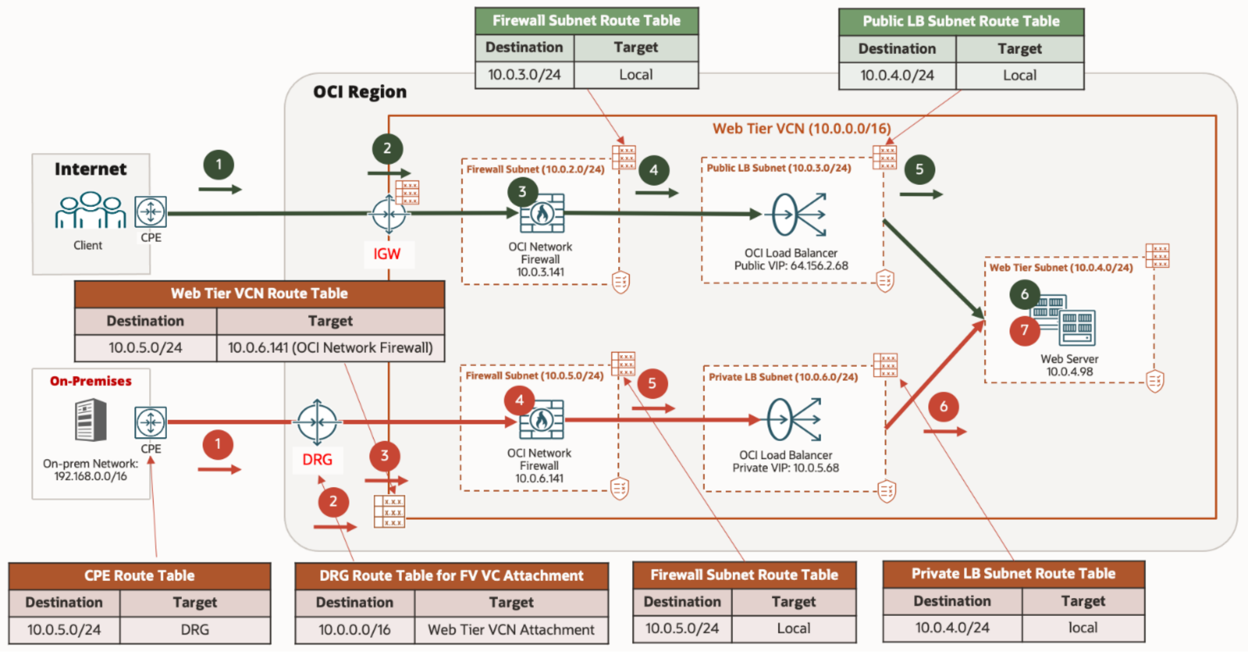
Return traffic follows the same path in reverse. Traffic moving through spoke VCN01 to spoke VCN02 through the Service Hub and OCI network firewall is supported by this topology.

Routing Use Case for OCI Network Firewall Insertion with Load Balancers

You can insert the OCI network firewall into a network architecture in combination with the OCI Load Balancer service. For more information about OCI Load Balancer, refer to the Load Balancer documentation. The following scenarios show supported OCI network firewall insertion used with OCI Load Balancer.

OCI Network Firewall Frontending OCI Load Balancer

Placing the OCI network firewall in front of a public or private load balancer at the perimeter of a VNC has several benefits, particularly related to security, traffic management, and compliance. The OCI network firewall acts as the first line of defense, blocking unauthorized traffic and preventing direct exposure of the load balancer and backend servers to potential threats from the internet or on-premises. This setup helps ensure that only legitimate traffic reaches the load balancer. The OCI network firewall is crucial for securing internet or private facing applications, meeting compliance, and providing comprehensive network security for your organization with public exposure. When you place the OCI network firewall in front of a public or private load balancer, it significantly enhances security by ensuring that threats and malicious activity can be detected and mitigated.



OCI Region
Internet
Client
CPE
IGW
Web Tier VCN (10.0.0.0/16)
Firewall Subnet (10.0.2.0/24)
OCI Network Firewall 10.0.3.141
Public LB Subnet (10.0.3.0/24)
OCI Load Balancer Public VIP: 64.156.2.68
Web Tier Subnet (10.0.4.0/24)
Web Server 10.0.4.98
On-Premises
On-prem Network: 192.168.0.0/16
CPE
DRG
Firewall Subnet (10.0.5.0/24)
OCI Network Firewall 10.0.6.141
Private LB Subnet (10.0.6.0/24)
OCI Load Balancer Private VIP: 10.0.5.68
1
2
3
4
5
6
7
1
2
3
4
5
6
7

Firewall Subnet Route Table

Destination	Target
10.0.3.0/24	Local

Public LB Subnet Route Table

Destination	Target
10.0.4.0/24	Local

Web Tier VCN Route Table

Destination	Target
10.0.5.0/24	10.0.6.141 (OCI Network Firewall)

CPE Route Table

Destination	Target
10.0.5.0/24	DRG

DRG Route Table for FV VC Attachment

Destination	Target
10.0.0.0/16	Web Tier VCN Attachment

Firewall Subnet Route Table

Destination	Target
10.0.5.0/24	Local

Private LB Subnet Route Table

Destination	Target
10.0.4.0/24	local

Figure 13: The topology for OCI network firewall frontending load balancer. The red lines and numbers represent traffic flow from on-premises, and the green lines and numbers represent traffic flow from the internet.

On premises, the traffic flow moves through the following steps:

1. Traffic originating from on-premises to the private load balancer IP address 10.0.5.68 uses the CPE routes table which contains routes for OCI networks with the next hop pointing to the DRG.
2. The DRG route table lookup contains a next hop target for the web tier hub VCN attachment.
3. The web tier VCN attachment contains a web tier VCN route table for ingress routing to route the traffic towards the destination private load balancer subnet with the private IP address 10.0.6.141 of the OCI network firewall, instead of routing directly to the private load balancer subnet.
4. The OCI network firewall permits or denies the traffic based on the configured security policies.
5. If the traffic is permitted, the OCI network firewall forwards the traffic to the private load balancer subnet using its subnet route table entry, which contains an implicit local route for the web tier subnet.
6. The private load balancer receives the traffic and uses its subnet route table in the private load balancer subnet, which contains an implicit local route to the web tier subnet.
7. Traffic arrives at the web tier server.

