ORACLE

OCI Zero Trust Packet Routing Best Practices Guide

February, 2026, Version [1.0]

Public

Introduction

Oracle Cloud Infrastructure (OCI) Zero Trust Packet Routing provides an intent-based access control model for network communication. Instead of managing IP addresses, OCI Zero Trust Packet Routing lets you define which workloads can communicate using security attributes. This guide provides detailed, practical guidance for planning, deploying, and validating OCI Zero Trust Packet Routing in your OCI environment.

This document is designed for cloud architects, network administrators, and security practitioners responsible for implementing OCI Zero Trust Packet Routing at scale.

The goals of this guide are to

- Help you plan and adopt OCI Zero Trust Packet Routing in a phased approach.
- Provide clear guidance on defining security attributes and namespaces.
- Demonstrate best practices for writing security attribute to security attribute policies.
- Illustrate how to handle transitional scenarios where some workloads can't yet have an OCI Zero Trust Packet Routing security attribute applied.
- Provide troubleshooting guidance using OCI Network Path Analyzer and audit logs.

Planning your OCI Zero Trust Packet Routing adoption

Start small and grow gradually. Begin with a pilot workload or a set of related workloads within a single virtual cloud network (VCN) or across VCNs. This focused approach helps validate OCI Zero Trust Packet Routing security attribute application, policy creation, and access control before rolling out to production workloads.

Key planning steps

- **Identify candidate VCNs within a tenancy**: Select VCNs where workloads have clear communication patterns.
- **Document communication flows**: Map which workloads should communicate (for example, web → app → database) that you plan to migrate to OCI Zero Trust Packet Routing. To help ensure accuracy, reference security artifacts such as a port matrix or network flow table. If available, include a simple network diagram that shows workloads, their assigned OCI Zero Trust Packet Routing security attributes, and the communication paths being migrated. This helps validate that your security attribute assignments and policies align with the intended scope of OCI Zero Trust Packet Routing migration.
- **Determine the OCI Zero Trust Packet Routing security attribute application**: Identify which workloads can have an OCI Zero Trust Packet Routing security attribute applied immediately and which require transitional IP-based access. As part of planning, create a combined migration table that tracks the following for each workload or resource group (namespace and security attributes):
    - Subnet placement
    - Direction of communication (ingress/egress)
    - Security list (SL) and network security group (NSG) rules
    - The corresponding OCI Zero Trust Packet Routing policies for the starting, interim, and final states

  This helps maintain a consistent record throughout the migration. Also, always follow a safe migration strategy: Never apply a security attribute to an existing workload before adding the corresponding OCI Zero

Trust Packet Routing policy that preserves its current access. This helps ensure continuity and prevents unintended traffic drops during the transition.

- **Establish a rollback plan**: Keep NSG or SL rules temporarily until OCI Zero Trust Packet Routing enforcement is validated.

The pilot phase should confirm that OCI Zero Trust Packet Routing is implemented correctly in your environment. Consider defining clear milestones and exit criteria to guide your transition to OCI Zero Trust Packet Routing. This helps your teams, security stakeholders, and application owners adopt OCI Zero Trust Packet Routing in a structured, low-risk, and predictable manner. Below are general guidelines you can use to create four to five well-defined milestones for your OCI Zero Trust Packet Routing adoption journey, along with example exit criteria for each. Below are example milestones.

Milestone 1: Prepare and understand your environment. Build a clear picture of your cloud environment and understand which applications and workloads will first move to OCI Zero Trust Packet Routing. This helps ensure you're designing policy only for what matters and avoids surprises later.

This milestone's focus

- Inventorying VCNs, subnets, workloads, and key paths
- Understanding application-to-application connectivity
- Identifying the first apps/environments to onboard
- Helping ensure all internal security and governance approvals are in place

Exit criteria

- Complete list of resources and communication flows
- OCI Zero Trust Packet Routing scope (initial apps and workloads) agreed upon
- Initial plan for security attribute grouping drafted

Milestone 2: Define your security attribute model and assign security attributes. Establish a consistent security attribute naming and grouping model. A strong security attribute model forms the foundation of effective OCI Zero Trust Packet Routing policy design.

This milestone's focus

- Agreeing on naming conventions
- Grouping workloads using tiers or resource types
- Handling special cases or exceptions
- Assigning security attributes to resources in a controlled manner

Exit criteria

- Security attribute naming conventions finalized
- Security attribute assignments completed for the scoped environment

Milestone 3: Write, validate, and review OCI Zero Trust Packet Routing policies. Translate your intent into OCI Zero Trust Packet Routing policies and help ensure they reflect how your applications should communicate.