Over the internet, the traffic flow moves through the following steps:

1. Traffic originating from an Internet source to the public load balancer IP address 64.156.2.68 uses the CPE routes table which contains routes for OCI public load balancer subnet.
2. Traffic originating from an internet source arriving at the internet gateway is forwarded to the private IP address 10.0.3.141 of the OCI network firewall using its ingress route table entry.
3. The OCI network firewall permits or denies the traffic based on the configured security policies.

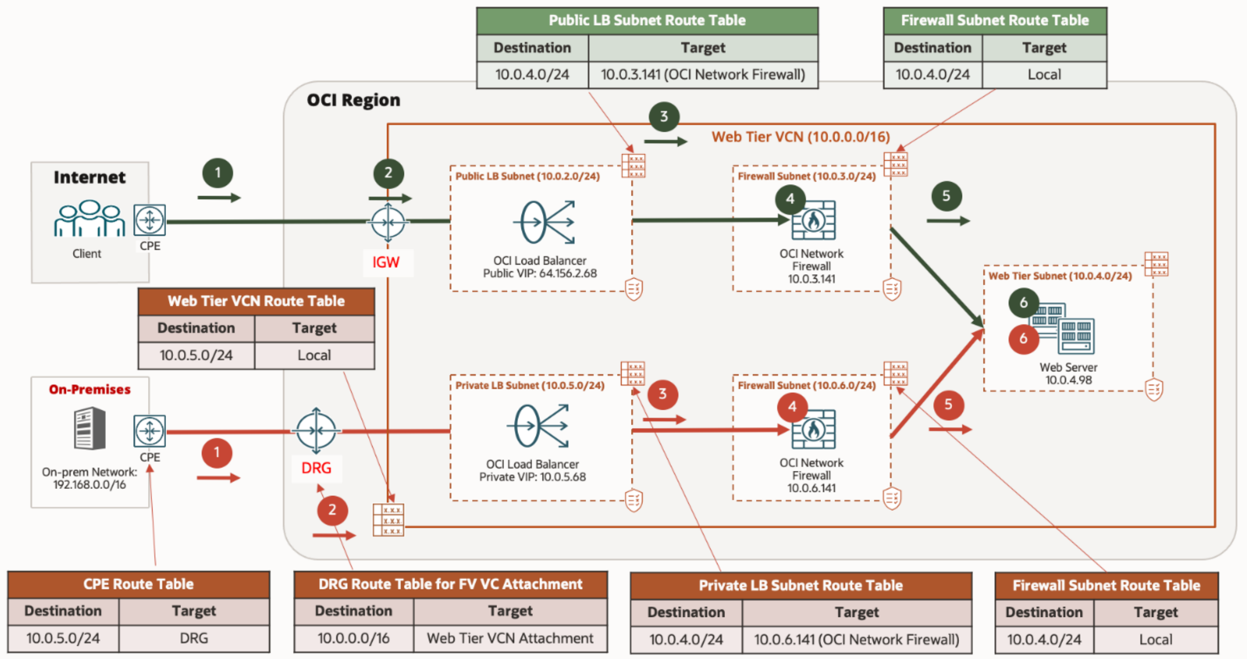
4. The OCI network firewall forwards the traffic to the public load balancer’s private IP address using its subnet route table.
5. The public load balancer receives the traffic and uses its subnet route table in the public load balancer subnet, which contains an implicit local route to the web tier subnet.
6. Traffic arrives at the web tier server.

Return traffic follows the same path in reverse.

OCI Network Firewall Backending OCI Load Balancer

Placing the OCI network firewall behind a public or private load balancer within a VCN provides a strategic advantage by layering security while optimizing traffic flow. In this configuration, the load balancer handles incoming traffic distribution, and the OCI network firewall acts as a secondary, more focused line of defense, inspecting and filtering traffic that has passed through the load balancer. This setup ensures that the firewall can manage and secure traffic with a higher level of granularity, particularly for inspecting threats and enforcing compliance at the application layer.

By positioning the OCI network firewall behind the load balancer, the load balancer can perform its core function of distributing traffic across healthy backend servers, while the firewall focuses on inspecting legitimate traffic for deeper threats. This setup provides a balance between efficient traffic management and robust security.



Public LB Subnet Route Table

Destination	Target
10.0.4.0/24	10.0.3.141 (OCI Network Firewall)

Firewall Subnet Route Table

Destination	Target
10.0.4.0/24	Local

Web Tier VCN Route Table

Destination	Target
10.0.5.0/24	Local

CPE Route Table

Destination	Target
10.0.5.0/24	DRG

DRG Route Table for FV VC Attachment

Destination	Target
10.0.0.0/16	Web Tier VCN Attachment

Private LB Subnet Route Table

Destination	Target
10.0.4.0/24	10.0.6.141 (OCI Network Firewall)

Firewall Subnet Route Table

Destination	Target
10.0.4.0/24	Local

Figure 14: The topology for OCI network firewall backending OCI load balancer. The red lines and numbers represent traffic flow from on-premises, and green lines and numbers represent traffic flow from the internet.

On premises, the traffic flow moves through the following steps:

1. Traffic originating from on-premises to the private load balancer IP address 10.0.5.68 uses the CPE routes table which contains routes for OCI networks with the next hop pointing to the DRG.
2. The DRG route table lookup contains a next hop target for the web tier hub VCN attachment, which contains an implicit local route for the private load balancer subnet.
3. The private load balancer receives the traffic and uses its subnet route table in the private load balancer subnet with the private IP address 10.0.1.99 of the OCI network firewall, instead of routing directly to the web tier subnet.

4. The OCI network firewall permits or denies the traffic based on the configured security policies.
5. If the traffic is permitted, the OCI network firewall forwards the traffic to the web tier subnet using its subnet route table entry, which contains an implicit local route for the web tier subnet.
6. Traffic arrives at the web tier server.

Over the internet, the traffic flow moves through the following steps:

1. Traffic originating from an internet source to the public load balancer IP address 64.156.2.68 uses the CPE routes table, which contains routes for OCI public load balancer subnet.
2. The internet gateway route table lookup contains a next hop target for the public load balancer subnet.
3. The public load balancer receives the traffic and uses its subnet route table in the public load balancer subnet with the private IP address 10.0.3.141 of the OCI network firewall, instead of routing directly to the web tier subnet.
4. The OCI network firewall permits or denies the traffic based on the configured security policies.
5. If the traffic is permitted, the OCI network firewall forwards the traffic to the web tier subnet using its subnet route table entry, which contains an implicit local route for the web tier subnet.
6. Traffic arrives at the web tier server.