This milestone's focus

- Drafting policies based on real communication needs
- Validating policies with app owners
- Testing or simulating expected access
- Documenting standard patterns for future policies

Exit criteria

- Policies drafted for all scoped flows
- Validation completed with relevant teams
- Tests confirm policies behave as expected
- Policies established for reuse in future apps

Milestone 4: Rollout, monitor, and move to enforcement. Help ensure all workloads are correctly tagged and OCI Zero Trust Packet Routing policies enforce the intended access without disrupting operations. This milestone confirms that your OCI Zero Trust Packet Routing deployment is functioning as expected in a live environment.

This milestone's focus

- Assign security attributes to all OCI Zero Trust Packet Routing–supported resources.
- Monitor service health for at least three days.
- Test and verify that all required traffic flows are allowed and no critical communication is blocked.
- Confirm that monitoring, security scanning, and administrative access (SSH via bastion) continue to function properly.

Exit criteria

- All resources are correctly tagged with security attributes.
- Services operate normally without unintended disruptions.
- Connectivity, monitoring, and scanning validated successfully.

Once stable, expand gradually to other workloads and VCNs.

Designing security attributes and namespaces

A namespace is a logical container for one or more security attributes. A security attribute is a label you assign to supported OCI resources, and it can be referenced in OCI Zero Trust Packet Routing policies to govern allowed communication.

Selecting a namespace

- **Default namespace**: For small environments, the default `Oracle-ZPR` namespace is sufficient.
- **Custom namespace**: For large-scale or multiteam environments, create namespaces aligned with organizational structure. A recommended pattern is service-name.lifecycle (for example, inventory-dev for the development instance of a service). This helps ensure namespaces are unique, descriptive, and scalable.
    - `Zpr.application i.e zpr is namespace and application is security attributes`
    - `Zpr.finance`
    - `Zpr.devops`

Referencing security attributes in policies

- Policies use the combination of namespace and security attribute to define which workloads are allowed to communicate.

- For the default namespace, only the security attributes need to be referenced.
- For custom namespaces, the namespace name must be included along with the security attributes.
- If traffic crosses outside the OCI Zero Trust Packet Routing–managed scope, IP addresses must be used instead of security attributes.

Security attribute naming conventions

Security attribute names should be clear, descriptive, and consistent. The pattern you choose depends on your environment and organizational needs. You can base security attribute names on the function or tier of your application (e.g., web, app, database) or on the resource type.

Function or tier: web:frontend, app:payment-service, db:orders

Resource type: svc:bastion, compute:web, db:orders

Best practices for security attribute design

- Keep names descriptive and stable.
- Avoid embedding environment names unless necessary.

Writing OCI Zero Trust Packet Routing policies

OCI Zero Trust Packet Routing policies define which workloads can communicate based on their security attributes. Policies cover different scenarios depending on where workloads reside and their migration state: within the same VCN, across different VCNs, communicating with on-premises or internet endpoints, or during transitional phases where some workloads don't yet have security attributes applied. This overview provides context for the syntax and examples that follow.

Policy syntax overview

Single VCN syntax

```
in <VCN security attribute name> VCN allow <source SA> endpoints to connect to
<destination SA> endpoints
```

Example

```
in network:backend-vcn VCN allow app:payment-service endpoints to connect to
db:orders endpoints
```

Cross-VCN syntax

```
allow <source SA> endpoints in <source VCN SA> VCN to connect to <destination SA>
endpoints in <destination VCN SA> VCN
```

Example

```
allow web:frontend endpoints in network:frontend-vcn VCN to connect to app:payment-
service endpoints in network:backend-vcn VCN
```

Tagged-to-untagged (transitional) syntax

```
in <VCN security attribute name> VCN allow <source SA> endpoints to connect to <IP address of untagged workload>
```

Example:

```
in network:backend-vcn VCN allow app:payment-service endpoints to connect to '10.0.2.5/32'// This is a sample for tagged to untagged policy
```

Policy best practices

- Write the most restrictive policy that satisfies intended communication.
- Use end of line comments or naming conventions for clarity.
- Replace IP-based transitional policies once all workloads have OCI Zero Trust Packet Routing security attributes applied.