Return traffic follows the same path in reverse.

OCI Network Firewall Insertion with an OCI Load Balancer in SSL mode

In the previous section, we explored OCI network firewall routing insertion use cases with OCI load balancers to effectively secure traffic flows. This section expands on those scenarios, specifically focusing on a use case where SSL mode is enabled on the load balancer. Here, we examine how to use the OCI Network Firewall service to decrypt traffic, perform in-depth inspection, and enforce security policies, helping ensure enhanced security and visibility across encrypted network paths that include the OCI load balancer.

In OCI, you can implement SSL in various ways depending on security and performance requirements when using the Load Balancer. You can explore these options in the blog post, Load Balancing SSL Traffic in OCI. The main use cases include the following examples:

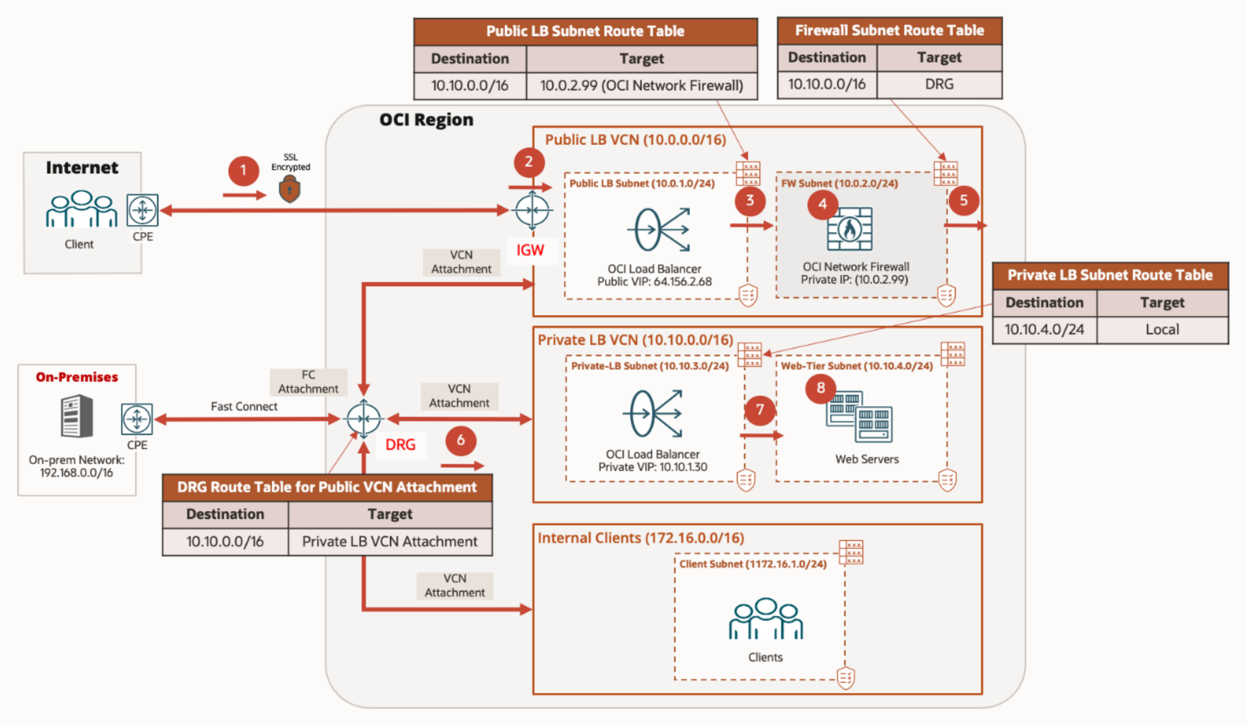
- **SSL termination:** The SSL connection terminates at the load balancer, enabling backend servers to process unencrypted traffic.
- **SSL tunneling:** Secures the entire transport channel between the client and backend servers without the Load Balancer decrypting the traffic.
- **End-to-end SSL:** The load balancer terminates the client SSL connection and initiates a new encrypted connection to the backend servers. This configuration is useful for cases where the load balancer must inspect or modify HTTP headers.

You can seamlessly integrate the OCI network firewall into the path of the OCI load balancer to enhance security supporting all use cases without breaking the encrypted tunnel. In termination mode, the firewall can inspect traffic before SSL termination at the load balancer, providing advanced threat protection and enforcing security policies at the public side of the traffic flow. In tunneling mode, it helps ensure secure, encrypted communication throughout the network path. In end-to-end mode, the firewall can inspect traffic after SSL termination at the load balancer, providing advanced threat protection and enforcing security policies across the private side of the traffic flow.

The certificates required by the OCI network firewall for inbound SSL inspection depend on which SSL mode the OCI load balancer is operating in.

The following scenario show supported OCI network firewall insertion with the OCI load balancer in either tunneling or end-to-end SSL mode. In this scenario, the network infrastructure provides two distinct access paths to the web servers, based on whether the users are internal (within the organization's private network) or external (coming from the internet). The objective is to provide secure and efficient access to the same backend resources (web servers) while implementing robust security controls. To protect the perimeter of the network from the untrusted internet, we deploy the OCI network firewall. The OCI network firewall is strategically placed between two OCI load balancers enabled with SSL, one public and one private.

This design uses separate load balancers for external and internal users, helping ensure that traffic is securely segregated. External users are prevented from directly accessing internal resources without first having their traffic inspected by the OCI network firewall, and the design allows for internal users to follow a different SSL encryption standard on the private load balancer. The OCI network firewall applies security policies to external traffic, preventing the spread of malicious activity and helping ensure that traffic from external users is thoroughly inspected for potential threats before reaching internal services.



Public LB Subnet Route Table

Destination	Target
10.10.0.0/16	10.0.2.99 (OCI Network Firewall)

Firewall Subnet Route Table

Destination	Target
10.10.0.0/16	DRG

Private LB Subnet Route Table

Destination	Target
10.10.4.0/24	Local

DRG Route Table for Public VCN Attachment

Destination	Target
10.10.0.0/16	Private LB VCN Attachment

Figure 15: The topology for OCI network firewall Insertion with OCI load balancer SSL

Over the internet, the traffic flow moves through the following steps:

1. Traffic originating from an internet source to the public load balancer IP address uses the CPE routes table, which contains routes for OCI public load balancer subnet. External users connect to the public load balancer using the public SSL certificate.
2. The internet gateway route table lookup contains a next hop target for the public load balancer subnet.
3. The public load balancer receives the traffic. The public load balancer terminates the SSL connection, then initiates new SSL connections to the backend server, which is the private load balancer listener IP address 10.10.1.30. The public load balancer subnet route table includes a private IP route rule to send traffic destined for the private load balancer through the OCI network firewall's private IP 10.0.2.99 instead of routing directly to the DRG.

4. The OCI network firewall permits or denies the traffic based on the configured security policies which contain rules for SSL inbound inspection. The OCI network firewall is configured with the SSL certificate and key matching the private load balancer.
5. If the traffic is permitted, the OCI network firewall forwards the traffic using its subnet route table which contains a route rule for all 10.10.0.0/16 traffic to be forwarded to the DRG.
6. The DRG route table lookup contains a next hop target for the private load balancer VCN attachment, which contains an implicit local route for the private load balancer subnet.
7. The private load balancer receives the traffic. The private load balancer terminates the SSL connection, then initiates new SSL connections to the backend server, which is the web server. The private load balancer subnet route table includes an implicit local route rule to send traffic directly to the web server.
8. Traffic arrives at the web tier server.

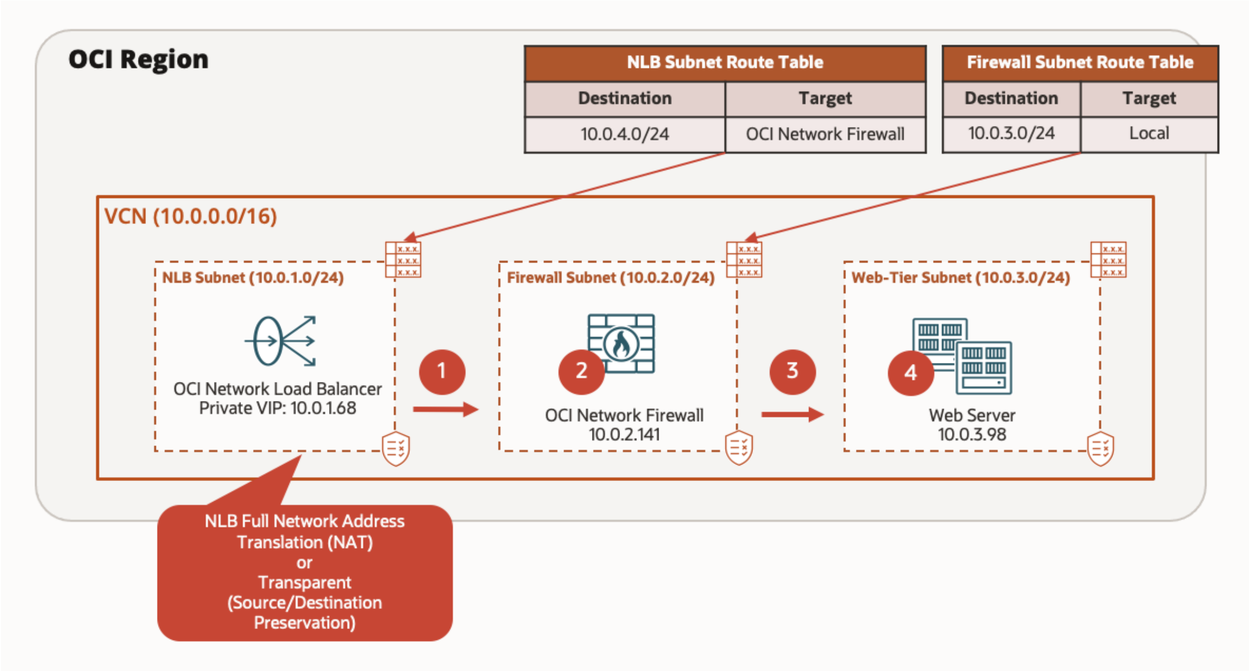
Return traffic follows the same path in reverse.

Routing Use Case for OCI Network Firewall Insertion with Network Load Balancers

You can insert the OCI network firewall into a network architecture in combination with the OCI network load balancer. The network load balancer supports NAT, source preservation and transparent (source and destination preservation) modes which are described in detail within our modes of operation network load balancer documentation. Understanding how each mode affects the source and destination of traffic flows is crucial to designing a secure and efficient network. You can use the network load balancer in full NAT mode in combination with OCI gateways, including NAT gateway, internet gateway, and DRG. However, because you can only use the network load balancer in transparent (source and destination preservation) mode with private network load balancers, you can only use it with the DRG.

Virtual Cloud Network Routing for Network Load Balancer

In an OCI setup, routing traffic for a network load balancer through a VCN that includes an OCI network firewall between subnets is a common design pattern for improved security and traffic control. When creating this setup, you typically place the network load balancer in a private subnet and configure routing rules in the VCN to direct traffic through an OCI network firewall in a separate subnet. You can configure the firewall with security policies to inspect and manage traffic between the client-facing and backend subnets, allowing only the necessary ports and protocols. This setup helps ensure that all traffic routed by the network load balancer is filtered through the OCI network firewall, enhancing security before reaching its destination within the VCN.


OCI Region
VCN (10.0.0.0/16)
NLB Subnet (10.0.1.0/24)
OCI Network Load Balancer
Private VIP: 10.0.1.68
1
Firewall Subnet (10.0.2.0/24)
2
OCI Network Firewall
10.0.2.141
3
Web-Tier Subnet (10.0.3.0/24)
4
Web Server
10.0.3.98
NLB Full Network Address Translation (NAT)
or
Transparent
(Source/Destination Preservation)

NLB Subnet Route Table

Destination	Target
10.0.4.0/24	OCI Network Firewall

Firewall Subnet Route Table

Destination	Target
10.0.3.0/24	Local

Figure 16: The flow of intra-VCN traffic routed through the private network load balancer in either full NAT or transparent (source and destination preservation) modes, passing through the OCI network firewall for inspection, before reaching the destination backend servers within the same VCN.