Migration and transitional policies

When adopting OCI Zero Trust Packet Routing, some workloads may already have OCI Zero Trust Packet Routing security attributes applied, while other workloads in the same VCN or in connected VCNs aren't yet migrated or migration is planned for a later time. It's important to ensure that workloads with applied attributes can continue to communicate with these untagged workloads during the migration phase.

For example, in a multitier application

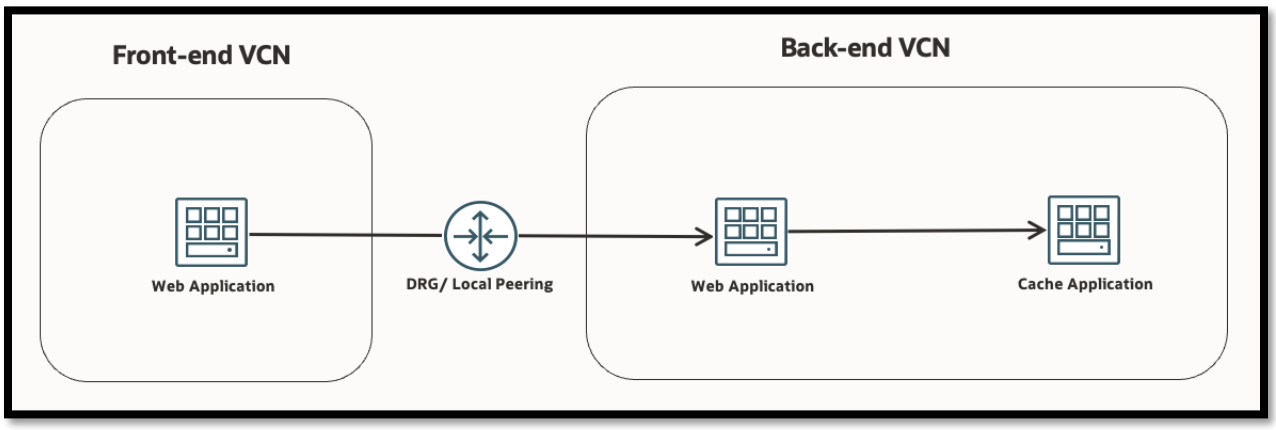

Figure 1: example application

- Web and app workloads have OCI Zero Trust Packet Routing security attributes applied (`web:frontend`, `app:payment-service`).
- A legacy cache workload in the backend VCN doesn't yet have an OCI Zero Trust Packet Routing security attribute, and migration is planned for a later phase.
- The goal is to migrate the core workloads to OCI Zero Trust Packet Routing while maintaining secure connectivity to the legacy cache instance.

OCI Zero Trust Packet Routing supports transitional IP-based policies to allow communication between workloads with applied OCI Zero Trust Packet Routing security attributes and those without. This helps ensure continuity of operations during phased adoption.

Transitional policy syntax

```
in <VCN security attribute name> VCN allow <source SA> endpoints to connect to <IP address of untagged workload>
```

Example

- Backend VCN workloads
  - `app:payment-service` (OCI Zero Trust Packet Routing security attribute applied)
  - Legacy cache instance at IP `10.0.2.5` (no OCI Zero Trust Packet Routing security attribute yet)
- Transitional policy

```
in network:backend-vcn VCN allow app:payment-service endpoints to connect to '10.0.2.5/32'
```