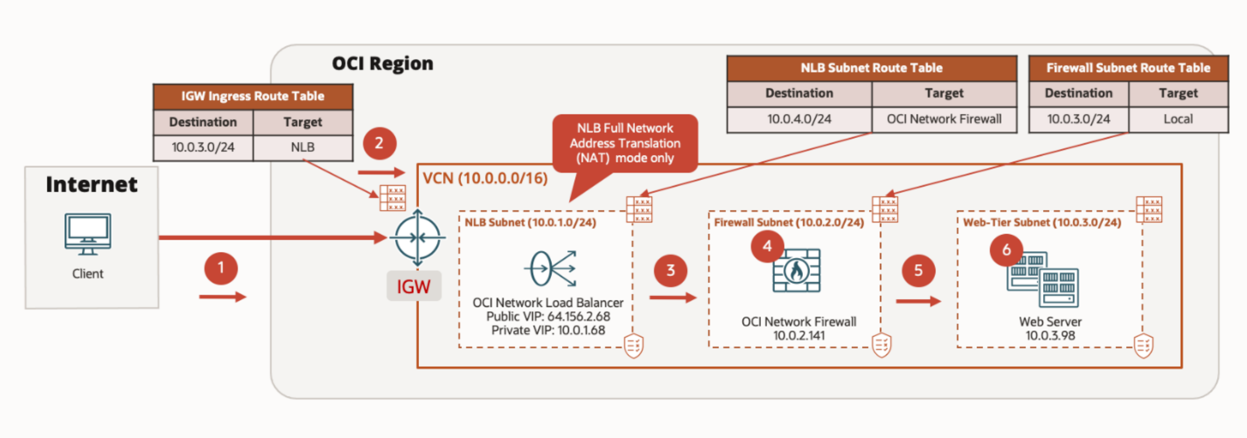
The traffic flow moves through the following steps:

1. The private network load balancer receives traffic from the source and uses its subnet route table in the private network load balancer subnet to route traffic to the private IP address 10.0.2.41 of the OCI network firewall instead of routing directly to the web tier subnet.
2. The OCI network firewall permits or denies the traffic based on the configured security policies.
3. If the traffic is permitted, the OCI network firewall forwards the traffic to the web tier subnet using its subnet route table entry which contains an implicit local route for the web tier subnet.
4. Traffic arrives at the web tier server.

Return traffic follows the same path in reverse.

Inbound Internet Traffic Through Internet Gateway Routing for Network Load Balancer

In the following inbound internet traffic scenario, traffic originates from the public internet and is routed to OCI through an internet gateway. The network load balancer handles the incoming internet traffic by translating the source (public IP) and destination (network load balancer) virtual IP (VIP) addresses, preserving the backend servers from direct internet exposure.



IGW Ingress Route Table

Destination	Target
10.0.3.0/24	NLB

NLB Subnet Route Table

Destination	Target
10.0.4.0/24	OCI Network Firewall

Firewall Subnet Route Table

Destination	Target
10.0.3.0/24	Local

Figure 17: The flow of inbound internet traffic through the internet gateway to the network load balancer in full NAT mode, network firewall, and backend servers.

Over the internet, the traffic flow moves through the following steps:

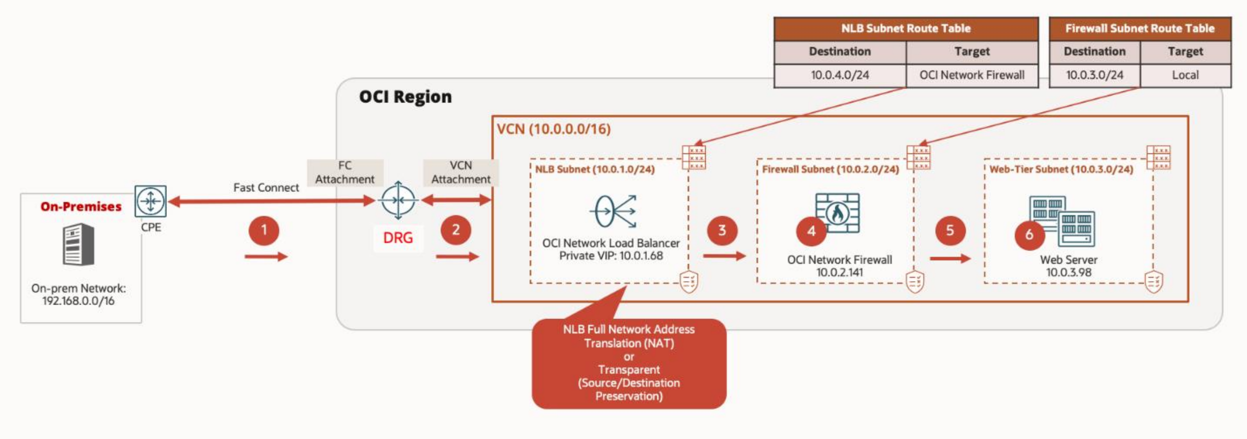
1. Traffic originating from an internet source to the public network load balancer IP address uses the CPE routes table, which contains routes for OCI public network load balancer subnet.
2. The internet gateway route table lookup contains a next hop target for the public network load balancer subnet.
3. The public network load balancer receives the traffic and uses its subnet route table in the public load balancer subnet with the private IP address 10.0.2.141 of the OCI network firewall instead of routing directly to the web tier subnet.
4. The OCI network firewall permits or denies the traffic based on the configured security policies.
5. If the traffic is permitted, the OCI network firewall forwards the traffic to the web tier subnet using its subnet route table entry, which contains an implicit local route for the web tier subnet.
6. Traffic arrives at the web tier server.

Return traffic follows the same path in reverse.

Inbound On-Premises Traffic with DRG Routing for Network Load Balancer

In scenarios where inbound traffic originates from an on-premises environment through VPN or FastConnect, OCI enables secure routing through the DRG to a network load balancer and then through an OCI network firewall. This setup is ideal for securing controlled access from on-premises networks to applications hosted in OCI.

Here, traffic from the on-premises environment reaches the DRG, which is connected to the VCN housing the network load balancer and firewall. Routing rules in the VCN are configured to direct incoming traffic first through the network load balancer, which distributes it across multiple backend resources for scalability. Before reaching these resources, the traffic is filtered by the OCI network firewall, where custom security policies can be applied for inspection, threat detection, and access control. This use case supports high-security requirements by combining load balancing, threat mitigation, and dynamic scalability for on-premises to cloud workloads.