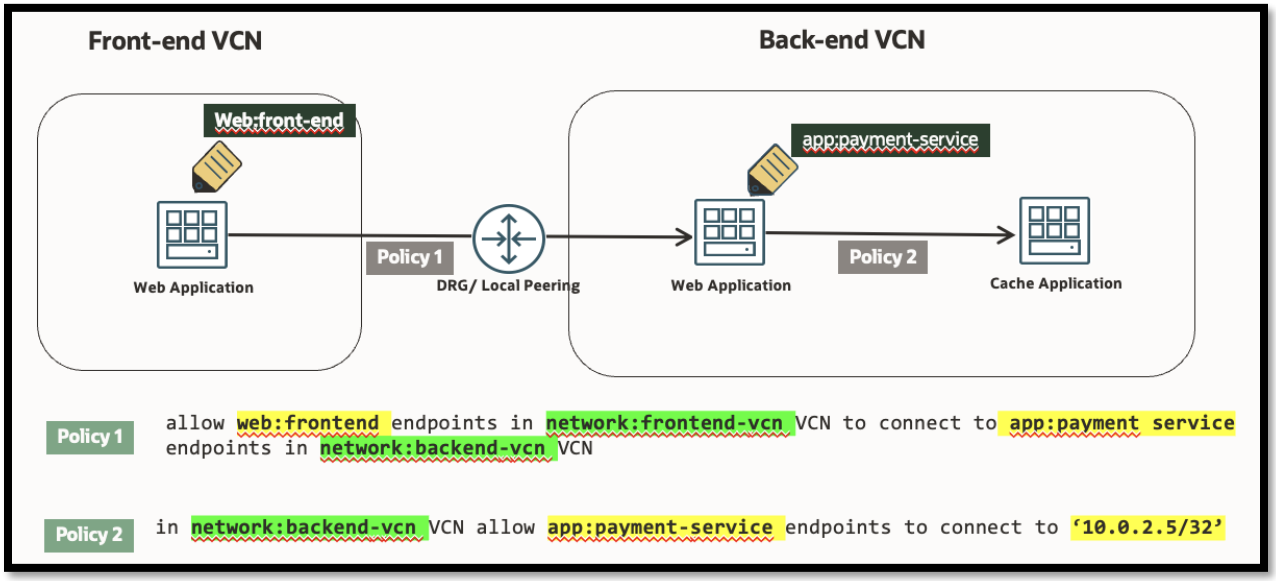

Figure 2: transitional phase

Best practices for transitional policies

- Apply only for workloads that can't yet have OCI Zero Trust Packet Routing security attributes.
- Limit the scope to essential communications.
- Remove transitional IP-based policies once untagged workloads are migrated and have OCI Zero Trust Packet Routing security attributes.
- Avoid broad IP-based rules that may expose additional resources.

This approach allows incremental migration of workloads while preserving secure and controlled connectivity. Using OCI Zero Trust Packet Routing's intent-based policies alongside transitional rules provide a clear path toward full zero trust adoption. However, transitional IP-based policies aren't intended to be a permanent operating model. You're encouraged to avoid remaining in the transitional phase indefinitely. The next step is to migrate the remaining legacy

workloads to OCI Zero Trust Packet Routing by applying appropriate OCI Zero Trust Packet Routing security attributes, defining security attribute to security attribute–based policies for the required communication, and removing the transitional IP-based policies. This completes the transition to a fully intent-driven OCI Zero Trust Packet Routing model. As illustrated in the diagram below, the cache service is assigned the app:cache security attribute, a security attribute–based policy is introduced, and the IP-based policy is removed.

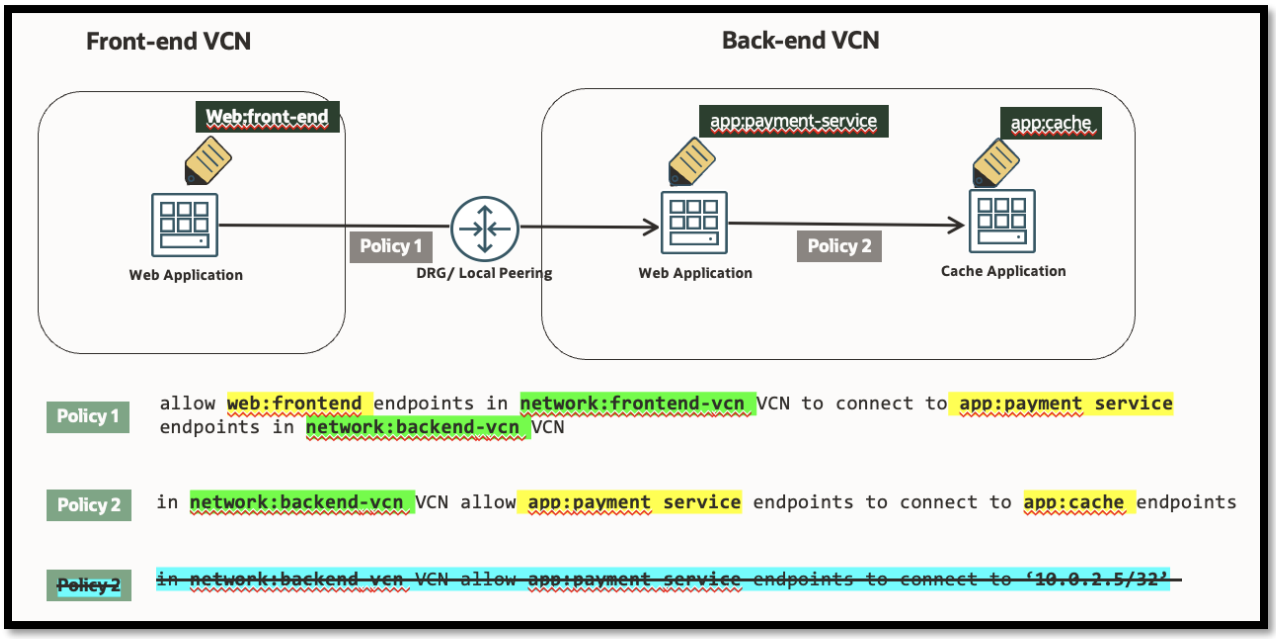

Figure 3: full migration to OCI Zero Trust Packet Routing

Troubleshooting with OCI Network Path Analyzer

OCI Network Path Analyzer provides a visual representation of how OCI Zero Trust Packet Routing enforces traffic between workloads. It integrates with OCI Zero Trust Packet Routing policies, as well as traditional NSG/SL configurations, to show whether workloads can communicate based on the applied policies. OCI Network Path Analyzer can also indicate if OCI Zero Trust Packet Routing policies exist for the selected workloads and whether those policies allow or deny traffic.

Using OCI Network Path Analyzer for OCI Zero Trust Packet Routing validation

1. **Launch OCI Network Path Analyzer**
   - You can launch OCI Network Path Analyzer directly from the OCI Zero Trust Packet Routing console for selected workloads.
   - Alternatively, open the OCI Network Path Analyzer UI from the OCI console for detailed path analysis.
2. **Select source and destination endpoints**
   - Choose the workloads you want to validate.
   - OCI Network Path Analyzer will consider applied OCI Zero Trust Packet Routing security attributes, VCNs, subnets, NSGs, and SLs.
3. **Review analysis results**
   OCI Network Path Analyzer displays
   - **Effective routing path**: how traffic flows through the network
   - **Applied NSG or SL rules**: any network rules affecting connectivity
   - **ZPR policy evaluation**: indicates if traffic is allowed or denied based on OCI Zero Trust Packet Routing policies

- **Missing or misapplied OCI Zero Trust Packet Routing security attributes**: highlights workloads that don't have the expected attributes applied
- **Policy availability**: shows whether OCI Zero Trust Packet Routing policies exist for the selected resources

Best practices when using OCI Network Path Analyzer

When using OCI Network Path Analyzer, ensure that the source and destination workloads have the correct OCI Zero Trust Packet Routing security attributes and that policies are scoped to the appropriate VCNs and namespaces. Use OCI Network Path Analyzer results with OCI Audit logs to validate policy evaluation and connectivity behavior. Run OCI Network Path Analyzer iteratively when onboarding new workloads or updating policies to confirm the impact of changes.

Using OCI Zero Trust Packet Routing with existing NSG and SL rules

Many organizations adopting OCI Zero Trust Packet Routing already have NSGs and SLs defined. Understanding how OCI Zero Trust Packet Routing interacts with these network controls is critical for planning and adoption.

Key principles

- For any communication to succeed, both NSG/SL rules and OCI Zero Trust Packet Routing policies must permit it.
- If OCI Zero Trust Packet Routing permits traffic but NSG/SL blocks it, traffic will be dropped.
- Conversely, if NSG/SL allows traffic but OCI Zero Trust Packet Routing denies it, traffic will also be dropped.

For new customers

- You don't need to rewrite all NSG and SL rules to match OCI Zero Trust Packet Routing policies.
- You can keep NSG/SL rules broadly permissive (open) while writing specific OCI Zero Trust Packet Routing policies to control access.
- Traffic will flow only if there is an OCI Zero Trust Packet Routing policy permitting it, even when NSG/SL rules are open.

Guidelines for a smooth adoption

1. Define OCI Zero Trust Packet Routing security attributes and policies first
    a. Identify workloads and the intended communication paths.
    b. Write SA-to-SA OCI Zero Trust Packet Routing policies to allow required connectivity.
2. Validate policies
    a. Use OCI Network Path Analyzer and OCI Audit logs to verify that intended traffic is allowed.
    b. This helps ensure the policies behave as expected before applying security attributes.
3. Apply security attributes to workloads
    a. OCI Zero Trust Packet Routing policies become effective only after security attributes are applied.
    b. Until then, NSG/SL rules alone govern connectivity.
4. Use automation to minimize downtime
    a. Apply security attributes using scripts or Terraform for large fleets.
    b. Consider a phased rollout, applying attributes incrementally across VCNs or resource groups.