NLB Subnet Route Table	
Destination	Target
10.0.4.0/24	OCI Network Firewall

Firewall Subnet Route Table	
Destination	Target
10.0.3.0/24	Local

Figure 18: The flow of inbound traffic from the on-premises network through the DRG to the network load balancer, in either full NAT or transparent modes, passing through the OCI network firewall for inspection, before reaching the destination backend servers within the same VCN.

On-premises, the traffic flow moves through the following steps:

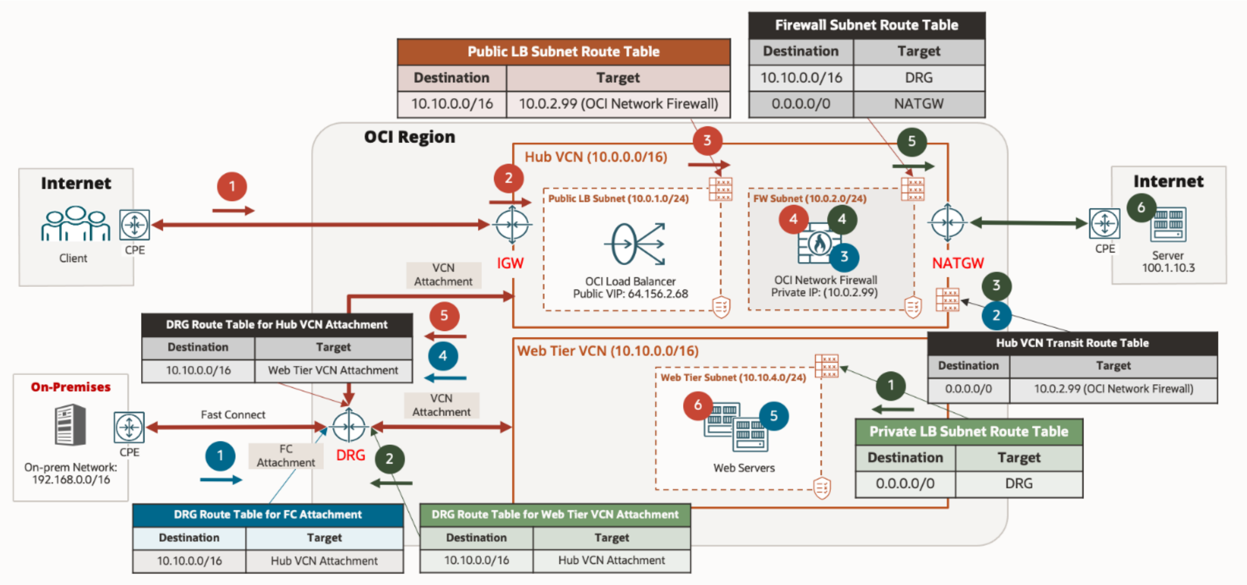
1. Traffic originating from on-premises to the private network load balancer IP address 10.0.1.68 uses the CPE routes table, which contains routes for OCI networks with the next hop pointing to the DRG.
2. The DRG route table lookup contains a next hop target for the VCN attachment which contains an implicit local route for the private network load balancer subnet.
3. The private network load balancer receives the traffic and uses its subnet route table in the private network load balancer subnet with the private IP address 10.0.2.41 of the OCI network firewall instead of routing directly to the web tier subnet.
4. The OCI network firewall permits or denies the traffic based on the configured security policies.
5. If the traffic is permitted, the OCI network firewall forwards the traffic to the web tier subnet using its subnet route table entry which contains an implicit local route for the web tier subnet.
6. Traffic arrives at the web tier server.

Return traffic follows the same path in reverse.

Routing Use Case for Single OCI Network Firewall Insertion

Managing separate OCI network firewalls for north-south (internet bound) and east-west (inter-VCN and on-premises) increases operational complexity and cost. Teams must handle different configurations, rule sets, and monitoring tools, which can lead to inconsistent security policies and potential security gaps. The cost of provisioning and maintaining two firewall solutions can also be substantial. In OCI, the concepts of public and private subnets and their associated route tables determine how resources communicate both internally and externally. Moreover, you can only assign resources, such as the OCI network firewall, to either a public or private subnet, never at the same time. Because private subnet resources can only egress to the internet through a NAT gateway and can't use an internet gateway, if you need the OCI network firewall to inspect north-south and east-west traffic flows, deploy separate OCI network firewalls for each traffic pattern: North-south (internet-bound) and east-west (inter-VCN and on-premises).

The following scenario illustrates a supported OCI network firewall insertion design that allows for the use of a single OCI network firewall to manage both north-south (internet-bound) and east-west (Inter-VCN and on-premises) traffic patterns. In this design, an OCI network firewall is deployed within a central hub VCN to inspect and secure traffic flows inbound from the internet, outbound to the internet, and finally from the on-premises.



Public LB Subnet Route Table

Destination	Target
10.10.0.0/16	10.0.2.99 (OCI Network Firewall)

Firewall Subnet Route Table

Destination	Target
10.10.0.0/16	DRG
0.0.0.0/0	NATGW

DRG Route Table for Hub VCN Attachment

Destination	Target
10.10.0.0/16	Web Tier VCN Attachment

Hub VCN Transit Route Table

Destination	Target
0.0.0.0/0	10.0.2.99 (OCI Network Firewall)

Private LB Subnet Route Table

Destination	Target
0.0.0.0/0	DRG

DRG Route Table for FC Attachment

Destination	Target
10.10.0.0/16	Hub VCN Attachment

DRG Route Table for Web Tier VCN Attachment

Destination	Target
10.10.0.0/16	Hub VCN Attachment

Figure 19: The topology and routing for routing insertion of a single OCI network firewall for traffic flows. The red lines and numbers represent traffic flow from the Internet to the web server. The green lines and numbers represent egress traffic flow to the internet through the NAT gateway. The blue lines and numbers represent traffic flows from on-premises to the web server. The black route tables are used for more than one type of traffic flow.

From the internet, the traffic flow moves through the following steps:

1. Traffic originating from internet source to the public load balancer IP address uses the CPE routes table, which contains routes for OCI public load balancer subnet.
2. The internet gateway route table lookup contains an implicit next hop target for the public load balancer subnet.
3. The public load balancer receives the traffic. The public load balancer terminates the SSL connection, then initiates new SSL connections to the backend server, which is the private IP address of the web server within the web tier VCN. The public load balancer subnet route table includes a private IP route rule to send traffic destined for the private IP address of the web server through the OCI network firewall's private IP 10.0.2.99 instead of routing directly to DRG.
4. The OCI network firewall permits or denies the traffic based on the configured security policies.
5. If the traffic is permitted, the OCI network firewall forwards the traffic using its subnet route table, which contains a route rule for all 10.10.0.0/16 traffic to be forwarded to the DRG. The DRG route table lookup contains a next hop target for the web tier VCN attachment which contains an implicit local route for the web tier subnet.
6. Traffic arrives at the web tier server.

The traffic flow egress to the internet through NAT gateway moves through the following steps:

1. Traffic originating from the from a web tier server in the web tier VCN subnet is forwarded to the DRG using its subnet route table entry.
2. The DRG route table on the web tier VCN attachment forwards traffic using the hub VCN attachment where the centralized OCI network firewall is deployed.
3. The service hub attachment VCN route table for DRG ingress routing forwards the traffic to the private IP address 10.0.2.99 of the OCI network firewall instead of routing directly to the NAT gateway in the same VCN.

4. The OCI network firewall permits or denies the traffic based on the configured security policies.
5. If the traffic is permitted, the OCI network firewall forwards the traffic to the NAT gateway using its subnet route table entry.
6. Traffic arrives at the web server on the internet.

On-premises, the traffic flow moves through the following steps:

1. Traffic originating from on-premises uses the CPE routes table, which contains routes for OCI networks with the next hop pointing to the DRG. The DRG route table lookup contains a next hop target for the hub VCN attachment.
2. The hub VCN attachment contains a transit VCN route table for ingress routing to route the traffic toward the private IP address 10.0.2.99 of the OCI network firewall instead of routing directly to the web tier VCN.
3. The OCI network firewall permits or denies the traffic based on the configured security policies.
4. If the traffic is permitted, the OCI network firewall forwards the traffic to the DRG using its subnet route table entry which towards the web tier VCN. The DRG route table lookup contains a next hop target for the web tier VCN attachment.
5. Traffic arrives at the web tier server.

Unsupported Routing Use Cases for OCI Network Firewall Insertion

When deploying the OCI network firewall, certain routing scenarios can fall outside the scope of supported configurations. These common unsupported scenarios can lead to network communication issues, security policy enforcement gaps, or performance degradation. Understanding the limitations and avoiding these routing configurations is crucial to ensuring optimal firewall performance and secure traffic flow within the OCI environment.

Internet Gateway Targets Resources Outside Local VCN

In OCI, an internet gateway is designed to route traffic to and from public IP addresses within a VCN, but it can’t direct ingress traffic to another VCN or to private subnets. This limitation exists because the route table rules associated with the internet gateway can’t target resources outside of a public subnet. Consequently, scenarios that involve routing ingress internet traffic through a central OCI network firewall for inspection and then forwarding it to another VCN or private subnet aren’t supported.

As a workaround, you can implement the OCI network firewall in each internet-facing VCN as a distributed solution. This approach allows each VCN to handle internet-bound traffic independently, enabling security inspection without requiring cross-VCN routing.

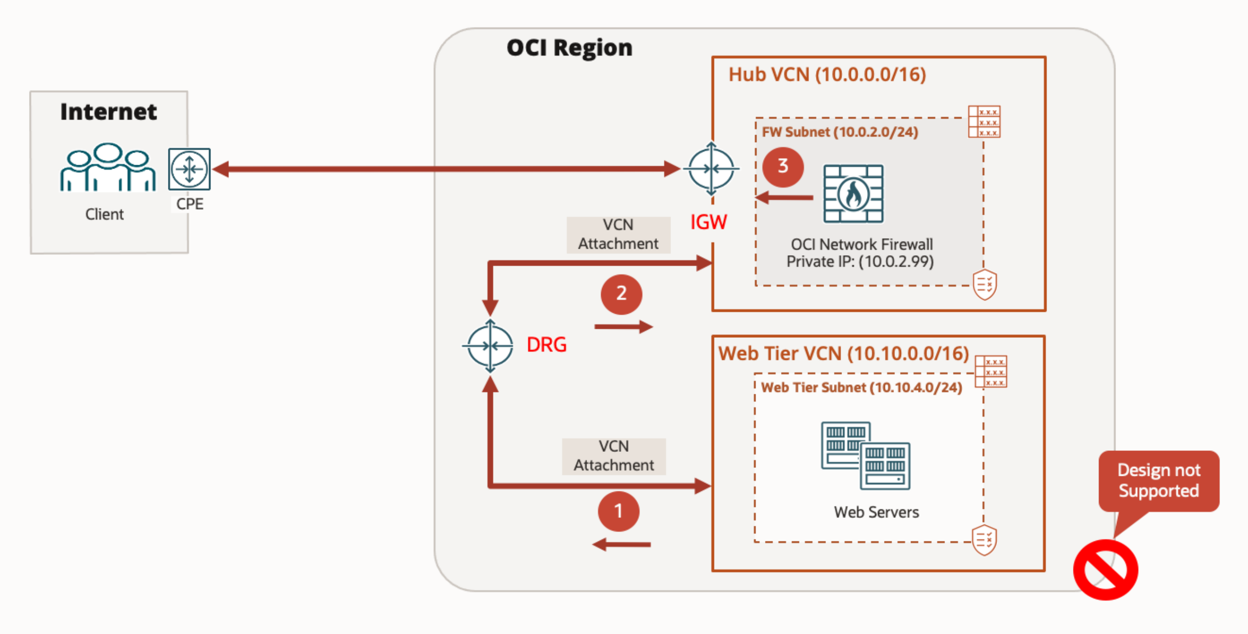


Figure 20: The topology for internet gateway targeting resources outside a local VCN