Best practices

- Keep NSG/SL rules permissive during the initial OCI Zero Trust Packet Routing rollout to reduce service disruption.
- Avoid relying solely on NSG/SL rules for security once OCI Zero Trust Packet Routing is in place.
- Plan and communicate changes with application teams to minimize unexpected downtime.

This approach helps ensure that OCI Zero Trust Packet Routing adoption can proceed safely and incrementally, leveraging existing NSG/SL configurations while moving to an intent-based, policy-driven access model.

OCI Zero Trust Packet Routing permissions and IAM policies

As organizations expand their OCI Zero Trust Packet Routing deployments, application or compartment administrators often need to manage policies for their own workloads without relying on tenancy-level administrators for every change. Delegating this responsibility improves operational efficiency, reduces delays, and supports teams that frequently deploy or modify services.

At the same time, security attributes define which workloads are allowed to communicate. Assigning or modifying an SA effectively changes a workload's trust level. Unrestricted security attributes management could introduce risk if users assign privileged attributes to resources they control, potentially granting unintended access. For example, if a database only allows connections from workloads labeled with a specific security attribute, a person who can freely assign attributes could launch a new instance and apply that security attribute, thereby gaining unauthorized access. For this reason, attribute assignment should be treated with the same care as policy creation.

Delegating administration safely

Delegation can be implemented without weakening security by scoping administrative permissions appropriately; for example, designated compartment administrators or approved identity groups can manage OCI Zero Trust Packet Routing policies and attributes while being restricted to resources within their authorized compartments. This approach lets teams operate independently within their environments without affecting other workloads or compartments in the tenancy.

Administrative scope should always be aligned with resource scope. Administrators may be able to define policies, but those policies should only apply to resources they're authorized to manage. This helps ensure operational agility while maintaining strong security boundaries.

To support environments where applications scale dynamically, attribute assignment should be integrated into the provisioning workflow. Automation identities, such as deployment pipelines or infrastructure-as-code tools, can create resources and automatically apply predefined attributes to help ensure new instances have the correct trust level. These identities shouldn't have permissions to create new attributes or modify policies, preserving security while supporting elasticity.

Separating responsibilities

A secure deployment separates resource lifecycle actions from trust assignment actions. This prevents a single identity from both creating a workload and granting it privileged network access.

Function	Recommended owner
Security attribute and namespace definition	Security administrators

Policy creation and review	Authorized administrators
Resource creation	Application teams
Attribute application	Automation identities or restricted roles

This model lets application teams deploy workloads efficiently while helping ensure that trust decisions remain controlled.

Managing attribute permissions

Security attribute permissions should be granted based on role and function:

- Limit creation and modification of SAs to trusted administrators.
- Allow SA application only to approved roles or automation identities.
- Avoid granting broad SA management rights to general users.

Carefully controlling these permissions helps ensure that SAs remain reliable indicators of workload identity and trust level.

For most organizations, a layered delegation model provides the best balance between efficiency and security. The security team defines the SAs and governance standards, authorized administrators manage policies within their scope, application teams handle workload deployment, and automation systems provision resources with the correct attributes. This combination allows teams to act independently while maintaining consistent trust enforcement across the tenancy.

Common anti-patterns to avoid

- Writing overly broad policies (e.g. all-to-all communications, or using 'all-endpoints')
- Reusing SAs inconsistently across VCNs
- Leaving transitional IP-based rules after full OCI Zero Trust Packet Routing security attribute application

OCI Zero Trust Packet Routing troubleshooting checklist

1. **Verify OCI Zero Trust Packet Routing security attribute application**
    - Confirm both source and destination workloads have correct attributes applied.
    - Validate namespace and SA name consistency.
2. **Check policy coverage**
    - Ensure relevant policies exist (single VCN, cross VCN, or transitional).
3. **Use OCI Network Path Analyzer**
    - Visualize allowed/denied paths and check for missing SAs.
4. **Check OCI Audit logs**
    - Confirm OCI Zero Trust Packet Routing policy evaluation and identify denied connections.
5. **Validate connectivity**

- Test application-level communication.

6. **Iterate and correct**
   - Adjust policies or SAs, and remove transitional IP rules

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