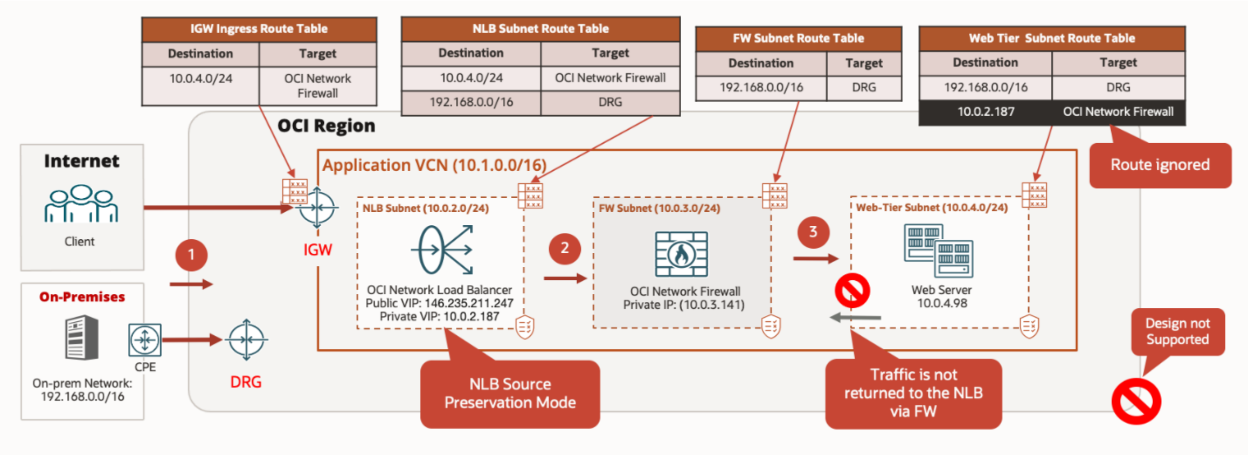
As a workaround, you can deploy the OCI network firewall in each respective internet-facing VCN as a distributed solution.

Network Load Balancer Source Preservation Mode

In the following design scenario, an OCI network load balancer operates in source preservation mode. In this mode, the network load balancer performs a destination NAT, translating the listener’s VIP to the backend server's IP address, while preserving the original source IP address and port information as it forwards traffic to the backend server. This setup preserves client IP visibility and session persistence, which can be crucial for certain applications.

However, this configuration introduces a critical limitation: return traffic bypasses the OCI network firewall because, in Source Preservation mode, backend servers are configured to bypass subnet route table rules that route traffic through the firewall. Instead, return traffic is directed back to the network load balancer, bypassing the firewall entirely. The OCI network firewall relies on inspecting both inbound and outbound traffic to apply security policies effectively. This security gap makes the design unsuitable for use cases requiring comprehensive traffic inspection and enforcement.

As referenced in the previous section on routing insertion use cases with network load balancers, only specific routing configurations are currently supported. OCI doesn’t support return to sender functionality through the OCI network firewall, and as a result, this design is considered unsupported in OCI as of this publication.



IGW Ingress Route Table

Destination	Target
10.0.4.0/24	OCI Network Firewall

NLB Subnet Route Table

Destination	Target
10.0.4.0/24	OCI Network Firewall
192.168.0.0/16	DRG

FW Subnet Route Table

Destination	Target
192.168.0.0/16	DRG

Web Tier Subnet Route Table

Destination	Target
192.168.0.0/16	DRG
10.0.2.187	OCI Network Firewall

Route ignored

NLB Source Preservation Mode

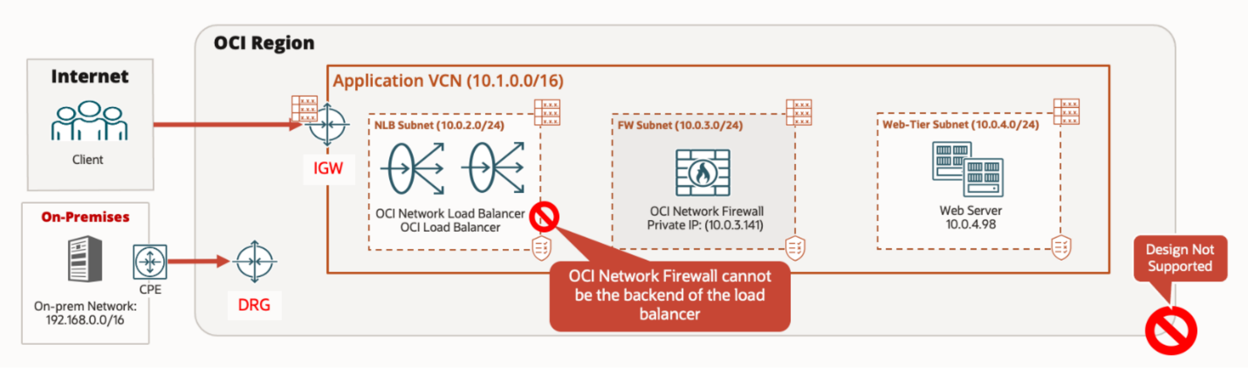
Traffic is not returned to the NLB via FW

Design not Supported

Figure 21: The topology for network load balancer source header (IP and port) preservation mode

OCI Network Firewall Backends for Load Balancers

Placing the OCI network firewall into a backend set of either an OCI network load balancer or OCI load balancer to enhance scalability and performance, high availability isn't supported because the OCI network firewall can't function as a backend for either the network load balancer or load balancer. This limitation arises from the lack of support for health checks with the OCI network firewall, which is a requirement for both load balancers. For true high availability, refer to the previous High Availability section that describes the OCI Network Firewall service's built-in high availability capabilities, which are designed to provide seamless failover and reliability without the need for any other deployed infrastructure, such as load balancers.



OCI Network Firewall cannot be the backend of the load balancer

Design Not Supported

Figure 22: Topology for OCI network firewall backends for load balancers

Conclusion

The OCI Network Firewall service offers a robust suite of features and capabilities that are essential for securing cloud environments. With its high availability, stateful network filtering, and advanced security measures, such as intrusion detection and SSL inspection, you can effectively safeguard their data and applications. The comprehensive policy-building framework allows for tailored configurations that meet specific operational needs, while flexible routing insertion scenarios facilitate seamless integration with existing infrastructures. By understanding and utilizing these functionalities, enterprises can enhance their security posture and ensure reliable connectivity across their cloud resources. The collection of real-world network design examples included in this tech brief provides a valuable resource for those looking to enhance their understanding of deploying, managing, and empowering their organization to confidently navigate the complexities of modern cloud security using the OCI Network Firewall service.

To learn more about the OCI Network Firewall and details on configurations, review the following resources:

- OCI Network Firewall Cloud Security services
- OCI Network Firewall online documentation
- OCI Network Firewall reference architecture
- 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

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

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